Joint Publication 6-0

Joint Communications System

10 June 2015
Incorporating Change 1
04 October 2019

PREFACE

1. Scope

a. This publication is the keystone document for the communications system series of publications. It provides fundamental principles and guidance to plan, execute, and assess communications system support to joint operations.

b. An array of information, underpinned by joint doctrine, is utilized to employ combat power across the range of military operations. The communications system provides the means to synchronize joint forces.

c. Reliable, secure, and synchronized information sharing among joint forces, multinational forces, and with non-Department of Defense agencies is essential for effective command and control in today's network-enabled environment. Information systems and networks provide the means to send, receive, share, and utilize information. The synthesis of advanced communications system capabilities and sound doctrine leads to information superiority, which is essential to success in all military operations.

2. Purpose

This publication is the Chairman of the Joint Chiefs of Staff (CJCS) official advice concerning communications in joint operations and provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners. It does not restrict the authority of the joint force commander (JFC) from organizing forces and executing the mission in a manner deemed most appropriate to ensure unity of effort.

3. Application

a. Joint doctrine established in this publication applies to the Joint Staff, commanders of combatant commands, subordinate unified commands, joint task forces, subordinate components of these commands, the Services, the National Guard Bureau, and combat support agencies.

b. This doctrine constitutes official advice concerning the enclosed subject matter; however, the judgment of the commander is paramount in all situations.

c. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the CJCS, normally in coordination with the other members of the Joint Chiefs of Staff, provides more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

DANIEL J. O'DONOHUE
Lieutenant General, USMC
Director, Joint Force Development

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 6-0
DATED 10 JUNE 2015

- **Reassigns cyberspace responsibilities to the United States Cyber Command in accordance with the latest *Unified Command Plan.***

- **Relocates cyberspace operations from The Role of the Communications System section in Chapter I, "Joint Communications System Overview," to the Cyberspace and Cyberspace Operations section in Chapter II, "The Information Environment."**

- **Applies correct cyberspace-related terminology and aligns Joint Publication (JP) 6-0, *Joint Communications System,* with JP 3-12, *Cyberspace Operations.***

- **Aligns electromagnetic spectrum management and operations with other JPs.**

- **Removes the reference to joint cyber centers as a requirement for a combatant command.**

- **Updates multiple references to correct publications.**

Intentionally Blank

TABLE OF CONTENTS

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Provides an overview of the Joint Communication System**
- **Describes the Information Environment**
- **Addresses Joint Force Communication, System Operations, and Management Planning**
- **Covers Information Sharing and Services**
- **Addresses Communications System Support to the President, the Secretary of Defense, and the Intelligence Community**

Joint Communications System Overview

Introduction

A joint communications system is composed of the networks and services that enable operations of joint and multinational military capabilities and assist the joint force commander (JFC) in command and control (C2) of military operations.

The Department of Defense information network (DODIN) is all Department of Defense (DOD) cyberspace, including the DOD's end-to-end digital communications systems supporting the JFC.

The joint functions of C2, intelligence, fires, movement and maneuver, protection, information, and sustainment depend on communication systems that tie together joint operations. Communication systems enable JFCs and their staffs to initiate, direct, monitor, question, and react.

Command and Control Systems

Elements of the C2 System. The first element of a C2 system is the people—people who acquire information, make decisions, take action, communicate, and collaborate with one another to achieve objectives. The second element of the C2 system is comprised of the facilities, equipment, communications, staff functions, and procedures essential to a commander's ability to plan, direct, monitor, and control operations of assigned forces pursuant to the missions assigned.

Quality of Information. There are three basic uses for information. The first is to help create situational awareness (SA) as the basis for a decision. The second is to direct and coordinate actions to execute the decision. The third is to help assess the performance and effectiveness of those actions.

Information Management (IM). Good IM makes accomplishment of other tasks less complex. Automation and standardization of communications processes and procedures improve IM and aid the commander's effectiveness and speed of C2.

Records management (RM) is the practice of maintaining records, including categorizing, storing, securing, destruction, or archival preservation. The goal of RM is to protect valuable historical archives and ensure permanent records are accessible and readable for years to come.

The Role of the Communications System

The communications system is the JFC's principal tool to collect, process, store, disseminate, and manage information. Given the criticality of information, the security of the communications system is paramount to ensuring the commander can trust the information provided and received. Effective C2, through the exchange of information, integrates joint force components and enables them to function effectively across vast distances, in austere or complex environments, and in all weather conditions.

Communications System Principles

Joint force employment decisions are influenced by the communications system's ability to network the force. This inseparably links network control to C2 prioritization and decisions. The communications system must be **interoperable, agile, trusted**, and **shared** to provide the flexibility to dynamically meet mission objectives.

Communications System Functions

Information system components that make up the joint communications system facilitate the capabilities to **collect, process, store, disseminate**, and **manage** information.

Essential Services

The following information technology (IT) services form the minimum capabilities required by the JFC:

- Voice services, to include assured and non-assured voice.
- Video services, to include video conferencing.
- Collaborations services, to include messaging, presence, multi-user chat, and web conferencing.
- Common operational picture services, to include global picture and a common tactical picture.
- Joint planning, execution, and assessment services.
- Intelligence services.
- C2 system services.
- Web-based access to mission services.
- Cross-domain information sharing services.
- Control of IT services.
- Communications interoperability with allies and other mission partners.

The Information Environment

The joint information environment framework is a set of mandatory standards, protocols, and principles that provides a secure and reliable shared IT infrastructure, enterprise services, and a single security architecture to achieve information superiority, improve mission effectiveness, increase security, and improve IT efficiency. This framework enables DOD to acquire, operate, secure, and maintain IT capabilities to improve information sharing and better address cybersecurity.

Cyberspace and Cyberspace Operations

Cyberspace. Cyberspace is a global domain within the information environment consisting of the interdependent networks of IT infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Digital communications systems are a subset of cyberspace; virtually all DOD operations and administration rely on a secure and stable cyberspace.

Cyberspace Operations (CO). CO are the employment of cyberspace capabilities where the primary purpose is to achieve JFC objectives in or through cyberspace. Although most of these actions are simply cyberspace-enabled activities, cyberspace forces conduct the CO missions using digital communications systems and other cyberspace capabilities. Specifically, the DODIN operations and defensive cyberspace operations-internal defensive measures (DCO-IDM) missions protect these digital communication systems and, when directed, other portions of blue cyberspace.

Department of Defense Information Network Operations Construct

The DODIN supports DOD missions and functions and is central to joint and multinational operations. Joint operations, which vary in scope, purpose, and conflict intensity, require portable, universally accessible technologies to realize C2 and further enhance mission effectiveness. The DODIN supports all military operations by enabling US mission partners to securely and seamlessly share required information.

The Tactical Level

The tactical network environment may be supported with joint communications nodes. A node is capable of connecting to the local information network through both DOD and non-DOD transport systems and is capable of providing a deployed force with networks and services at both the unclassified (e.g., Non-classified Internet Protocol Router Network and classified (e.g., SECRET Internet Protocol Router Network) levels.

Network Operations, Network Management Cross Flows

Deployed networks within the DODIN require a framework to address the network management cross flows required to establish seamless transitions across systems to support information exchange between administrative, logistics, and tactical networks.

Operations in Degraded and Denied Environments

Adversaries operate in a gray zone, conducting actions short of war such as misleading or inaccurate information activities and cyberspace attacks to offset US technological advantages. Enemies often adopt strategies that take advantage of a range of capabilities to deny friendly forces a conventional

force-on-force fight. Enemies are pursuing technologies to challenge our freedom of maneuver and our ability to operate in the electromagnetic spectrum (EMS)/information environment.

Roles and Responsibilities

The provisioning of DODIN enterprise services includes all combatant commanders' (CCDRs') missions, DOD agencies, and all DOD users from anywhere in the world. The DODIN supports DOD users who are deployed or operating away from their home base. The DODIN IT infrastructure, information services, data, policies, standards, and procedures must support the operational forces in all of their assigned missions. The DODIN must be flexible and tailorable to accommodate changes required by the various CCDR missions. The DODIN must also be capable of supporting operations at all levels of warfare from strategic to tactical operations. To enable the DODIN to adequately support the operational commanders, proper coordination of network assets ensures all CCDRs receive a similar level of service and effectiveness.

Joint Force Communication, System Operations, and Management Planning

Planning and Management Organizations

Communications system management combines centralized control with decentralized execution and provides effective and efficient communications system support for the JFC:

- **Joint Network Operations Control Center (JNCC).** The JNCC, through the components and Services, controls the joint communications networks under JFC authority and US Cyber Command's directive authority for cyberspace operations.
- **Service Component Management.** Service components and assigned support organizations should designate a single office within their communications staffs to coordinate with the joint force communications system directorate of a joint staff (J-6).

- **The joint IM board** serves as the JFC's principal organization to draft the commander's information dissemination policy and coordinates IM functions within the joint force.

Planning and Management Structure

The CCDR, through the CO planning staff and J-6, provides communications system guidance and priorities that support the commands and the components through the theater network operations control center theater network operations control center (TNCC) or the equivalent organization. The TNCC works closely with subordinate JNCCs to ensure accurate, timely, and detailed reporting by subordinate and supporting agencies and organizations. Additionally, the TNCC works closely with the (CCDR's) CO planning staff and the CO-integrated planning element to support CO planning, DODIN operations, DCO-IDM, information dissemination management, and to share SA of CCDR's communications systems.

Communications Planning and Management

Systems Requirements. The JFC's mission, C2 framework, and location of assigned forces determine the essential elements of the communications system employed. Specific command relationships and the organization of units and staffs drive the interconnecting communications methods and means. The communications system supports and provides an assured flow of information to and from commanders at all levels during all phases of an operation. The communications system must be disciplined, flexible, interoperable, responsive, mobile, survivable, secure, and sustainable to enable common awareness, speed decision making, and integrate actions of the joint force.

Planning and Operations. Joint planning and operations are the development and implementation of campaign plans, contingency plans, and operation orders prepared in response to requirements from the President, Secretary of Defense (SecDef), or Chairman of the Joint Chiefs of Staff (CJCS). They include a system of policies, procedures, processes, and reporting structures—supported by

communications and IT used by the joint planning and execution community to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities associated with joint forces.

Multinational Communications System Operations

Multinational communications system operations may be composed of allied and/or coalition partners. A multinational force can be composed of diverse groups of security and information sharing environments. Planning considerations include network federation, governance, and management of a federated network and EMS operations; equipment compatibility; procedural compatibility; application and configuration management compatibility; cybersecurity, including requirements for cryptographic security; identification, friend or foe; lessons learned from previous operations; video networks (e.g., video teleconferencing, sensor video feeds, commercial news feeds, and global broadcast services); and data link protocols.

Communications Planning Methodology

Planners within J-6 coordinate with their counterparts within the operations, intelligence, logistics, administrative, and policy communities to ensure proper consideration and inclusion of communications system support in mission execution. In addition, they plan the evolution of the communications system to support future operations. Communications system planning is divided into five areas: mission analysis; information requirements analysis; interoperability, compatibility, and supportability analysis; capability analysis; and allocation of communications system assets.

Communications Planning Factors

The important factors for a communications system plan are feasibility and the adequacy of the plan to satisfy the JFC's information requirements. A useful first step is the constant assessment of the communications system plan during the development process for its consistency with basic communications system principles.

Other factors to consider as the communications system plan is developed are:

- **Organic communications system resources.**
- **Practical communications system support.**
- **Time-phased force and deployment data flow.**
- **Joint reception, staging, onward movement, and integration.**
- **Incremental building.**
- **Modular packaging.**
- **Interoperability.**
- **Standardization.**
- **Impact of internal and external changes to C2.**
- **Operational contract support.**
- **Training.**
- **Discipline.**
- **Timeliness.**
- **Simultaneous planning.**

Communications System Employment

Communications system needs and capabilities of a small joint force with a limited humanitarian mission are vastly different from those of a CCDR with continuing, multitasked, multinational-based combat missions. The phases of a joint operation or campaign are situation- and mission-dependent. Timelines between phases may be severely compressed and may not follow each other or terminate in the expected sequence. However, defined phases provide a guideline for the JFC and communications system planner.

Information Sharing and Services

US national security depends on the ability to share the right information, with the right people, at the right time. **Information sharing** requires sustained and responsible **collaboration** between federal, state, local, tribal, territorial, private-sector, and multinational partners. The dynamic operational environment presents challenges to continue improving information sharing and safeguarding processes and capabilities. While innovation has enhanced the ability to share, increased sharing has created the potential for vulnerabilities requiring strengthened safeguarding practices.

Mission Partners

Joint forces must be able to integrate effectively with US Government departments and agencies, partner-nation militaries, and indigenous and regional stakeholders. This integration must be scalable, ranging from the ability of an individual unit to utilize the expertise of a nongovernmental partner to multinational operations. The mission partner environment information sharing capability framework has been developed using these criteria to enable assured information exchange among mission partners and consists of a combination of people, systems, policies, procedures, and processes to plan, prepare, and execute operations within a collaborative information environment.

Enablers

The five touchstones of information sharing are: culture, policy, governance, economics and resources, and technology and infrastructure. To enable the achievement of DOD information sharing objectives, the DODIN should:

- Promote and encourage sharing.
- Achieve an extended enterprise.
- Strengthen agility to accommodate unanticipated partners and events.
- Ensure trust across organizations.

Other enablers are global authentication, access control, directory services, and cloud services that provide any authorized user with common and portable identity credentials and visibility of, and access to, all appropriate operational, business support, or intelligence-related information, services, and applications related to their mission and communities of interest.

Other Information Considerations

Information and Communications Technology. Growing numbers and types of networked devices increase the "threat surfaces" in cyberspace.

Insider Threat Mitigation. Due to continued high-profile information protection failures, the JFC should take actions to better safeguard information and deter and detect malicious insider activity on the DODIN and within the joint force headquarters.

Intelligence Community. Intelligence provides threat assessments that are crucial to force protection and military operations for homeland defense.

Communications System Support to the President, the Secretary of Defense, and the Intelligence Community

National Military Command System

The National Military Command System (NMCS) is a system of critical command centers, C2 nodes, and underlying support systems that are a priority component of the DODIN. It is designed to support the President, SecDef, CJCS, and other senior leaders in the exercise of their responsibilities through the range of military operations. The NMCS provides the means by which the President and SecDef receive warning and intelligence that underpin accurate and timely decision making. Additionally, it provides the means by which national leaders apply the resources of the Services, assign military missions, and communicate strategic direction to CCDRs or other commanders.

Nuclear Command and Control System

The Nuclear Command and Control System (NCCS) comprises the critical core NMCS capability that enables the President to consult with SecDef, the CJCS, CCDRs, and other advisors to assess the scope and intent of a threat and direct the transfer, deployment, employment, recall, or termination of US nuclear weapons. General operational responsibility for the NCCS lies with the CJCS and is centrally directed through the Joint Staff.

Intelligence

The intelligence portion of the DODIN is designed to provide an architecture that can be individually tailored to the specific needs of a joint force, ensures survivability and flexibility through distributed operations, and can be rapidly reconfigured and recovered to accommodate changing demands and responsibilities. Although intelligence organizations use a variety of sensors and other information sources to collect and analyze data and produce intelligence products, the communications system support to intelligence is normally limited to providing the communications

interface and transport media required to move intelligence and related information.

National Security and Emergency Preparedness Communications

The Department of Homeland Security Office of Emergency Communications leads the national security and emergency preparedness communications efforts and the office programs and services coordinate emergency communications planning, preparation, and evaluation to ensure safer, better-prepared communities nationwide.

Conclusion

This publication is the keystone document for the communications system series of publications. It provides doctrine to plan, execute, and assess communications system support to joint operations.

Intentionally Blank

CHAPTER I
JOINT COMMUNICATIONS SYSTEM OVERVIEW

"Fighting with a large army under your command is nowise different from fighting with a small one: it is merely a question of instituting signs and signals."

Sun Tzu
***The Art of War*, circa 500 BCE**

1. Introduction

a. A joint communications system is composed of the networks and services that enable operations of joint and multinational military capabilities and assist the joint force commander (JFC) in command and control (C2) of military operations. Effective C2 is vital for proper integration and employment of capabilities. The Department of Defense information network (DODIN) is all Department of Defense (DOD) cyberspace, including the DOD's end-to-end digital communications systems supporting the JFC (see Appendix A, "Department of Defense Information Network Telecommunications Infrastructure Components," for more information). The DODIN is the set of information capabilities and associated processes to collect, process, store, disseminate, and manage 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. Most DOD cyberspace actions use cyberspace to enable other types of activities that employ cyberspace capabilities to complete tasks but are not undertaken as part of one of the three cyberspace operations (CO) missions: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DODIN operations. This publication explains how DODIN operations and defensive cyberspace operations-internal defensive measures (DCO-IDM) contribute to the protection and operation of communications systems. The DODIN unifies DOD's information systems and networks into an information system that provides increased information capabilities to the joint force. Communications systems are more than electronic boxes, wires, and radio signals, and the DODIN is more than a collection of information networks. The interdependence of the parts, as well as the processes, policies, and data on those systems, permeate daily life and preparation for and execution of operations. An effective communications system helps commanders maintain the unity of effort to apply their forces' capabilities at critical times and places to achieve objectives.

b. Commanders must make decisions in conditions of uncertainty. Access to accurate, reliable, and timely information reduces uncertainty and the risk of making poor decisions. The DODIN provides commanders with the ability to collect, process, store, disseminate, and manage decision quality information. To facilitate the execution and processes of C2, the C2 systems must rapidly furnish reliable and secure information to the chain of command. The joint functions of C2, intelligence, fires, movement and maneuver, protection, information, and sustainment depend on communication systems that tie together joint operations. Communication systems enable JFCs and their staffs to initiate,

direct, monitor, question, and react. Ultimately, effective C2 depends on the right person having the right information at the right time to support decision making.

c. The term mission partner refers to those with whom DOD cooperates to achieve national objectives. This includes other departments and agencies of the United States Government (USG); state and local governments; allies, multinational force members, host nations (HNs), and other nations; international organizations; nongovernmental organizations (NGOs); and the private sector.

For more information, see Department of Defense Directive (DODD) 8000.01, Management of the Department of Defense Information Enterprise (DOD-IE).

2. Command and Control Systems

a. **Elements of the C2 System.** The first element of a C2 system is the **people**—people who acquire information, make decisions, take action, communicate, and collaborate with one another to achieve objectives. Members of the joint force—from the senior commander framing a strategic concept to the most junior Service member at the tactical level calling in a situation report—are integral components of the joint communications system and not merely users. The second element of the C2 system is comprised of the **facilities, equipment, communications, staff functions, and procedures** essential to a commander's ability to plan, direct, monitor, and control operations of assigned forces pursuant to the missions assigned. Although families of hardware are often referred to as systems, the C2 system is more than simply equipment. High-quality equipment and advanced technology do not guarantee adequate communications or effective C2. Both start with well-trained and qualified people supported by an effective guiding philosophy and procedures.

b. **Quality of Information.** There are three basic uses for information. The first is to help create situational awareness (SA) as the basis for a decision. The second is to direct and coordinate actions to execute the decision. The third is to help assess the performance and effectiveness of those actions. Effective C2 is inherently dependent on information: obtaining it; evaluating its accuracy; judging its value based on situational context; processing it into useful form; acting on it; and sharing it with forces who need it in the most expeditious, secure manner. The C2 system must present information in a manner that is understood and useful at every required level of decision making—strategic, operational, and tactical. The seven attributes shown in Figure I-1 help characterize information quality. Combining pieces of information with context produces ideas or provides knowledge.

c. **Information Management (IM).** Managing and maintaining quality information is an important military task. Good IM makes accomplishment of other tasks less complex. Automation and standardization of communications processes and procedures improve IM and aid the commander's effectiveness and speed of C2. Improved technology in mobility, weapons, sensors, and communications continues to reduce reaction time, increase the operating tempo, and produce large amounts of information. Unmanaged information

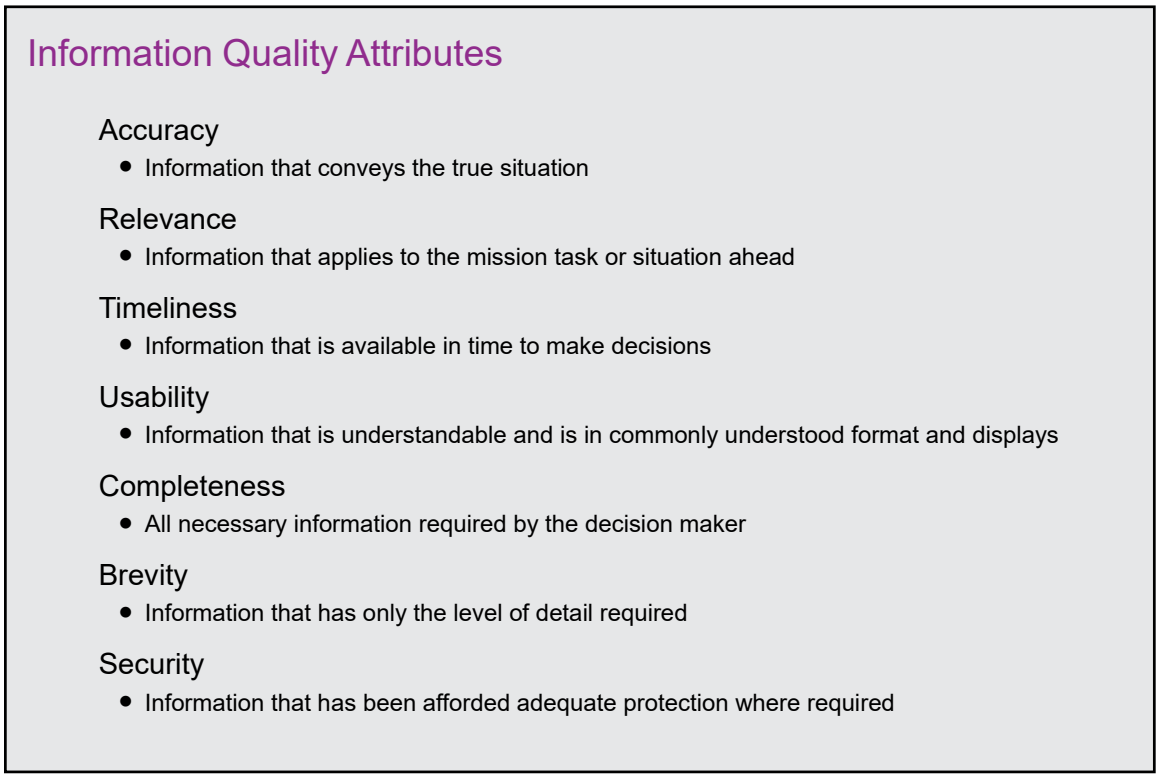


Figure I-1. Information Quality Attributes

degrades the commander's decision making and, possibly, joint force operation. The joint communications system must complement human skills and reduce or remove anticipated or known limits to mission accomplishment. A well-crafted and coordinated set of integrated procedures and interoperable systems is important to operating in a joint, multinational, and interagency environment of current and future operations. The communications system must be of sufficient scale, capacity, reach, reliability, resilience, survivability, and robustness to support evolving operational and training missions. Additionally, the communications system should integrate new technologies to facilitate delivery of the right information to the right location at the right time in an actionable format for the intended user.

d. The IM plan prescribes exactly "what" information is needed, while the communications plan focuses on "how" the information needs are to be fulfilled. Coordination of the IM and communications plans ensures all relevant C2 systems supporting the mission are identified, and adequate planning is performed to ensure provisioning of their service.

For a more detailed discussion on IM, see Joint Publication (JP) 3-33, Joint Task Force Headquarters.

e. Records management (RM) is the practice of maintaining records, including categorizing, storing, securing, destruction, or archival preservation. The goal of RM is to protect valuable historical archives and ensure permanent records are accessible and readable for years to come. Documents are paper or electronic files (e.g., e-mail, contracts,

memos, charters, standard operating procedures) containing data/information. Records are types of documents that are final, detail a specific outcome or decision needing to be retained for continuity and historical purposes, and are not meant to be altered.

For a more information on record management, see Department of Defense Instruction (DODI) 5015.02, DOD Records Management Program.

3. The Role of the Communications System

a. The JFC requires a secure, robust, and reliable communications system to assimilate information, effectively communicate and exercise authority, and direct forces over large geographic areas and a wide range of conditions. A communications system that provides connectivity throughout the operational area from the strategic to tactical levels is vital to plan, conduct, and sustain operations, and enable information superiority. The JFC must maintain communications with higher, supported, supporting, and subordinate commands during all phases of an operation and in all types of operational environments. Operations at all levels routinely require long-range, mobile communications. Commanders must consider en route, intratheater, and intertheater communications. In addition, the JFC's communications system must be capable of interfacing with mission partner communications systems. This same standard and rigor of communications must be maintained throughout the supporting and subordinate commands. This requirement supports information security as well as a positive information flow.

b. The communications system is the JFC's principal tool to collect, process, store, disseminate, and manage information. Given the criticality of information, the security of the communications system is paramount to ensuring the commander can trust the information provided and received. Effective C2, through the exchange of information, integrates joint force components and enables them to function effectively across vast distances, in austere or complex environments, and in all weather conditions. The joint force's mission and structure drive specific information flow and processing requirements, and the joint force's location and information requirements drive the configuration and capabilities of the communications system. The objective is to rapidly achieve secure information sharing to facilitate a common understanding of the current situation throughout the operational environment.

c. Processes and procedures help ensure information availability and access across the operational environment and facilitate:

(1) **Joint and Multinational Operations and Interagency Coordination.** The communications system facilitates joint and multinational operations and interagency coordination by providing the means to share operational area visualization; manage information; and facilitate collaborative planning, rehearsal, execution, and assessment with mission partners.

(2) **Strategic Agility.** The communications system supports the rapid deployment and employment of task-organized forces anywhere in the world. Rapid information sharing around the globe permits simultaneous, interactive planning from widely dispersed locations, thereby enabling remote staffs to develop and coordinate an operation plan (OPLAN) and execute an operation order (OPORD). Strategic agility provides JFCs the ability to reachback to data repositories, thereby increasing deployability, reducing footprint, and enhancing access to global intelligence assets. The communications system supports collaboration that assists JFCs in conducting detailed, concurrent, and parallel planning.

(3) **Tactical Flexibility.** The communications system enables the joint force to enhance SA and timely decision making to rapidly and positively identify and engage targets and to develop and conduct a wide range of military operations. The communications system supports the development and dissemination of the commander's intent and planning guidance, fostering decentralized execution. Timely delivery of information concerning targets, movement of forces, condition of equipment, levels of supplies, and disposition of assets—both friendly and threat—to the joint force enables more effective decentralized execution.

(4) **Network-Enabled Operations**

(a) The joint communications system enables the interconnection (networking) of geographically separated forces, which permits network-enabled operations. Network-enabled operations are military operations that exploit information and networking technology to integrate dispersed human decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system. Network-enabled operations exploit the combat power derived from the networking of well-informed, geographically dispersed forces. A securely networked force can increase operational visibility and combat power, achieving greater speed of command decisions and increasing the lethality, survivability, and responsiveness of the force.

(b) Network connectivity is mission-critical and can determine mission viability during planning and execution. The loss of network connectivity can put the force at risk, threatening lethality and survivability. The inseparable link between tactical communications, force capability, and C2 should be continually addressed during planning and execution to mitigate the adverse impact of unforeseen consequences. Since a significant portion of any communications system relies upon wireless transmissions, access to the electromagnetic spectrum (EMS) must be a consideration when planning network connectivity. Today, all joint force operations depend on assured EMS access throughout the operational environment. The joint force's growing dependence on the EMS is a critical vulnerability that our enemies will seek to exploit. The joint force's ability to achieve EMS superiority is a key to success throughout the operational environment and the electromagnetic operational environment (EMOE).

For more information on EMS operations, see JP 6-01, Joint Electromagnetic Spectrum Management Operations.

(c) For existing electronic information systems and information technology (IT) services, records will be managed electronically, manually, or a combination of both.

(5) **Information Superiority**

(a) Information superiority is the operational advantage derived from the ability to collect, process, and disseminate a trusted and uninterrupted flow of information, while exploiting, manipulating, or denying an adversary's ability to do the same. The joint communications system must promote information superiority.

(b) Information superiority is a priority before hostilities begin. This requires DOD to develop policies; doctrine; tactics, techniques, and procedures (TTP); organizational relationships; and technologies to win the information fight. The quality of information depends upon the accuracy, relevance, timeliness, usability, brevity, security, and completeness of information from all sources. A priority responsibility of command is to ensure access to relevant information sources within and among all DOD and non-DOD organizations from strategic to tactical levels of military operations and in multinational operations with mission partners. The continuous sharing of relevant information from a variety of sources facilitates the fully networked joint force's achievement of shared SA among DOD components, all levels of the USG, multinational partners, and, when authorized, the private sector.

d. **EMS Operations**

(1) Information and data exchange will ultimately rely on the EMS for dissemination. The EMOE is congested by friendly and neutral emitters and contested by enemy operations. The EMOE consists of the background electromagnetic environment and the friendly, neutral, and adversarial electromagnetic order of battle within the electromagnetic area of influence of a given operational area. The joint force must execute joint electromagnetic spectrum operations (JEMSO). JEMSO are military actions undertaken by two or more Services operating in concert to exploit, attack, protect, and manage the EMOE. These actions include/impact all joint force transmissions and receptions of electromagnetic energy. JEMSO is employed in an offensive and defensive manner to achieve unity of effort and support of the commander's objectives.

(2) Statutory requirements and the variety of USG departments and agencies present within the homeland make domestic EMS operations very different than EMS operations conducted in support of operations overseas. Defense support of civil authorities mandates coordination with local and state-level authorities.

4. Communications System Principles

a. The joint force capitalizes on information and near simultaneous dissemination to turn information into actions. An effective communications system helps the JFC conduct distributed operations. Joint force employment decisions are influenced by the communications system's ability to network the force. This inseparably links network

control to C2 prioritization and decisions. The communications system must be interoperable, agile, trusted, and shared to provide the flexibility to dynamically meet mission objectives (see Figure I-2). Networked joint forces increase operational effectiveness by enabling dispersed forces to more efficiently communicate, maneuver, populate, access, and share a common operational picture and attain the desired end state at all levels of command.

b. Detailed communications system techniques and procedures necessary to deploy and sustain a joint force are contained in the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6231.01, *Manual for Employing Joint Tactical Communications,* and annex K (Command, Control, Communications, and Computer Systems) of the JFC's OPLANs, OPORDs, or campaign plans.

c. The DODIN is a global enterprise enabling all combatant command (CCMD) missions, Service core functions, and combat support agency activities. Commander, United States Cyber Command (CDRUSCYBERCOM), is the supported commander for global DODIN operations and DCO-IDM, including those operations that span multiple CCMDs. Combatant commanders (CCDRs) are supported for DODIN operations and DCO-IDM conducted in support of their requirements. The CCDRs establish regional priorities for mission assurance, which will drive prioritization of DODIN operations and DCO-IDM. CO will be deconflicted through the synchronization of United Sates Cyber Command (USCYBERCOM) and CCMD operational processes.

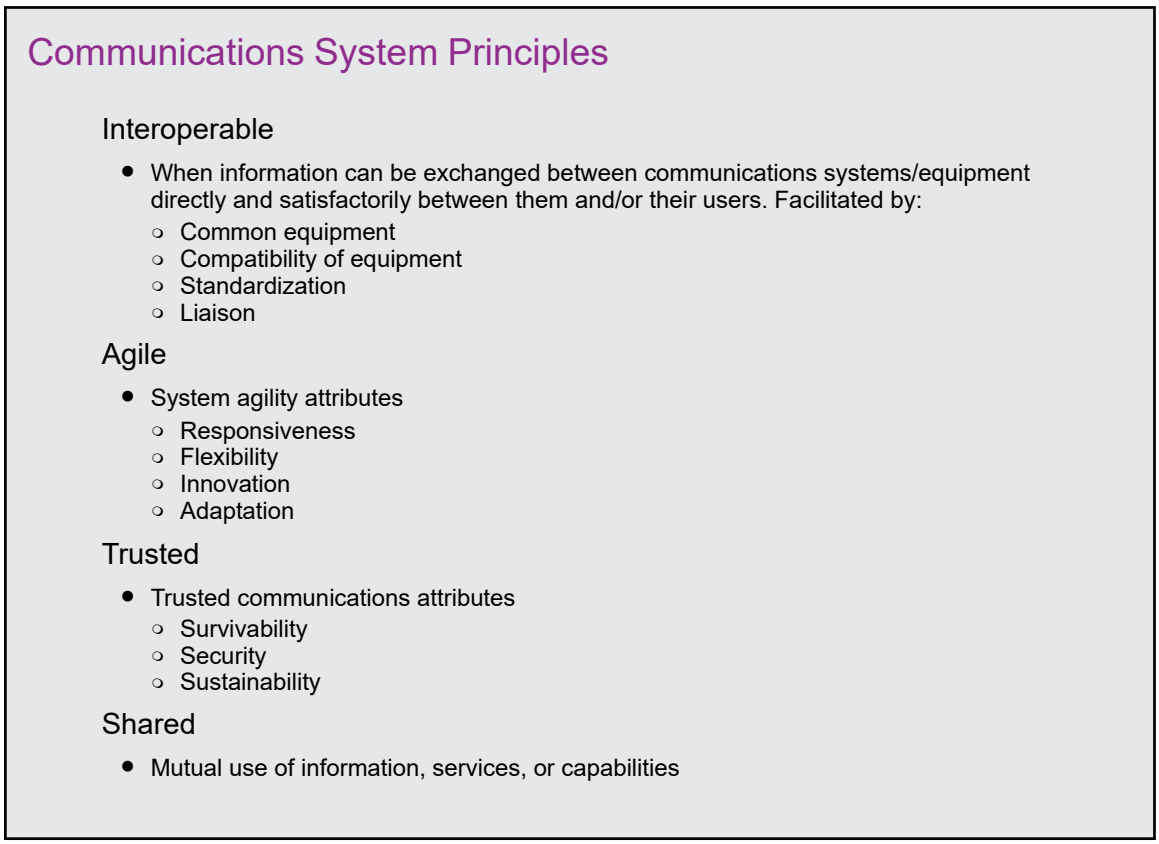


Figure I-2. Communications System Principles

5. Communications System Functions

a. The communications system supporting US military forces must anticipate and adapt to changing demands and provide information that meets all information quality attributes. By meeting these fundamental objectives, the communications system enables joint forces to seize opportunities and meet mission objectives. The communications system facilitates information sharing and decision support and is an essential building block in the operational environment.

b. Information system components that make up the joint communications system facilitate the capabilities to collect, process, store, disseminate, and manage information (see Figure I-3).

6. Essential Services

a. The Joint Chiefs of Staff (JCS) validate essential services required to support the JFC and joint operations. These services must be available across the range of military operations and under all operational circumstances, to include degraded cyberspace; disconnected, intermittent, limited-bandwidth users; and a nuclear-based electromagnetic pulse.

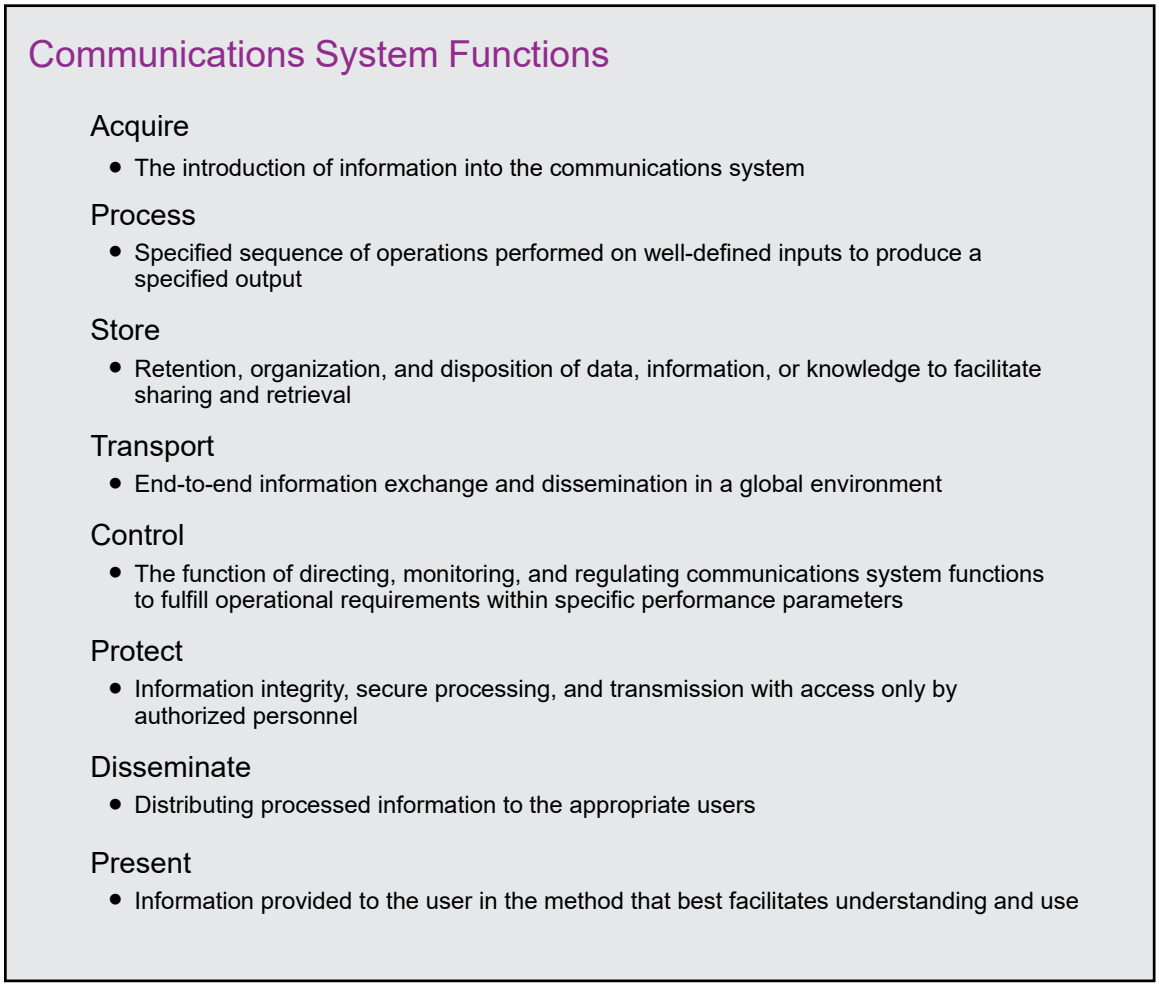


Figure I-3. Communications System Functions

b. The following IT services form the minimum capabilities required by the JFC:

(1) Voice services, to include assured and non-assured voice.

(2) Video services, to include video conferencing.

(3) Collaborations services, to include messaging, presence, multi-user chat, and web conferencing.

(4) Common operational picture services, to include global picture and a common tactical picture.

(5) Joint planning, execution, and assessment services.

(6) Intelligence services.

(7) C2 system services.

(8) Web-based access to mission services.

(9) Cross-domain information sharing services.

(10) Control of IT services.

(11) Communications interoperability with allies and other mission partners.

c. The services listed above must be available to the JFC on any end-user interface or device in the operational area. Service delivery must conform to the operational context of the JFC and the available end-user interfaces.

d. The services listed are those that directly support the JFC, but there are a number of support services the JFC must provide as well, including network management, communications management, and communications support.

e. All end-user services must meet the requirements of the JFC in the operational context, and any metrics for service delivery must be based on operational requirements.

Intentionally Blank

CHAPTER II
THE INFORMATION ENVIRONMENT

"Advances in information technology have significantly changed the generation of, transmission of, reception of, and reaction to information. These advances have increased the speed and range of information, diffused power over information, and shifted socio-cultural norms. The interplay between these advances provides our competitors and adversaries additional ways to offset the diminishing physical overmatch of the world's preeminent warfighting force."

Joint Concept for Operating in the Information Environment (JCOIE),
July 2018

1. General

a. The information environment continues to evolve and adapt. The information environment, as part of the operational environment, is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This publication primarily addresses the DOD systems portion of the information environment. These systems are the DODIN and all individuals and organizations that secure, operate, and defend the DODIN.

b. The joint information environment framework is a set of mandatory standards, protocols, and principles that provides a secure and reliable shared IT infrastructure, enterprise services and a single security architecture to achieve information superiority, improve mission effectiveness, increase security, and improve IT efficiency. This framework enables DOD to acquire, operate, secure, and maintain IT capabilities to improve information sharing and better address cybersecurity.

2. Cyberspace and Cyberspace Operations

a. **Cyberspace.** Cyberspace is a global domain within the information environment consisting of the interdependent networks of IT infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Digital communications systems are a subset of cyberspace; virtually all DOD operations and administration rely on a secure and stable cyberspace.

b. **CO.** CO are the employment of cyberspace capabilities where the primary purpose is to achieve JFC objectives in or through cyberspace. Although most of these actions are simply cyberspace-enabled activities, cyberspace forces conduct the CO missions using digital communications systems and other cyberspace capabilities. Specifically, the DODIN operations and DCO-IDM missions protect these digital communication systems and, when directed, other portions of blue cyberspace.

(1) DODIN operations missions secure, configure, operate, extend, maintain, and sustain DOD cyberspace to create and preserve the confidentiality, availability, and

integrity of the DODIN. These missions are informed by threat intelligence but are focused on addressing vulnerabilities before they are exploited by cyberspace threats.

(a) Cyberspace security actions are the tactical actions taken in the context of the DODIN operations mission to reduce vulnerabilities. Cyberspace security actions occur within protected systems to prevent any unauthorized activity, including access, escalation of privileges, exfiltration of data, and creation of denial effects. Cyberspace security measures include any action that results in a more secure system, including user training, penetration testing, and threat emulation.

(b) Conduct of Cyberspace Security. Service-retained cyberspace forces, CCMD cyberspace forces, Reserve Component, and DOD agency and activity staffs take most of the actions required to secure the various backbones, sub-nets, segments, enclaves, and private networks of the DODIN. These staffs include cybersecurity service providers (CSSPs) and network operations and security centers (NOSCs) established by the Services and DOD agencies to provide DODIN protection services under support agreements with system owners.

(2) DCO. DCO missions focus on defeating specific threats that compromise the security, or threaten to compromise the security, of the digital communications systems. DCO-IDM missions, informed by intelligence, occur within protected system or network to identify and remove the threat, using established TTP.

(a) Cyberspace Defense Actions. DCO-IDM missions are executed using a series of cyberspace defense actions to defeat specific threats that breach or threaten to breach established cyberspace security measures. These actions include threat hunting, detection, characterization, countering, and mitigation. Tactics can include isolating, rerouting, reconstituting, and restoring activities.

(b) Conduct of Cyberspace Defense. Regardless of the personnel or DODIN segments involved, when personnel with DODIN security responsibilities detect compromise of cyberspace security measures, they transition, in accordance with (IAW) standing authorities, to the cyberspace defense actions to restore security to the affected portion of the DODIN. The defense of the DODIN is segregated into multiple layers:

1. Organic Defenses. These include the network infrastructure, personnel, and cyberspace defense capabilities resident within a CCMD, Service, agency, or field activity, including administrators assigned to DODIN segments. Cyberspace defense actions at this level include threat detection and system emergency patching, reconfiguration in response to the face of a specific active threat, and monitoring of system logs and other internal threat indicators.

2. Dedicated Defenses. These include network infrastructure and computer systems designed to perform dedicated cyberspace defense actions, such as intrusion detection sensors, gateway security stacks, and other boundary defenses.

3. Enterprise Defenders. Personnel that perform cyberspace defense actions at the NOSCs and CSSPs and other similar enterprise-level positions.

4. Cyber Protection Force (CPF). The CPF includes various types of cyberspace protection teams (CPTs) organized, trained, and equipped to defend assigned portions of cyberspace in coordination with and in support of segment owners, CSSPs, NOSCs, and users. CPTs work closely with intelligence and malware analysts to fully prepare to face current cyberspace threats. They hunt inside blue cyberspace for suspected or hidden threat activity.

For additional information on CO, see JP 3-12, Cyberspace Operations.

3. Department of Defense Information Network Operations Construct

a. The DODIN supports DOD missions and functions and is central to joint and multinational operations. Joint operations span global and regional campaigns, including military engagements, security cooperation, deterrence activities, crisis response, limited contingency operations, and large-scale combat operations. Joint operations, which vary in scope, purpose, and conflict intensity, require portable, universally accessible technologies to realize C2 and further enhance mission effectiveness. The DODIN supports all military operations by enabling US mission partners to securely and seamlessly share required information. However, multinational information sharing seams and challenges exist, requiring extensive manual cross-domain [network] transfers as information is shifted out of one controlled security domain [network] and injected manually into another.

b. Adopting common TTP and shared capabilities improves operational effectiveness, simplifies the OPORDs process, helps to standardize "train and equip" requirements across the DOD components, enhances and hardens security across the DODIN, and enables components to allocate and align existing resources to better support priorities.

c. Military operations require an agile information network to achieve an advantage for DOD personnel and mission partners. Personnel in DOD must be able to access the information required to perform their assigned functions from the point of need, consistent with security and required access restrictions to achieve information advantage. Users must have timely access to the information and resources they require, anywhere and anytime, enabling them to maintain SA and make informed decisions. The primary threats come from enemy and adversary CO and will most likely be targeted against the unclassified portion of the DODIN.

4. The Tactical Level

Communications for tactical forces are not standardized. In addition to the vast number of state and non-state actors in the operational area, the sheer quantity and diversity of systems—exacerbated by the plethora of TTP; data, video, and voice formats; networks; and architectures employed—present a formidable challenge for successful tactical

information exchanges. Tactical information is information required, provided, or collected for use by tactical formations while in mission execution. The persistent need to communicate crucial and timely information to tactical units increases the potential for unintended and exploitative use of sensitive information by threat forces. The tactical network environment may be supported with joint communications nodes. A node is capable of connecting to the local information network through both DOD and non-DOD transport systems and is capable of providing a deployed force with networks and services at both the unclassified (e.g., Non-classified Internet Protocol Router Network [NIPRNET]) and classified (e.g., SECRET Internet Protocol Router Network [SIPRNET]) levels.

5. Network Operations, Network Management Cross Flows

Deployed networks within the DODIN require a framework to address the network management cross flows required to establish seamless transitions across systems to support information exchange between administrative, logistics, and tactical networks. As such, the need to delineate network management roles and responsibilities is critical. At the tactical level, the joint force typically requires information exchanges to occur for short durations. The movement of forces may require exchanges in hours/days with administrative networks that require continuous availability. Each system needs tailored network management systems, lines of control, and authority requirements to meet operational needs.

6. Operations in Degraded and Denied Environments

a. Enemies and adversaries contest the use of the information environment as a means of denying operational access and diminishing the capability of the US and multinational forces. The ability to command, control, and communicate with globally deployed forces is a key enabler for protection of US national interests and, as such, is also a key enemy target. Adversaries operate in a gray zone, conducting actions short of war such as misleading or inaccurate information activities and cyberspace attacks to offset US technological advantages. Enemies often adopt strategies that take advantage of a range of capabilities to deny friendly forces a conventional force-on-force fight. Enemies are pursuing technologies to challenge our freedom of maneuver and our ability to operate in the EMS/information environment. The cost of entry is low, and the global proliferation of technology means that the individual now has access to capabilities once reserved for global powers. These extensive adversarial investments in electronic warfare and space control pose potential threats to US operations.

b. The growth of anti-access and area denial capabilities around the globe, the changing US overseas defense posture, the emergence of more contested space and cyberspace, and the increasingly constrained EMS availability for global operations may alter the advantages that the US has enjoyed over the past decades. Enemies and adversaries will see the adoption of these capabilities against the US as a favorable course of action (COA) for them. Those able to field layered and fully integrated anti-access and area denial capabilities will attempt to deny US operational access altogether, while others

with less robust and comprehensive capabilities may simply attempt to inflict greater losses than they perceive the US will tolerate politically.

c. Enemies and adversaries will deliberately attempt to deny friendly use of the EMS. Technological advances including artificial intelligence, the Internet, cloud computing, and increasing cybersecurity threats create an increasingly complex information environment. Due to heavy reliance on the communications system, 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 C2 systems and planning for operations in a denied or degraded environment. Therefore, mitigation techniques to contend with a loss of bandwidth; connectivity; and position, navigation, and timing must be addressed during joint planning.

d. Degraded operations may be the result of hostile actions but can also be due to the lack of sufficient resources to allocate to all areas where needed. They can also be the result of the lack of coverage in an operational area or a result of electromagnetic interference (EMI). Implementing JEMSO driven by electromagnetic battle management will facilitate integration, deconfliction, and execution of EMS operations.

e. The DODIN supports continued operations in degraded and denied environments. Operations relying on the DODIN and operations of the DODIN itself must continue even in times of crisis. Therefore, continuity of operations, disaster recovery, and distributed control may minimize the impacts of isolated disruptions within the DODIN. Failures within the DODIN should be transparent to the end users, relying on systems and capabilities that automatically and immediately transfer to designated alternate capabilities enabling operations to continue uninterrupted.

f. A joint satellite communications (SATCOM) integrated operations environment can improve SA and provide more efficient coordinated creation of effects in space and cyberspace in support of the joint warfighter.

7. Roles and Responsibilities

a. The achievement of information superiority requires unity of effort to manage, secure, operate, and defend the DODIN. As a practical matter, unity of effort is necessary due to the vast number of IT resources required to support worldwide DODIN operations. The provisioning of DODIN enterprise services includes all CCDRs' missions, DOD agencies, and all DOD users from anywhere in the world. The DODIN supports DOD users who are deployed or operating away from their home base. The DODIN IT infrastructure, information services, data, policies, standards, and procedures must support the operational forces in all of their assigned missions. The DODIN must be flexible and tailorable to accommodate changes required by the various CCDR missions. The DODIN must also be capable of supporting operations at all levels of warfare from strategic to tactical operations. To enable the DODIN to adequately support the operational commanders, proper coordination of network assets ensures all CCDRs receive a similar level of service and effectiveness.

b. CDRUSCYBERCOM directs DODIN security, operations, and defense. CCDRs, Services, and DOD agencies will coordinate with USCYBERCOM to ensure global impacts to the DODIN are properly considered. USCYBERCOM also prepares and, when directed, enables actions throughout the operational environment, permits freedom of action in cyberspace, and denies the same to our adversaries.

(1) **Office of the Secretary of Defense**

(a) **DOD Chief Information Officer (CIO)**

1. The DOD CIO is the principal staff assistant and senior advisor to the Secretary of Defense (SecDef) for IT (including national security systems and defense business systems), information resources management, and efficiencies. The DOD CIO is the DODIN architect and develops, maintains, and enforces compliance with the DODIN architecture. The DOD CIO also consults with comparable intelligence community (IC) authorities on matters of policy, implementation, and operation. The DOD CIO enforces standards for interoperability, cybersecurity policy, data sharing, use of enterprise services, and DODIN program synchronization.

2. The **DOD CIO Executive Board** is the single senior governance forum for DOD IT and the principal forum used to advise the DOD CIO on the full range of matters (including statutory and regulatory) pertaining to the DODIN. Chaired by the DOD CIO, the board is composed of CIOs and/or senior communicators from the Services, the Joint Staff, the IC, USCYBERCOM, Cost Assessment and Program Evaluation, and the five Undersecretaries of Defense.

(b) The **Undersecretary of Defense for Policy** serves as the lead within DOD to develop, coordinate, and monitor implementation of overarching DOD policy related to cyberspace and provides policy oversight of the programs and activities of USCYBERCOM.

(c) The **Undersecretary of Defense for Intelligence** serves as the principal staff assistant to SecDef in developing information security policy and guidance. Concerning joint communications, the Undersecretary of Defense for Intelligence advises and assists the DOD CIO on acquisition programs that significantly affect intelligence, counterintelligence, and security capabilities.

(2) **Chairman of the Joint Chiefs of Staff (CJCS)**

(a) Unless otherwise directed, communications between the President and SecDef and the CCDRs are transmitted through the CJCS. The CJCS exercises operational oversight over those portions of the DODIN utilized for such communications.

(b) The CJCS operates the National Military Command System (NMCS) for SecDef to meet the needs of the President, SecDef, and the JCS. The CJCS establishes

operational policies and procedures for all components of the NMCS and ensures their implementation.

(c) The CJCS also promulgates instructions and other guidance with regard to joint doctrine. These instructions include criteria and standards for assessing and reporting readiness of DODIN assets.

(d) The Joint Staff J-6 [Director Command, Control, Communications, and Computers/Cyber] provides advice and recommendations about the communications system and cyberspace matters to the CJCS and serves as the Joint Staff CIO. As chairman of the Military Command, Control, Communications, and Computers Executive Board (MC4EB), the Director, Joint Staff J-6, coordinates and resolves DODIN issues among the Services and member agencies. The MC4EB is the CJCS's principal military advisory forum for assessing the IT aspects of communications matters to support the joint force. The MC4EB coordinates among DOD components, between DOD and other USG departments and agencies, and between DOD and representatives of foreign nations. This coordination includes operational communications guidance and direction to the CCDRs, Services, and DOD agencies. The MC4EB utilizes panels, which are functionally oriented bodies with expertise usually in one specific area, to research and prepare issues for discussion and/or resolution. IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3265.01, *Command and Control Governance and Management,* the Joint Staff J-6 provides capability sponsorship and technical and programmatic oversight of the joint C2 family of programs, to include the Global Command and Control System (GCCS) family of systems and the Global Combat Support System-Joint (GCSS-J) to facilitate effective communications system operations.

(e) The **Combined Communications-Electronics Board (CCEB)** is a five-nation combined military communications organization whose mission is the coordination of any military communications system matter that is referred to it by a member nation. The member nations of the CCEB are Australia, Canada, New Zealand, the United Kingdom, and the US. The CCEB consists of a senior communications system representative from each of the member nations. The US representative for the CCEB is the Joint Staff J-6, who also chairs the MC4EB. The CCEB defines an environment that optimizes information sharing and overcomes the disadvantages of transient multinational force organizations. The CCEB seeks to achieve interoperability not just with technical standards and common procedures but also by spanning technologies and systems. The CCEB develops and seeks agreement on policies, procedures, and standards, including Allied communications publications (ACPs), which enable the exchange of information during multinational operations.

(f) The Joint Staff J-32 [Deputy Directorate for Intelligence, Surveillance, and Reconnaissance Operations] identifies processing, exploitation, and dissemination shortfalls in associated communications architecture.

(3) **CCDRs**

(a) Geographic combatant commanders (GCCs) oversee and coordinate DODIN planning and employment within their areas of responsibility (AORs). They exercise authority over DODIN assets assigned to their commands. Through their CO planning staff, they utilize the USCYBERCOM cyberspace operations-integrated planning element (CO-IPE), the Defense Information Systems Agency (DISA), and Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) operations center, as well as Service component command DODIN operations centers as appropriate. To this end, they collaborate with their respective Service components, DISA, Defense Intelligence Agency (DIA), JFHQ-DODIN, and USCYBERCOM to create and maintain SA over theater and global networks.

(b) CCDRs report on the readiness of assigned DODIN resources as a part of the CJCS's Readiness Reporting System consisting of the joint force reporting review, CCMD assessments, and plan assessments. The joint combat capabilities assessment provides the President, through SecDef and the CJCS, a current assessment of the military's ability to execute its assigned mission in support of the national military strategy. The joint combat capabilities assessment assesses all functional areas, including communications system theater and strategic DODIN infrastructure shortfalls and limitations affecting the communications system.

For more information, see CJCSI 3401.01, Joint Combat Capability Assessment.

(c) CCDRs are the operational sponsors of the joint communications system. Through a joint information environment framework, global standardization greatly enhances access to the right information, by the right users, at the right time and place. CCDRs can tailor information systems using a DODIN operations framework based on assigned forces and assigned missions. Thus, within each CCMD, this framework is commander-centric based on commander-approved DODIN operational requirements. The DODIN operations framework is a flexible construct that adapts to the commander's operational requirements.

1. **Global and regional campaigns.** The CCDR's network consists of the system infrastructure, much of which is globally connected. Day-to-day operations are characterized by well-secured networks that are prepared to support CCDR's campaign and contingency plans.

2. **Response operations (flexible response options/flexible deterrent options).** The network may transition into a more decentralized capability; the CCDR postures network capabilities and authority for eventual delegation to one or more JFCs, if required.

3. **Contingency execution.** The CCDR begins decentralization/transition of network capability/authority to subordinate commanders, based on the nature and requirements of the contingency.

4. **Transitions to global/regional campaign conditions.** Commanders initiate the transition of network capabilities/authority back to a global/theater-based enterprise.

(d) CCDRs identify, categorize (in terms of mission criticality), and assess risks to their mission-critical assets (including information assets) via annex C (Operations), appendix 15 (Critical Asset Risk Management) of their OPLANs.

(e) CCDRs validate appendix 16 (Cyberspace Operations) to annex C (Operations) and annex K (Command, Control, Communications, and Computer Systems) portions of their appropriate OPLANs periodically as a part of CJCS-sponsored or command-sponsored exercises. These exercises will identify unresolved issues, verify operational procedures and interoperability, and provide joint training.

(f) GCCs identify their multinational interoperability requirements in the GCC's campaign plan. These requirements should be tested periodically as part of multinational exercises to identify unresolved issues, verify operational procedures and interoperability, and provide multinational training.

(g) GCCs identify mission partner coordination and communications system requirements. The operational area may have a large number of USG departments and agencies, international organizations, and NGOs. Communications support, where needed, should be consistent with US law, regulations, and doctrine. CCMD staffs should coordinate as necessary to promote unified action.

(h) CCDRs execute JEMSO to achieve EMS superiority, which enables DODIN capabilities to operate as they are intended. JEMSO integrates joint EMS management (i.e., frequency management and joint spectrum interference resolution), electronic warfare, and intelligence, as well as HN coordination executed by a CCMD's joint frequency management office to achieve unity of effort within the EMS.

For more information on JEMSO, see JP 3-13.1, Electronic Warfare, *and JP 6-01,* Joint Electromagnetic Spectrum Management Operations.

(i) **Theater IM Cell.** The theater IM cell is a full-time function collocated within the CCDR's joint operations center (JOC). The theater IM cell members combine the guidance published in the commander's dissemination policy with operational information, intelligence, and network architecture/communications status information. The theater IM cell works closely with the theater network operations control center (TNCC) to coordinate potential changes in either the Global Broadcast Service schedule or Defense Information Systems Network (DISN) changes to fulfill updates in the commander's information dissemination requirements.

(j) CCDRs synchronize and validate DODIN operations-specific language in annex K (Command, Control, Communications, and Computer Systems) with appendix 16 (Cyberspace Operations) to annex C (Operations). Planning and execution of DODIN

operations should be tested periodically as part of CJCS- or command-sponsored exercises to identify operational procedures, coordinate with USCYBERCOM and other DOD and non-DOD mission partners, and provide joint training.

(4) **Military Departments and Services.** IAW guidelines and direction from SecDef, each Military Department or Service, as appropriate, has the following common functions and responsibilities pertaining to joint operations:

(a) 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.

(b) As DODIN providers and managers, extend DODIN common services, to include voice, data, and video, to their organizations within the sustaining base.

(c) Ensure Service-managed portions of the DODIN are secure, assured, and interoperable and all personnel are appropriately trained.

(d) Provide spectrum engineering and management within their respective Military Departments to optimize the use of the EMS. Operation of EMS-dependent equipment will be in compliance with HN and international EMS management and support agreements and approved allocations.

(5) **CDRUSCYBERCOM**

(a) USCYBERCOM secures, operates, and defends the DODIN as part of its overall responsibility for CO. USCYBERCOM executes the DOD missions of DODIN operations, OCO, and DCO. USCYBERCOM advocates for national requirements and standards and, in coordination with other CCDRs, assesses the operational readiness of the DODIN.

(b) As military lead for security, operation, and defense of the DODIN, USCYBERCOM conducts cyberspace incident reporting and develops coordinated response actions for the synchronized protection of DOD cyberspace. These include defensive actions to defeat unauthorized activity through coordinated release and distribution of orders and directives.

(c) CDRUSCYBERCOM exercises directive authority for cyberspace operations (DACO) over all DOD components. DACO is vested in CDRUSCYBERCOM to issue orders to all DOD components for directing the execution of global DODIN operations and DCO-IDM to compel unity of effort to secure, operate, and defend the DODIN. CDRUSCYBERCOM may transfer or delegate DACO in total or in part for specific times and purposes, to ensure the timely and efficient security, operation, and defense of the DODIN. The ability of CDRUSCYBERCOM to exercise DACO does not restrict or limit the ability of DOD components to proactively strengthen the security of their networks and to take authorized defensive actions against ongoing or impending

exploitation or attacks. CDRUSCYBERCOM established the JFHQ-DODIN as the operational component primarily responsible for DODIN operations and DCO-IDM missions. As a part of these responsibilities, JFHQ-DODIN exercises DACO over all DOD components for operational and tactical planning, execution, and oversight, while enabling USCYBERCOM to focus on the operational and strategic levels of these missions. JFHQ-DODIN enables the effective C2 of DODIN operations and DCO-IDM and coordinates CCMD DODIN operations and DCO-IDM planning requirements through the USCYBERCOM CO-IPE.

(6) **Commander, United States Space Command (CDRUSSPACECOM)**

(a) CDRUSSPACECOM has space operations authorities and responsibilities that include SATCOM operations as a segment of the DODIN and positioning, navigation, and timing operations, which heavily supports the DODIN. CDRUSSPACECOM plans and conducts space operations and advocates for capabilities to meet CCMD, Service, and DOD agency operational requirements and strategic planning.

(b) Additionally, CDRUSSPACECOM develops, coordinates, and executes space operations, to include policies and procedures, apportionment plans, constellation deployment plans, satellite positioning and repositioning plans, and satellite scheduling deconfliction. CDRUSSPACECOM also assesses how these various plans impact communications support to current and future operations and coordinates action prior to execution.

For further information, see JP 3-14, Space Operations, *and CJCSI 6250.01,* Satellite Communications.

(7) **Joint Communications Support Element (JCSE).** On order, the JCSE immediately deploys to provide en route, early entry, scalable C2, communications, and computers to the GCCs, special operations commands, and other USG departments and agencies as directed. On order, the JCSE also provides additional services within 72 hours to support larger joint task force (JTF) and joint special operations task force headquarters (HQ). JSCE can globally deploy within hours of notification to provide communications packages tailored to the specific needs of a JTF, HQ, or a joint special operations task force.

(8) **JFC**

(a) The JFC ensures an adequate and effective communications system is available to support the C2 requirements of the assigned mission. The JFC exercises this responsibility through the communications system directorate of a joint staff (J-6).

(b) The J-6:

1. Publishes communications system plans, annexes, and operating instructions to support the assigned mission. In so doing, the J-6 (along with the CCDR's CO planning staff) coordinates with subordinate commands to provide communications

system assets required to support the JFC. This may include coordinating primary responsibility for communications with a subordinate or component command. The J-6 also coordinates lateral communications between subordinate commands.

2. Provides overall management of the communications system supporting the JFC. As the forces deploy, the J-6 establishes a joint network operations control center (JNCC) to establish network control and management within the operational area.

3. Reviews and coordinates communications system plans prepared by subordinate commands.

4. Provides for interoperability of the joint communications system.

5. Supports joint planning, coordination, and control of the EMS through the joint frequency management office.

(9) **DOD Agencies.** Similar to other DOD component responsibilities, DOD agencies develop and maintain their information system in a manner that is consistent with and reflective of the DODIN architecture. Agency-specific programs are to be planned, resourced, acquired, and implemented IAW defense resource priorities. Those DOD agencies, which are also part of the IC, are subject to the policies and guidance of the IC CIO.

(a) **DIA** engineers, develops, implements, and manages the Top Secret and sensitive compartmented information (SCI) portion of the DODIN, including the configuration of information, data, and communications standards for intelligence systems, in coordination with the Joint Staff, Services, other DOD agencies, and Office of the Secretary of Defense. Included within this is the overall operational management of the Joint Worldwide Intelligence Communications System (JWICS), a strategic, secure, high-capacity telecommunications network serving the IC with voice, data, and video services. DIA establishes defense-wide intelligence priorities for achieving interoperability between tactical, theater, and national intelligence-related systems and between intelligence-related systems and tactical, theater, and national elements of the DODIN. DIA exercises operational management of JWICS via the JWICS operations center.

(b) The **National Security Agency** develops and prescribes cryptographic standards and principles that are technically secure and sound; develops and provides executive management of DOD cryptographic hardware and software systems; and provides specialized support to the President, SecDef, and operating forces.

(c) The **National Geospatial-Intelligence Agency,** as the functional manager for geospatial intelligence, develops the architecture for the National System for Geospatial Intelligence (NSG). As the functional manager for NSG, the National Geospatial-Intelligence Agency actively communicates its architecture to members of the geospatial IC and promotes common standards and interoperability among NSG segments.

The NSG community consists of members of the IC, Military Departments, CCMDs, and elements of the civilian community. NSG partners include international entities, industry, academia, and DOD and civilian community services providers.

For more information on geospatial intelligence, see JP 2-03, Geospatial Intelligence in Joint Operations.

(d) **DISA:**

1. Provides, operates, and assures C2, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to the joint force, national-level leaders, and other partner nations.

2. Provides DOD transport services that are used for voice, data, and video services through a combination of terrestrial and satellite assets and services.

3. Provides enterprise-level development, integration, and management services for interagency, strategic, multinational, and joint C2 and combat support capabilities.

4. Works in conjunction with other DOD components to ensure the security of DOD enterprise systems and supports the CCDRs and deployed forces by designing and deploying proactive protections, deploying threat detection, and performing other necessary security functions.

5. Provides standards, interoperability testing, spectrum support and deconfliction, and integrated architecture development for DOD information systems.

6. Provides the DOD enterprise with a network-enabled service-based, shared enterprise infrastructure that supports ubiquitous user access to reliable capabilities and decision-quality information.

7. Provides enterprise-wide systems engineering support for the DODIN to ensure it is planned, acquired, operated, maintained, managed, and improved effectively and efficiently for end-to-end interoperability down to the tactical edge.

8. Provides tailored acquisition policies, processes, procedures, capabilities, lifecycle oversight, and a qualified workforce that acquires quality products and services to satisfy user needs and provide improvements to mission capabilities.

For more information on DISA responsibilities, see DODD 5105.19, Defense Information Systems Agency (DISA).

(e) **National Guard.** National Guard joint force headquarters-state (NG JFHQ-State) prepares their state communication plans in support of state active duty and Title 32, United States Code, missions. They submit their peacetime EMS requirements

through existing spectrum support channels. The Army National Guard submits through NG JFHQ-State to Army Frequency Management Office-Continental United States. During contingency operations, the NG JFHQ-State submits spectrum requests through the National Guard Bureau J-6 [Spectrum Management Branch], who will then forward the requests to the Army Frequency Management Office. Air National Guard units submit their peacetime and contingency operations spectrum requests through the Air National Guard A-6 [Spectrum Management Office], which then submits those requests to the Air Force Spectrum Management Office.

CHAPTER III
JOINT FORCE COMMUNICATION, SYSTEM OPERATIONS, PLANNING, AND MANAGEMENT

"Clearly, networking a force dramatically improves its capabilities for information sharing. This does not mean that all elements of the force are sharing information with each other all the time—but rather that all involved have the capability to share and access needed information. Sharing information is a prerequisite for a force to be able to develop shared situational awareness and to yield the warfighting benefits associated with enhanced collaboration and synchronization."

Network Centric Warfare Report to Congress, March 2001

1. Planning and Management Organizations

Communications system management involves the employment and technical control of the assigned communications system. Communications system management enables planners to maintain an accurate and detailed status of the network, all networked assets, and IT services. It combines centralized control with decentralized execution and provides effective and efficient communications system support for the JFC. Communications management policy and procedures are introduced in Chapter IV, "Information Sharing and Services."

a. **JNCC.** The J-6 responds to the JFC for all communications system issues required to accomplish the mission. The JNCC plans and manages the deployed communications system. The JNCC, through the components and Services, controls the joint communications networks under JFC authority and USCYBERCOM's DACO. Functional component commanders and subordinate JFCs may establish a NOSC to serve as their single point of contact for communications system issues.

b. **Service Component Management.** Service components and assigned support organizations should designate a single office within their communications staffs to coordinate with the joint force J-6. Service component communications support organizations should formulate and publish plans, orders, and internal operating instructions for the use of their communications systems. All components' technical control facilities perform network control and reconfiguration. For example, they change circuit paths, direct troubleshooting to resolve problems, and provide status information. Communications system management organizations need to account for traffic management in a packet-routed environment and execute circuit management functions.

c. **The joint information management board (JIMB)** serves as the JFC's principal organization to draft the commander's information dissemination policy and coordinates IM functions within the joint force. The IM officer chairs the JIMB for the chief of staff or other staff directorate. A JIMB should be convened during the initial development of the joint force IM plan and as required thereafter to manage information and operational data throughout the operation. The JIMB should be composed of representatives from each

staff section, component, and supporting agency and operates under the supervision of the chief of staff, or other appropriate staff directorate, as best meets the JFC's mission needs. The commander or a senior representative provides direct input into the JIMB by detailing the commander's view of the operational environment management and its impact on information flow and IM.

For more information on JIMB, see JP 3-33, Joint Task Force Headquarters.

2. Planning and Management Structure

a. **CCMD J-6.** The CCDR, through the CO planning staff and J-6, provides communications system guidance and priorities that support the commands and the components through the TNCC or the equivalent organization. The TNCC works closely with subordinate JNCCs to ensure accurate, timely, and detailed reporting by subordinate and supporting agencies and organizations. Additionally, the TNCC works closely with the CCDR's CO planning staff and the CO-IPE to support CO planning, DODIN operations, DCO-IDM, information dissemination management, and to share SA of CCDR's communications systems. The TNCC, in conjunction with the CCDR's CO planning staff, must also synchronize and coordinate the GCC's communication systems requirements. The TNCC is a supporting operations center to the GCCs' JOC and is responsible for AOR-wide SA of DODIN events and activities. It facilitates AOR-wide coordination of processes, such as authorized service interruptions and restorals; develops and conveys operational impact assessments of planned and unplanned DODIN operations and DCO-IDM activities and events; supports development of COAs; and ensures implementation of the supported CCDR's orders and direction. The CCMD J-6, in coordination with the CCDR's CO planning staff, identifies defense critical infrastructure DODIN assets IAW DODD 3020.40, *Mission Assurance (MA),* within the CCMD's AOR.

b. **Joint Force J-6**

(1) The J-6 provides the communications system to support reliable, timely information flow in support of unified action. The operational arm of the J-6 is the JNCC. To direct DODIN operations and retain SA, the JNCC requires timely support from each subordinate command's communications control center, the NOSC. Subordinate command and agency NOSCs assimilate and integrate DODIN operations SA data within their respective operational areas. Each NOSC installs, maintains, and operates network management and intrusion detection hardware and software and populates a local database to build a near real time view of their system.

(2) The J-6 assists the JFC in all communications system responsibilities. The J-6 establishes a JNCC to serve as the single control agency for the management and operational direction of the joint communications system. The JFC may task subordinate Service or component commanders to provide personnel augmentation to the J-6 to ensure the appropriate subject matter expertise exists within the JNCC. CCDRs and component commanders should task their J-6 communications staff to coordinate with the JFC's J-6.

(3) The J-6 assists the JFC with joint frequency management through the use of the Global Electromagnetic Spectrum Information System which provides spectrum management capabilities to further enhance the ease of use, efficiency, and effectiveness of spectrum management.

For more information on EMS management, see JP 6-01, Joint Electromagnetic Spectrum Management Operations.

(4) The joint electromagnetic spectrum operations cell (JEMSOC) is responsible for the administrative and technical management of the EMS. This includes maintaining a database of frequencies, in conjunction with the intelligence directorate of a joint staff (J-2) and operations directorate of a joint staff (J-3) of friendly, adversary, enemy, and neutral/civil emitters and receivers. The JEMSOC assigns frequencies, analyzes and evaluates potential conflicts, resolves internal conflicts, recommends alternatives, and participates in EMS use conflict resolution.

For more information on the joint restricted frequency list (JRFL) and frequency deconfliction procedures, refer to JP 3-13.1, Electronic Warfare.

c. **JNCC.** The J-6 establishes a JNCC to serve as the operations center for the deployed portion of the DODIN supporting a joint force. It manages the CCMD-assigned DODIN tactical communications, cyberspace security, and cyberspace defense resources deployed during operations and exercises. The JNCC, like the TNCC, is regionally focused on supporting the CCMD operations and is a subordinate contributing activity to the TNCC focused on DODIN operations, DCO-IDM, and information dissemination management. Network service centers belonging to deployed components and subordinate commands in the CCMD AOR are subordinate to and report through the JNCC. The JNCC:

(1) Exercises technical management over communications control centers belonging to deployed components and subordinate commands.

(2) Serves as the single control agency for management and operational direction of the joint communications networks and infrastructure.

(3) Performs planning, execution, technical, and management functions.

(4) Develops/disseminates standards/procedures and collects/presents communications system management statistical data. Functional components and subordinate JFCs should designate a single office within their communications staffs to coordinate with the JNCC.

(5) Provides network operations SA to the TNCC. Receives guidance from the TNCC and reports compliance and status to the TNCC.

d. **CCDR's CO Planning Staff:**

(1) Serves as the CCDR's staff for planning and oversight of CCMD DODIN operations, DCO, and OCO.

(2) Serves as the primary source for direction from the CCDR to aligned and supporting enterprise elements, to include the aligned USCYBERCOM joint force HQ-cyberspace, relevant operations centers, and CPTs.

(3) Should be integrated with the CCMD's cross-functional staff organization.

(4) Coordinates CO within the CCMD to integrate and synchronize CO with other military operations.

(5) Leverages direct support relationships with in-theater cyberspace forces, combat support agencies, and the USCYBERCOM CO-IPE to create CCMD-required effects in cyberspace in theater and to establish AOR cyberspace shared SA.

e. **Subordinate Communications Units**

(1) Subordinate communications units must ensure reliable, timely information flow to both the JFC and their own commanders. Service component communications system organizations should formulate and publish plans, orders, and internal operating instructions for the use of their communications systems.

(2) Normally, there will not be a conflict between support provided to the JFC's joint network and the respective subordinate commander's network. When there is conflict, a subordinate's NOSC must coordinate with the JNCC to prioritize its activity. Additionally, it is critical that each NOSC provide timely, accurate communications system SA to the JNCC. The NOSC can also coordinate with the JNCC to obtain technical and/or interoperability assistance.

3. Communications Planning and Management

a. **Systems Requirements.** The JFC's mission, C2 framework, and location of assigned forces determine the essential elements of the communications system employed. Specific command relationships and the organization of units and staffs drive the interconnecting communications methods and means. The communications system supports and provides an assured flow of information to and from commanders at all levels during all phases of an operation. The communications system must be disciplined, flexible, interoperable, responsive, mobile, survivable, secure, and sustainable to enable common awareness, speed decision making, and integrate actions of the joint force. It is critical in a fast-paced and highly technical environment that the communications system accommodate information exchanges at the tactical level.

b. **Planning and Operations.** Joint planning and operations are the development and implementation of campaign plans, contingency plans, and OPORDs prepared in response to requirements from the President, SecDef, or CJCS. They include a system of policies,

procedures, processes, and reporting structures—supported by communications and IT used by the joint planning and execution community to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities associated with joint forces. Joint planning provides for orderly and coordinated problem solving and decision making to address joint planning.

For additional information on joint planning and operations, see JP 5-0, Joint Planning, *and JP 3-0,* Joint Operations.

(1) The joint planning and execution community develops campaign plans for CCMD military engagement and security cooperation activities and contingency plans for a broad range of contingencies based on requirements identified in planning directives. The planning process is structured to support iterative, concurrent, and parallel planning throughout the planning community to produce thorough and fully coordinated contingency plans in noncrisis situations when time permits. Communications planners must understand the commander's concept of operations and intent and have a clear picture of the overall C2 structure.

(2) While planning for contingencies is based on hypothetical situations, planning in a crisis is based on circumstances that exist at the time planning occurs. Planning in a crisis responds to an incident or situation involving a threat that typically develops rapidly and creates a condition of such diplomatic, economic, or military importance that the President or SecDef considers a commitment of US military forces and resources to resolve the situation. Usually, the time available to plan responses to such real-time events is short. In as little as a few days, a feasible COA must be developed and approved and timely identification of resources accomplished to ready forces, schedule transportation, and prepare supplies for movement and employment of US military force.

c. Communications system planners ensure the organization's communications network can facilitate a rapid, unconstrained flow of information from its source through intermediate collection and processing nodes to its delivery to the user. Communications system planners should clearly understand the capabilities and limitations of all potentially available strategic, operational, and tactical communications systems and equipment, whether they are organic to Services, other CCDRs and agencies; belong to non-US forces; are commercial; or are provided by an HN. Typically, the combined system will provide voice, data, and video communications. Building the communications system to support the JFC requires knowledge of the joint force organization, the commander's concept of operations, available communications, and how they are employed. Additional consideration must also be given to the enemy's capability and intent to deny or disrupt communications.

d. The J-6 plans and establishes the communications system and the communications estimate of supportability (see Appendix B, "Joint Force Communications System Planning Guide") during COA development and selection during the planning process.

e. **Plans and Orders.** The J-6 provides input to orders and plans, publishes guidance, coordinates communications system support and services, and gains authorization of joint force networks. The role of the joint communications planner with the commander and mission partners is to provide continuous automated flow and processing of information during all phases of an operation. J-6 coordination within the staff and with mission partners is key and the earlier the better. At a minimum, the joint force J-6 maintains close and constant coordination with the supported CCMD J-6, JEMSOC, the TNCC, the CCDR's CO planning staff, the theater network operations center, CCMD joint frequency management office, CCMD communications security (COMSEC) manager, component operations centers, DISA liaison officer/field office, the JCSE point of contact, partner nations, and NGOs. The primary documents for publishing communications system guidance are appendix 16 (Cyberspace Operations) to annex C (Operations) and annex K (Command, Control, Communications, and Computer Systems) of the basic order. JP 3-33, *Joint Task Force Headquarters,* provides key planning checklists and information for the communications planner. After the communications system plan is developed and approved, the J-6 ensures all networks receive appropriate accreditation. The J-6 may be the authorizing official for theater communications system networks. The authorizing official will assign a security control assessor within each component. For all other DODIN networks, the J-6 must consolidate validated system risk management requirements and forward a consolidated network security authorization package to the next higher joint force J-6. IC networks will be authorized by the assigned IC authorizing official.

For more information on the accreditation process, see DODI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT), *and DODI 8330.01,* Interoperability of Information Technology (IT), Including National Security Systems (NSS).

f. **Communications Planning Considerations**

(1) **Identifying Key Terrain in Cyberspace.** Key terrain in cyberspace is similar to key terrain in the physical domains in that holding it provides a combatant a position of marked advantage. A unique characteristic of terrain in cyberspace is that these localities have a virtual component, which exists in the logical network layer of cyberspace. Planners correlate mission objectives in each plan with key terrain to ensure mission dependencies in cyberspace are identified and prioritized for protection. In many cases, the systems, networks, and telecommunication infrastructure that support a mission objective will be interdependent. These complex interdependencies may require in-depth analysis to develop customized risk mitigation methodologies. Identification of key terrain in cyberspace is a prerequisite for determining appropriate cyberspace security and cyberspace defense actions within a plan. All terrain in cyberspace supporting an objective, or plan, is collectively referred to as mission-relevant terrain in cyberspace. Each DOD component identifies key terrain that enables their missions, plans, and core functions.

For more information on key terrain in cyberspace, see JP 3-12, Cyberspace Operations.

(2) **Support to Intelligence.** The communications system planned by the J-6 is the primary means through which information and intelligence flows throughout the operational environment. Communications system planning must be conducted in close coordination with the J-2 to identify supportable data relay and dissemination resources. Support provided by the communications system does not typically cover the collection and production of intelligence. The IC has a number of systems that are not part of the DODIN. (See Chapter V, "Communications System Support to the President, Secretary of Defense, and the Intelligence Community.")

(3) **Interagency Partners, International Organizations, and Communications.** Of increasing importance to joint operations is effective connectivity to USG departments and agencies and international organizations. Presidential Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans,* directs DOD agencies and Services to share classified and unclassified information with interagency partners. In some situations, information sharing will also occur with multinational partners, international organizations, and NGOs. JFCs should identify interagency information exchange requirements (IERs) and coordinate connectivity/access as required. The National Guard Bureau can facilitate communications with state and local governments to support defense support of civil authorities operations through the National Guard Coordination Center and the NG JFHQ-State. Many of these users will require the use of nonsecure commercial communications, to include freeware applications and social media, to coordinate their operations. Such systems contain vulnerabilities that pose a risk to the DODIN. The JFC(s) may need to set up separate communications networks for these users outside the DODIN for boundary protection consisting of appropriate devices such as gateways, routers, firewalls, guards, or cross-network domain solutions.

(4) **Morale, Welfare, and Recreation Communications.** The J-6 may also plan for local cellular and wireless services, which can be for official use or authorized morale, welfare, and recreation purposes. Due to EMS considerations and security concerns, the J-6 should obtain a threat summary from the J-2 for threats to communications networks in theater. Wireless networks in particular must be closely managed due to security risks.

(5) **Military Auxiliary Radio System (MARS).** MARS provides DOD-sponsored emergency communications on a local, national, and international basis as an alternate communications capability for the Army and Air Force. The program consists of licensed amateur radio operators who are interested in military communications. MARS has provided morale, welfare, and official record and voice communications traffic for the Army and Air Force and authorized USG civilian personnel stationed throughout the world. The combined MARS programs are composed of a volunteer force of over 3,000 dedicated and skilled amateur radio operators. The MARS program:

(a) Provides DOD-sponsored emergency communications on a local, national, and international basis as an adjunct to normal communications.

(b) Provides auxiliary communications for military, civil, and/or disaster officials during periods of emergency.

(c) Assists in effecting normal communications under emergency conditions.

(d) Creates interest and furnishes a means of training members in military communications procedures.

(e) Provides a potential reserve of trained radio communications personnel.

(f) Handles morale and voice communications for the Army and the Air Force and authorized USG civilian personnel stationed throughout the world.

(6) **Support to Homeland Security and Defense Support of Civil Authorities.** The Department of Homeland Security (DHS) is the lead federal agency for homeland security. When requested by DHS and approved by SecDef, DOD supports DHS in providing homeland security. Similarly, DOD provides support to local, state, and federal authorities when a request for assistance has been received and approved by SecDef. DOD's involvement in homeland security and support of civil authorities may be impacted by such factors as competing use of allocated bandwidth (both civilian and military) and limited interoperability between communications systems. Interfaces that could be activated pursuant to SecDef authorization include military web portals accessible by nonmilitary domain servers; unclassified defense collaborative tool suites or similar commercial collaboration tools; JTF-owned deployable commercial voice switching; secure video teleconferencing (VTC) in each governor's office; radio cross-banding so land mobile radios, tactical satellite (TACSAT) radios, high-frequency radios, and cell phones can communicate with each other; links to national laboratories and other subject matter experts; and commercial Internet.

(a) Commanders and communications system planners should conduct the detailed planning and analysis necessary to determine US-based communications system requirements required to support federal, state, and local agencies in the event SecDef approves a request for support from DOD. For example, the JTF J-6 may need to rapidly gather information on the commercial communications infrastructure from the National Response Framework Emergency Support Function #2 (Communications) representative.

(b) The JTF J-6, as required and when authorized, must be prepared to bridge the potential communications gap between civilian, DOD, and other USG departments and agencies to develop mission-oriented communications solutions.

For more information on communications system planning for the homeland, see JP 3-27, Homeland Defense, *and JP 3-28,* Defense Support of Civil Authorities.

(7) **World Wide Web/Internet.** Communications planning and execution is dependent upon persistent access to cyberspace. As the world's population increasingly gets its information from the Internet, protected access to the World Wide Web is imperative for joint force communications, public affairs operations, and open-source

intelligence. This includes media and public perception analysis, global media SA, and the operation of Websites for informing critical, worldwide audiences.

(8) **Joint Network Communications Control.** Controlling networks is the science of solving communications problems by using logical and methodical procedures. Network architecture is normally aligned with the CCDR's multitiered C2 structure—the CCMD J-6, the joint force J-6, and the staff equivalents of the joint force components and subordinate commands. This relationship can be easily extended to the multinational command elements, their communications control centers, and communications capabilities when a multinational force is formed. DODIN operations are discussed in more detail in Chapter IV, "Information Sharing and Services."

(9) **SATCOM Planning and Management.** SATCOM provides users with satellite capabilities to meet current and future communications requirements. SATCOM capabilities are managed, monitored, controlled, and integrated with terrestrial capabilities to provide a comprehensive, seamless communications infrastructure. Communications planners must have visibility into SATCOM and related network resources for planning, implementing, monitoring, and sustaining communications support to forces within operational areas. SATCOM capabilities must have efficient and responsive methods for managing the complexities of multiple SATCOM payloads operating in many different frequency bands and network constraints or conditions while supporting diverse missions worldwide. SATCOM managers must also have insight into threats which would remove or negate those resources. SATCOM tasks and responsibilities include:

(a) **CJCS.** Adjudicates allocation conflicts that cannot be resolved through United States Space Command's (USSPACECOM's) arbitration process at the respective CCMD or DOD agency, or by USSPACECOM.

(b) **CDRUSSPACECOM.** CDRUSSPACECOM has operational authority and configuration authority for SATCOM on-orbit assets; control systems; and SATCOM terminal infrastructure, including applicable DOD gateways, deemed necessary for the effective and efficient operation of SATCOM for DOD. CDRUSSPACECOM directs operations of DOD SATCOM resources to provide global SATCOM support as operations and evolving requirements dictate and advocates on behalf of non-DOD authorized users, special users, CJCS, and presidential SATCOM support requirements.

(c) **CCMDs and Heads of DOD Agencies.** These commands and agencies validate and prioritize satellite access requests supporting referenced plans or missions.

(d) **Joint Force J-6.** Validates, consolidates, and prioritizes all joint force satellite requests and adjudicates differing resource requirements of the joint force that cannot be resolved.

(e) **Regional SATCOM Support Center Functions.** This center provides general support to CCMDs, Services, USG departments and agencies, and international partners in the allocation of SATCOM resources as directed by CDRUSSPACECOM.

(f) **Users.** Satellite access may involve two separate, but linked, processes: authorization to access a satellite channel and authority from the HN to transmit from a ground SATCOM terminal or device, if applicable. When satellite channel access is granted without the inclusion of specified authority to radiate on that satellite channel frequency, a failure to obtain HN authorization may preclude use of the satellite link.

For additional details on SATCOM, see CJCSI 6250.01, Department of Defense Satellite Communications.

(10) **EMS**

(a) The EMS is a highly regulated and increasingly congested and contested resource. It is part of the physical environment characterized by frequency, energy, and time. Natural and man-made factors affect actions in and through the EMS just as in the air, on land, at sea, in space, and in cyberspace. Gaining and maintaining EMS superiority necessitates an understanding of both military and civilian systems that operate within the EMS (see Figure III-1). Primarily, personnel assigned to the JEMSOC (J-2, J-3, J-6) plan, coordinate, and control joint military use of the EMS. Close coordination between the J-6 and JEMSOC is also key to mission success.

(b) One objective of the JFC is to shape and control the EMOE to enable the secure, dependable operations of EMS-dependent capabilities (of which DODIN is key).

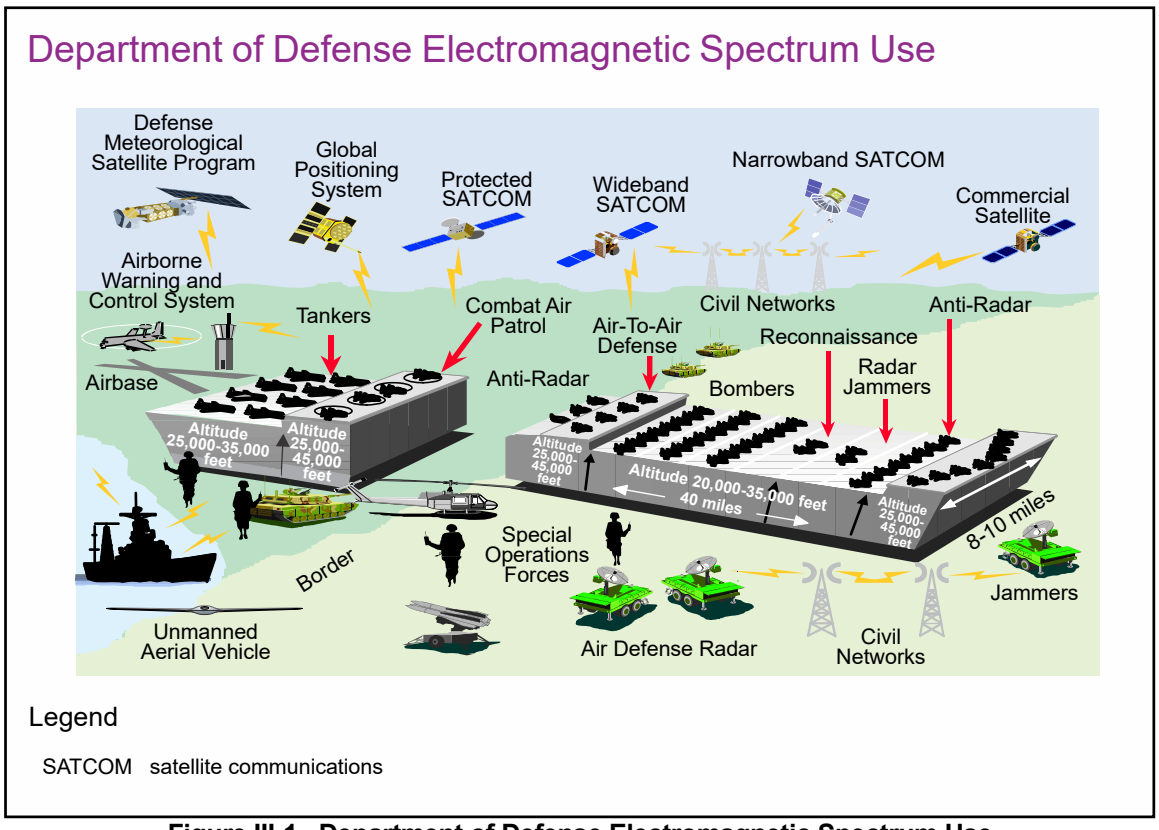


Figure III-1. Department of Defense Electromagnetic Spectrum Use

However, the EMOE transcends all physical domains and the information environment, and extends beyond defined borders or boundaries, thus complicating JEMSO.

(c) Any digital radio, or transceiver that is part of a digital data link, is part of the DODIN. Digital radios have internal computers and data storage that must be protected using the same principles used to protect other computers. They should be configured, installed, and operated so that they are secured from cyberspace threats and, if threatened, can be effectively defended.

For more information on JEMSO, see JP 3-13.1, Electronic Warfare; *JP 6-01,* Joint Electromagnetic Spectrum Management Operations; *CJCSI 3320.01,* (U) Joint Electromagnetic Spectrum Operations (JEMSO); *CJCSM 3320.01,* Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment; *and CJCSM 3320.04,* (U) Electronic Warfare in Support of Joint Electromagnetic Spectrum Operations.

4. Multinational Communications System Operations

a. Multinational communications system operations may be composed of allied and/or coalition partners. A multinational force can be composed of diverse groups of security and information sharing environments. Multinational forces will likely have differences in their communications system, classification limitations, language, terminology, doctrine, operating standards, capacity to share information, and willingness to share information, which can cause confusion and interoperability problems. Once the JFC establishes the specific C2 framework for a multinational operation, the IERs and information services are established and published in the Joining, Membership, and Exit instructions. Planning considerations include network federation, governance, and management of a federated network and EMS operations; equipment compatibility; procedural compatibility; application and configuration management compatibility; cybersecurity, including requirements for cryptographic security; identification, friend or foe; lessons learned from previous operations; video networks (e.g., VTC, sensor video feeds, commercial news feeds, and global broadcast services); and data link protocols. These and other considerations are further amplified in the following paragraphs:

(1) **Establish Liaison Early.** Liaison teams can be effective communications system interface solutions in multinational operations. Their importance as a source of both formal and informal information exchange cannot be overstated. Requirements for liaison should be established early and to the extent possible; liaison teams should be trained and maintained for known or anticipated requirements.

(2) **Identify Communications System Requirements Early.** The demand for information often exceeds the capabilities of the communications system within joint and multinational commands. It is crucial the JFC identify early communications system requirements external to the command or require support from national, multinational, and HN resources (e.g., space-based systems support, JCSE, and North Atlantic Treaty Organization [NATO] standing communications system equipment pool). Multinational

communications system planning must include the early establishment and incorporation of multinational networks. Lessons learned indicate initial requirements for multinational tools such as Battlefield Information Collection and Exploitation System and Combined Enterprise Regional Information Exchange System are typically understated. Resources need to be identified and planned for accordingly. Identification of the primary, secondary, and tertiary means to disseminate all required services is a critical planning responsibility, and planners must consider information classification requirements to facilitate exchange with partner nations.

(3) **Standardize Principles.** Standardization of principles and procedures by multinational partners for multinational communications is essential. As new technology is introduced and becomes more network enabled, this is an area of increasing concern. DODIN operations, including activities conducted to protect our networks, must be evaluated in the context of standardized IM principles and multinational networks.

(4) **Coordinate Agreement in Advance of Military Operations.** Multinational communications logistics arrangements should be coordinated in advance of all phases of military operations with probable multinational partners. This coordination should cover principles, procedures, and overall communications requirements and standards (including services, standard message text formats, standard databases and data formats, EMS management, and procedures for deconflicting frequency problems between multinational and civilian organizations). Multinational communications arrangements should take into account existing treaty obligations, as well as applicable status-of-forces agreements between the US and other nations. Formal agreements should be considered for cyberspace security and cyberspace defense actions within connected or overlapping, multinational communications systems.

(5) **Provide/Acquire Linguists, Interpreters, and Translators.** To ensure US interests are adequately protected, DOD provides or acquires its own linguists, interpreters, and translators.

(6) **Determine Releasability.** This planning consideration pertains to US security procedures and includes US keying material and equipment, and multinational connectivity to US networks. The operational acceptability and disclosure or release of COMSEC to foreign governments for multinational use will be determined and approved by the Committee on National Security Systems before entering into discussions with foreign nationals. Commanders and their staffs should be aware of the limitations in sharing information (classified or unclassified) with multinational partners. The JFC should plan for the additional time and coordination necessary to ensure compliance with established security requirements, to include COMSEC, compromise procedures, destruction guidance, account management, and foreign disclosure training. The dissemination, disclosure, or release of DOD information and/or intelligence to foreign governments for multinational use is approved only by DIA, the National Security Council, or the senior intelligence officer in theater and should not be confused with disclosure of US keying material or equipment outlined in the previous sentences of this paragraph.

For more information on multinational operations, see JP 3-16, Multinational Operations. *For more detailed guidance on foreign access, connections, and COMSEC release, see CJCSI 6510.06,* Communications Security Releases to Foreign Nations; *CJCSI 6211.02,* Defense Information System Network (DISN) Responsibilities; *and CJCSI 6510.01,* Information Assurance (IA) and Support to Computer Network Defense (CND).

(7) **Identify System Boundary Protection Criteria.** All established networks that involve multinational communications systems must include boundary protection (e.g., firewalls, guards) with security classification and restrictions IAW all the pertinent DOD security policy directives and instructions. The scope of the boundary protection criteria must be specified with no ambiguity among multinational communications system participants.

(8) **Identify Cross-Domain [Network] Criteria.** Information flow between different network security domains (e.g., between US and foreign mission partner information systems) requires the use of a cross-domain [network] solution.

(9) **Comply with USG Disclosure Policy.** Foreign disclosure officers should be appointed, trained, and certified early in the planning process at all levels of command directly involved in multinational operations. Their primary responsibility is to ensure common understanding of information that can be shared with multinational partners. Staffs at all levels should have sufficient numbers of foreign disclosure officers to sustain continuous operations.

For more information on sharing classified military information or national intelligence, refer to National Disclosure Policy-1, National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations; *DODD 5230.11,* Disclosure of Classified Military Information to Foreign Governments and International Organizations; *CJCSI 5221.01,* Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations; *Executive Order 12333,* United States Intelligence Activities; *Executive Order 13526,* Classified National Security Information; *and Intelligence Community Directive 403,* Foreign Disclosure and Release of Classified National Intelligence.

b. Commanders and planners must rapidly determine what is shared, when, and with whom. Communications system training required by multinational partners at each echelon has to be identified and resolved. Adapting a network to meet dynamic information-sharing rules advances modern military operations in a multinational environment. Commanders and planners must also understand the mission, intent, concept of operations, and information classification as an enabler of shared understanding. All specified, implied, and essential tasks have to be identified and understood by all mission partners. Different phases of a multinational operation at the strategic, operational, and tactical levels necessitate different and distinct levels and types of communications system and sustainability support. Finally, they should have a comprehensive knowledge of the multinational structure and relationships.

c. Communications system planning must be an integral part of joint force planning. Commanders and planners must understand, anticipate, and be prepared to deal with change. The joint communications planner must have a comprehensive knowledge of joint and mission partner C2 structure and relationships. They should clearly understand the capabilities and limitations of available strategic, operational, and tactical communications system resources. Planners should ensure communications that facilitate information sharing are established with non-US and HN commanders. Commanders and planners should identify communications system requirements that exceed their systems' capabilities (EMS access, equipment, or connectivity) within the joint or multinational force and coordinate any mitigating actions through appropriate channels when support is required. Collection of observations and lessons learned during this process will assist the JFC in the planning of future operations. Finally, they should ensure communications system capabilities and employment procedures for non-US forces are understood. To enhance multinational operations, at least three options for communications system assets and interoperability are available. Although any multinational operation is likely to use a mix of these three methods, the wider the participation, the greater will be the reliance on the use of voice links and liaison personnel. To accomplish this, commanders and planners should:

(1) Use system-to-system compatibility to ensure interoperability. The US may have to provide communications system resources to multinational partners to achieve this status.

(2) Establish and manage an interface between incompatible communications systems through a combination of interface hardware, software, and TTP to ensure interoperability.

(3) Establish basic (voice and/or data) communications links and ensure unity of effort through the use of TTP and liaison personnel.

CJCSI 2700.01, Rationalization, Standardization, and Interoperability (RSI) Activities, *focuses on enhanced communications system combat capabilities for US military forces to communicate and share data and information with multinational forces.*

d. The CCEB develops ACPs recognizing the importance of interoperability with the NATO Alliance. The ACPs (including basic and supplements) are used by more than 90 nations. ACPs provide communications instructions and procedures essential to the conduct of common military operations. ACPs facilitate the use of available communications services and provide a basis for detailed procedural and operational publications on communications subjects such as frequencies, call signs, address groups, and routing indicators.

For more information on multinational operations, see JP 3-16, Multinational Operations.

5. Communications Planning Methodology

a. **Planning Group.** Planners within J-6 coordinate with their counterparts within the operations, intelligence, logistics, administrative, and policy communities to ensure proper consideration and inclusion of communications system support in mission execution. In addition, they plan the evolution of the communications system to support future operations. Communications system planning is divided into five areas: mission analysis; information requirements analysis; interoperability, compatibility, and supportability analysis; capability analysis; and allocation of communications system assets.

(1) **Mission Analysis.** The J-6 and communications planners must clearly understand the mission, the commander's intent, concept of operations, task organization, commander's critical information requirements (CCIRs), and the C2 framework. Planners must also consider threat capabilities and COAs, as well as task force employment of non-communications EMS-dependent systems. During mission analysis, communications system planners develop the communications system estimate and specified and implied tasks to be performed by operators and communications system personnel. The communications system estimate is the J-6's assessment of COAs that serve as the foundation of the commander's estimate. Using foundational knowledge of the C2 framework and communications system capabilities, planners translate the concept of operations into specified and implied tasks during each phase of operations. Planners develop tasks for the deployment, implementation, operations, sustainment, modification, and restoration of C2 systems and networks to achieve information superiority throughout operations and support. Network management tools and C2 systems facilitate planning as well as SA. Planning and analysis of C2 is enhanced when commanders' mission analysis includes identification and prioritization of key terrain in cyberspace.

(2) **Information Requirements Analysis.** This analysis identifies communications requirements (who communicates with whom), the means/systems that will enable communication, and the products (including their volume) needed. Communications system planners work closely with all functional communities to develop IERs. IERs identify products to be transmitted and received, as well as the throughput, quantity, and characteristics of those products. The communications system is tailored to meet the projected IERs. During military operations, planners conduct analysis to see if the mission, concept of the operation and support, CCIRs, and C2 framework necessitate the increase or decrease of the IERs or new exchange requirements. Planners make adjustments to the IERs as appropriate.

(3) **Interoperability, Compatibility, and Supportability Analysis.** This analysis identifies technical protocols, formats, and operational and security concerns required for the JFC, to include mission partners' requirements. Planners identify interoperability, compatibility, and supportability requirements and assess them against documented capabilities. When the mission permits, key interoperability and compatibility solutions will be validated before mission execution. Any shortfalls or deficiencies are assessed for operational and mission impact. In cases where operational and mission impacts are too severe, the communications system planners determine whether it is

operationally and technically feasible to resolve the problem in theater; if not, they request assistance from higher HQ.

(4) **Capability Analysis.** This analysis matches information needs with capabilities/assets and identifies specific communications services/systems required. Based on mission analysis, information needs, interoperability, compatibility, and supportability analysis, communications system planners identify the C2 systems and networks that can support the OPLAN. Service component planners should be brought into capabilities analysis as soon as practicable. Capabilities analysis should be performed daily. The CCMD J-6 should provide an organic communications system and networking capability for deploying and in place units within the AOR. Normally, a Service component provides communications system support at each operating location within the AOR. Communications capabilities are matched against operational needs and limitations and shortages are identified for each location, major platform, and mission. Special attention will be given to the time-phased force and deployment data (TPFDD) information and in-transit communications for deploying units. In the end, a database will be created that indicates the C2 systems and networks needed at each location, for each mission, and for each major platform.

(5) **Allocation of Communications System Assets.** The objective is to provide the commander a tailored communications system support package. This ensures the communications system is embarked and sequenced to coincide with the arrival of forces and implements the phased communications system build-up and activation plan. After the template is developed, joint force, Service, and functional component planners examine all available resources and plan a tailored communications system. Planners engineer the various C2 systems and networks needed for the joint force. Central management of C2 systems and networks ensures their proper performance. Parent commands should maintain C2 of their organic communications units based on the mission. Mission requirements may dictate some task organization of communications system units to meet the enlarged or reduced roles of higher HQ. Where units are collocated, planners should use the communications services/system assets of one unit to cover the other unit's requirements. Through all phases of the operation, planners should utilize commercial services/systems where appropriate. Communications system planners shall centrally plan and manage strategic and tactical SATCOM, EMS use, and other C2 systems and networks to support:

(a) The joint force HQ.

(b) Service and functional components in the operational area down to the tactical level, where appropriate.

(c) Connectivity to the DISN, the commercial communications system and network, multinational communications systems and networks, and the Service communications system.

For more information on communications planning, see JP 3-33, Joint Task Force Headquarters, *and JP 5-0,* Joint Planning.

b. **Planning Tools.** Automated planning and management tools facilitate communications planning, engineering, activation, and modification. These tools:

(1) Create/modify databases for communications system equipment and organizations.

(2) Define the network topology based on sites and by organizations.

(3) Create/modify subordinate unit tasks, responsibilities, and schedules and track performance.

(4) Conduct feasibility analyses using modeling and simulation.

(5) Create/modify and support distribution of communications plans and orders (communications annexes, the joint communications-electronics operating instructions [JCEOI], JRFL, and communications service requests).

(6) Perform detailed network planning and engineering for a joint force network, including:

(a) Circuit switch planning and engineering.

(b) Voice network planning.

(c) Data network planning.

(d) Video network planning and engineering.

(e) DISA organizational messaging service planning and engineering.

(f) Message switch planning and engineering.

(g) Backbone transmission system planning and engineering across the EMS, to include SATCOM.

(h) Radio network planning and engineering.

(i) Engineering plans and orders.

(j) Coordination for link and network activations/deactivations.

(k) Coordination for and integration with HN communications system resources into the joint/multinational network.

(7) Graphically display network configurations and status changes.

(8) Provide the joint force access to communications system status information to enhance SA.

(9) Conduct performance analysis.

(10) Provide automatic capability to discover network devices and services, populate network management databases, and save each discovery for automated reporting of differences.

(11) Perform network device configuration/reconfiguration.

(12) Generate and process change orders.

(13) Perform automated fault management.

(14) Model, evaluate, and optimize proposed network changes.

(15) Assign and deconflict frequency resources.

(16) Perform automated communications propagation analysis.

(17) Support EMI resolution.

(18) Display regional communications system DCO status.

(19) Correlate cybersecurity events and cyberspace incidents with respect to their impact on C2 systems and networks.

(20) Support electronic key management systems.

For detailed guidance on the communications system operation planning process, refer to CJCSM 3130.03, Planning and Execution Planning Formats and Guidance. *See also CJCSM 6231.01,* Manual for Employing Joint Tactical Communications.

c. **Development of the Network Plan.** Planners use automated planning tools to integrate all communications system resources to ensure unity of effort, exploitation of total force capabilities, and the fusion of information. The network plan includes assignments of responsibility, hardware connectivity and configuration, software and application usage, and process functionality. The network plan provides the details necessary to bring communications system support together to provide the quality of service required by network users.

d. **Continuous Planning.** Planners must continuously update communications system plans until mission completion. Often, communications system support is first in and last out. As operations proceed through branches, sequels, and phases, planners must modify communications system plans as appropriate. The fog of war creates expected and

unexpected contingencies that the planner must handle. Performance information on C2 systems and networks needs continuous analysis to identify trends and tendencies that may need to be changed during future operations. Communications system resources are continuously tracked.

e. In the absence of automated planning tools, planners must be prepared to use manual planning techniques.

6. Communications Planning Factors

a. The J-6 should be brought into the planning process early. The J-6 must understand the concept of operations and provide advice to the JFC during planning.

b. **The important factors for a communications system plan are feasibility and the adequacy of the plan to satisfy the JFC's information requirements.** A useful first step is the constant assessment of the communications system plan during the development process for its consistency with basic communications system principles.

c. Although communications system planning is conducted in unison with the other planning elements of the joint staff, dynamic information needs dictate that communications system planners must anticipate user requirements throughout all phases of joint operations. Every aspect of joint operations depends upon information to direct and accomplish the assigned mission. Planners must identify requirements for system security (e.g., confidentiality, integrity) and incorporate them into communications system planning efforts. Incremental development, deployment, and employment of plans and initial communications system support are essential to meet the JFC's continually evolving mission.

d. Other factors to consider as the communications system plan is developed are:

(1) **Organic Communications System Resources.** Assignment of a unit to a mission will require a quick assessment of available organic communications system resources. The objective is to keep organic communications system resources intact. However, there are situations where this is not practical. Throughout the planning process, the planner must track organic communications system resources within each unit and HQ. In a joint force scenario, where a commander of a Service force is designated the JFC, the other Service components should plan to augment the lead Service force's organic communications system resources to facilitate the fulfillment of joint requirements.

(2) **Practical Communications System Support.** To the extent possible, communications planners should rely on agreed to standards and TTP to support the mission. In a complex network environment, changes and new approaches can have significant consequences if not planned and tested. Training, exercises, demonstrations, and experimentation provide lessons learned and outcomes to identify what works and does not work. As the planning for current operations is ongoing, the prudent outcomes of

brainstorming, exercises, training, demonstrations, and experimentation are employed in the current mission.

(3) **TPFDD Flow.** The JFC prioritizes the flow of units into theater. Communications system planners monitor and influence the flow of communications system units, personnel, and equipment into the operational area to support the C2 of forces in theater.

(4) **Joint Reception, Staging, Onward Movement, and Integration.** Planners must arrange for communications system support during joint reception, staging, onward movement, and integration. During this phase, employment of organic communications system resources is limited. Joint force planners coordinate with the Service components' planner for appropriate communications system support.

(5) **Incremental Building.** Because military operations seldom occur at the same location as the preponderance of our military forces, the JFC should expect planners to build the communications system incrementally. Most operations initially rely on SATCOM to move information between HQ and commanders. Based on the mission and assets, planners install voice, data, and video systems. Connections to the DISN and commercial networks become more extensive and robust as operations progress. Once the operation is complete, the communications system should also deactivate/redeploy incrementally.

(6) **Modular Packaging.** Based on the mission, commander's intent, OPLAN, capabilities, limitations, availability of equipment, and the communications infrastructure in the operational area, planners build modular packages to meet the commander's needs. Planners tailor these packages to existing conditions and link the individual communications system modules into a cohesive communications system.

(7) **Interoperability** should be achieved primarily by a commonality of equipment, software, and systems. Planners must know the capabilities and limitations of the other component communications system resources and must be able to integrate them into the joint communications system plan. Use of JCEOI and COMSEC must be coordinated with Service communications-electronics operating instructions/signal operating instructions and COMSEC.

(8) **Standardization** is required in the communications system. Planners should ensure equipment and system configurations are standardized and/or compatible to facilitate interoperable exchange of decision-quality information across employed units. The JFC's communications system requirements must not be compromised by uncontrolled use of nonstandard systems, protocols, or procedures.

(9) **Impact of Internal and External Changes to C2.** Planners must anticipate and respond to changes to variations in the initial mission in a timely manner. The communications system plan should include a variety of resources. Connectivity among commanders, HQ, and units down to the tactical level must incorporate alternate routes and

methods. A diversity of systems and alternate routes contribute to the communications system's flexibility, survivability, and responsiveness.

(10) **Operational Contract Support (OCS).** OCS is the process of planning for and obtaining supplies, services, and construction from commercial sources in support of joint operations. Using the OCS process, planners should plan for the use of commercial systems. The availability of commercial communications system resources may offer an alternative means to satisfy the JFC's needs and may reduce the number and size of deployed modular communications system packages. Commercial capabilities resident in the operational area compensate for tactical communications system resource shortages and meet the early information requirements of a joint force deployment. Planners must ensure the deployed modular packages include sufficient capabilities to interface with commercial systems. Commercial capabilities may also assist in meeting the JFC's tactical communications system redeployment requirements. The communications systems planner should coordinate with the operational community to ensure development or modification of alternate procedures for degraded or denied off-base network connectivity that are feasible, adequate, and acceptable to the user community.

For more information, see, JP 4-10, Operational Contract Support.

(11) **Training.** Communications system managers must be trained. Of particular importance is training of individuals to integrate and operate commercial capabilities and networks with the JFC's organic capabilities. Ideally, communications system personnel should possess adequate language skills to work with HN and multinational forces. Otherwise, units should train on the use of translators.

(12) **Discipline.** Communications system resources are limited. The JFC should ensure the information that moves through these limited resources supports necessary decision-making actions and overall mission execution. The mission and the commander's intent guide what information is provided to the joint force. The commander should provide additional guidance on what information is to be pushed and pulled to the joint force within the DODIN. Long-established procedures such as minimize should be used and augmented to promote communications system discipline beyond just controlling the flow of record message traffic (e.g., VTC, e-mail attachment size, and briefing slides). The communications plan should also accommodate disadvantaged (e.g., low bandwidth) users.

(13) **Timeliness.** The JFC should identify all critical information requirements. Development of priority lists that facilitate the timely restoration of the most critical information is essential.

(14) **Simultaneous Planning.** Planners should participate in the numerous planning cells of the joint force (e.g., targeting, future operations, information activities). The planning process for each of these cells is continuous and iterative. Communications system planners perform high-level planning to develop comprehensive estimates to design, engineer, implement, and maintain the communications system. Activation of communications system links and networks occurs when an OPORD is executed. During

the execution of an operation, planners must consider the next phase of the JFC's operational concept and plan for its support.

e. **Operational Limitations**

(1) **Connectivity.** The communications system should establish a level of robust connectivity that enables communication with the joint force, its subordinate forces, its higher HQ, and any additional reachback capabilities required. To the maximum extent possible, the hardware and software interfaces should be transparent to the system user. The continued flow of information should not depend on action by an intermediate user.

(2) **Range.** Planners must assess operational impacts of range against mission requirements, system capabilities, and information sharing priorities.

(3) **Environment.** The environment, to include hydrographic, terrain, meteorological, vegetation, manmade, and cultural features, affects the employment of the communications system and requires a tailored approach. Such environmental surroundings determine the usable frequencies, output power, and location of communications system resources.

f. **Collaborative Capabilities.** Planners should consider that successful collaboration requires more than just collaborative capabilities that help participants share information and knowledge in a collaborative information environment (CIE). A second component of this environment is infrastructure—the various information systems on which the tools reside and the networks that link these systems. The C2 systems, networks, and collaborative tools need procedures—based on accepted theory and practice and established to meet joint force needs, which regulate use in ways that facilitate collaboration. The full benefit of these capabilities is realized only with a fourth component—users who are trained to properly apply information classification standards to enable information exchange and to use the tools and systems and educated to understand the advantages and power of a CIE.

g. **Communications Risks and Risk Management**

(1) Connectivity is increasingly a mission-critical resource and its availability can determine mission viability during planning and execution. While network-enabled operations can increase force lethality, survivability, and operations tempo, conversely, network loss can reverse these performance enhancements and put the force at increased risk, potentially threatening the mission. In addition, protecting the confidentiality, integrity, and availability of information and information systems with implementation of security controls and measures, coupled with the use of intelligence to enable threat-based risk management, is essential to continued DODIN operations.

(2) Communications risks can include, but are not limited to, the following:

(a) Network and system vulnerabilities.

(b) Connectivity issues and outages.

(c) Unsynchronized and uneven deployment of technology upgrades and integration with legacy systems.

(d) Reliance on a mix of military and commercial networks/infrastructure.

(e) Globalization of IT and telecommunications networks.

(f) Cross-network domain spillages.

(g) Unauthorized disclosure of classified information or controlled unclassified information.

(h) Privacy loss through meta-data tagging.

(i) EMS issues (i.e., intentional or unintentional EMI, rules of engagement, or other restrictions on usage).

(j) Cyberspace threats (internal and external) to operations.

(k) Security of the global supply chain for IT systems in use by DOD.

(l) Loss or degradation of positioning, navigation, and timing information (e.g., Global Positioning System information).

(m) Presence and/or operations of the DODIN by non-DOD entities, including partner nations and commercial vendors.

(n) Lack of interoperability with essential mission partner systems.

(3) To reduce overall operations risk, skilled communications planners should be an integral part of the original operational planning team to assist in defining the problem, developing the plan, and providing for sufficient lead time to coordinate with outside communications support providers. This will reduce the risk of having operational planning teams with no communications expertise develop an unsupportable plan or not building enough flexibility and redundancy into a supportable plan.

(4) A comprehensive risk management program is the most effective way to protect the DODIN. Risk management identifies, measures, controls, and eliminates or minimizes uncertain events that may adversely affect system resources. The objective of risk management is to achieve the most effective safeguards against threats of both intentional and unintentional intrusions into a network or system. Intentional intrusions are planned against information resources and must be defeated by an effective defense in depth. Risk management also identifies network and information system vulnerabilities created by weaknesses in design, poor resource deployment, inadequate processes,

ineffective security procedures, or faulty internal controls that are susceptible to exploitation by authorized or unauthorized users.

For more information on the risk management framework process, see DODI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT), *and DODI 8330.01,* Interoperability of Information Technology (IT), Including National Security Systems (NSS).

7. Communications System Employment

a. Communications system needs and capabilities of a small joint force with a limited humanitarian mission are vastly different from those of a CCDR with continuing, multitasked, multinational-based combat missions. The phases of a joint operation or campaign are situation- and mission-dependent. Timelines between phases may be severely compressed and may not follow each other or terminate in the expected sequence. However, defined phases provide a guideline for the JFC and communications system planner. Within the phases of an operation, it may be helpful to consider several activities that potentially affect communications system employment. For example, actions during an early phase may require mobilization and other predeployment activities to set the terms and conditions for operations. During predeployment activities, JFCs exercise flexible deterrent options and tailor forces for deployment. Cybersecurity considerations are critical to all activities.

b. **Predeployment Activities**

(1) **During this time, the JFC is designated and forces are assigned.** SecDef and CJCS orders provide the JFC with guidance to initiate planning. The JFC issues a mission statement and commander's intent. Planners develop the concept of operations subsequent to receipt of the mission statement and commander's intent.

(2) **The objective** is to produce a communications plan to support the commander's intent, mission, and concept of operations and prepare initial communications system deployment packages to provide an initial operating capability that supports the operational plan. In addition, the planners should consider en route communications to support initial tactical entry.

(3) **The method.** The communications system planner uses the planning methodology previously discussed to develop a plan to support the commander's concept of operations. To begin mission analysis and initial planning, the communications system planner must clearly understand the command relationships of the joint force.

(a) The basis of all communications system planning is understanding what joint and multinational forces are assigned, attached, or in support of the JFC. Collaborative planning, both horizontal and vertical, is a priority throughout all phases of the operation. The JFC communications system planner must involve subordinate and supporting organizations throughout the planning process. Automated aids, historical data,

lessons learned, and intuitive judgment assists in developing the communications support plan. As the DOD lessons learned system of record, the Joint Lessons Learned Information System (JLLIS) provides the automated capability to collect, track, manage, and share insights and practices, and support the collaborative resolution of issues, from operations, exercises, and events. Consideration of JLLIS contents may provide solutions to planning problems not yet considered.

(b) During mission analysis, the joint force planner works simultaneously with component planners and supporting communications providers (such as DISA and USCYBERCOM) to evaluate the existing communications infrastructure in theater to determine the strategic and tactical communications assets required. Communications system plans must properly sequence the deployment of assets to support the operational plan. The commander's C2 capabilities are limited by the capacity of deployed communications system assets.

(4) **The means.** This phase of the operation will rely on the existing commercial, strategic, and tactical communications infrastructure.

c. **Deployment Activities**

(1) **The plan is completed and published.** The communications system is expanded to provide improved information flow between the JFC and component commanders. As the system deploys, large pieces are extended into the operational area. Communications system assets deploy or are built-up (e.g., contracted) incrementally in support of the operational area. Initial tactical communications are global but can be insufficient in capacity if not properly planned, coordinated, and employed. The primary focus of initial tactical communications system deployment packages is decision support to the on-scene commander and to providing the foundation for network expansion to support follow-on operations (e.g., lodgment expansion).

(2) **The objective** is to provide for the continuous flow of information between commanders during the initial phases of the operation and establish the base strategic and tactical communications system infrastructure to support follow-on operations.

(3) **The method.** Lift assets deploy the initial communications system capability. This initial communications system capability is composed of a modular package that provides the commander with voice, data, and video connectivity. The initial deployment package provides global connectivity, as well as the foundation, to build the remainder of the network incrementally. In austere tactical environments, the initial network is not robust and may be severely degraded when disturbed. Communications system support must include reliable, redundant capabilities that ensure the commander is always able to maintain C2 of component and supporting forces.

(4) **The means.** This phase of the operation relies on a mix of strategic, commercial, and tactical communications to support the introduction of forces into an operational area. The JFC employs super-high frequency (SHF) SATCOM, extremely

high-frequency SATCOM, tropospheric scatter radio, and other military and commercial assets to support strategic and tactical long-haul communications requirements. The joint force uses other systems, such as ultrahigh frequency (UHF), very high frequency, high frequency, and low frequency/very low frequency radios, to provide redundancy and support internal information requirements, as well as to support tactical users most vulnerable to disconnection, intermittent, and low-bandwidth limitations.

d. **Employment Activities**

(1) **Primary challenge during deployment is organization.** The J-6 must maintain an effective organization that enables rapid change. Although each subordinate command has responsibility to identify, schedule, and prioritize units and equipment for deployment, the J-6 needs to track arrival of communications equipment that supports key nodes. The J-6 provides a centralized point of contact for coordination and status for deploying communications system equipment and personnel and ensure joint communications assets are included on the TPFDD. As units deploy into theater, they typically require tactical entry into the DISN via one of the theater enterprise gateway locations. Access to enterprise gateway locations requires close coordination and troubleshooting between unit and DOD Gateway technical control. Consequently, the DISA will prioritize DOD Gateway activation support.

(2) The deployment process may constrain communications build-up during employment. Both lift availability and unit preparation for deployment may delay immediate establishment of portions of the communications system. The structured approach to build-up of the communications system enables theater capabilities to rapidly provide initial communications, followed by a managed expansion of communications support.

(3) **Network Monitoring, Control, and Reporting.** One of the critical functions of the JNCC during employment is network monitoring, control, and reporting. Control of communications system functions consists of assessing the effectiveness of communications system operations, providing information, maintaining the currency of the estimate, and changing communications system operations in response to the evolving operational scenario. Network monitoring takes a macro look at the operational area from the J-6 perspective with the objective of ensuring optimum network performance. Reporting requires the establishment of performance measures and reporting thresholds; delineation of organizational relationships, responsibilities, and procedures (e.g., formats, media, timelines, and others); and identification of special interest systems, circuits, or communications system support for critical operational functions. Near real time monitoring and reporting will facilitate decision making by enabling the JFC to rapidly and accurately assess networks for operational impact, prioritize missions, and assess mitigation options.

(4) The joint force and the Service and functional components continue a sequenced, balanced deployment. As assets arrive, they add capability and redundancy to the existing communications system. The JFC employs communications system assets to meet current requirements, as well as to support the planned operational scheme of maneuver.

(5) **The objective** is to produce a reliable, resilient, secure, jam-resistant, available, accessible, and robust communications system that supports the JFC's concept of operations.

(6) **The method.** A more capable communications system continues to arrive and expand as dictated by the mission, commander's intent, concept of operations, and, to a certain extent, lift assets. Large-capacity satellite, terrestrial switching, and transmission systems arrive during this phase of the operation. The J-6, through the JNCC, establishes numerous alternate routes to increase the robustness of the network. Units establish local area networks at the joint force and Service component levels and are connected to the global wide-area network (WAN) to increase information flow. As the system increases in complexity, more sophisticated systems are employed to maintain effective technical control over the expanding network. Throughout employment, the J-6 continues to plan the expansion and transition of the communications system to support the JFC's concept of operations for future operations.

(7) **The means.** The JFC relies on various systems, including JCSE systems, to connect to and expand other portions/services of the DODIN into the operational area. Large-capacity ground mobile forces and commercial satellite systems are added to the DODIN with a mix of satellite and terrestrial systems to further extend the communications system into the operational area. SHF and UHF terrestrial multichannel radios connect voice, data, and video via digital switches and technical control facilities. Joint forces make maximum use of existing commercial and government systems throughout employment activities.

e. **Sustainment Activities**

(1) **The J-6 continues to refine and improve the communications system.** The communications system remains robust and flexible to support changes in the scheme of maneuver. An increasing concern during this phase is the quantity and availability of repair parts and consumables that are necessary for preventive and routine maintenance.

(2) **The objective** is to sustain and improve the automated flow and processing of information between the various commanders and develop plans to support any changes in the OPLAN.

(3) **The method.** The continuing mission, the needs of the commander, and users guide any changes made to the existing communications system. These changes improve the overall capacity of the system to move information seamlessly and transparently among components and national organizations. The correction of design flaws and the increasing reliability of the communications system enable the communications personnel to turn their attention to those actions that keep the systems functioning. Once follow-on communications system resources are in place, the next step is to develop the plan for the redeployment of initial capabilities such as JCSE-controlled assets. Continued attention to preventive and routine maintenance, and adequacy of stocks of spare parts, repair parts, and/or consumables is essential to network health.

(4) **The means.** JNCC directs modifications to the communications system to respond to changing mission and cybersecurity requirements. Technical control facilities take on an increasingly important role as they make changes to the established systems and maintain continuous service to the customers. Service organic and common-user transportation assets move consumables and repair parts to established repair facilities.

f. **Transition Activities**

(1) **Branch and Sequel Planning.** Changes in the JFC's mission, organization, or operations may require changes to the communications system architecture. Another source of change may be shortfalls in communications system support to operations, equipment or network degradation, and/or availability of a new communications system capability. JNCC future operations planners must actively monitor for these potential changes and develop branches and/or sequels to respond appropriately.

(2) **Transition Planning.** Although the original communications system plan will have a transition plan, the dynamic operating environment will make it necessary to review and potentially modify or redraft the plan. In many cases, although major operations cease, a residual communications capability is required. Transition planning should consider both the transition of communications services to a permanent infrastructure and the potential deactivation of US communications system services. Frequently, services will transition to commercial or HN-provided communications system services.

(3) **Transition.** During this time, the J-6's priority is executing the transition plan. Proper execution of the transition plan requires the J-6 to liaise closely with the designated follow-on organization to conduct a smooth transition of responsibilities and control.

g. **Termination or Post-Conflict Activities**

(1) **The planner** must prepare for the termination of combat operations or the transition to post-conflict operations. This stage of planning and execution must establish the basis for redeployment operations and continue to meet the communications system needs of supported commands.

(2) **The objective** is to monitor the transition of communications system assets to meet changing operational requirements and ensure continuous support for the joint force.

(3) **The method.** It is imperative that communications system capabilities are not reduced too rapidly so it may continue to support the JFC's follow-on mission. The J-6 must retain a flexible, dynamic network to meet rapidly changing mission requirements. As subordinate elements reposition or are assigned new missions, the JNCC adjusts the network to provide continuous capabilities. Reliance on satellite systems may grow during this period as more forces prepare to redeploy while the operational area remains the same.

The planner employs redundant capabilities such as UHF TACSAT to ensure the continuous flow of information across the operational area. The planner must anticipate an increased reliance on the local commercial infrastructure to facilitate HN coordination.

(4) **The means.** As with the previous phases, this phase of the operation relies on various systems to connect to and expand the DODIN into the operational area. Large-capacity satellite systems continue to provide connectivity to other parts/services of the DODIN to dispersed forces throughout the operational area. Systems such as UHF TACSAT or HN communications provide redundant capabilities throughout the operational area.

h. **Redeployment Activities**

(1) **Planning is the most important part of** the redeployment activities. The communications system must continue to provide information flow to the commanders, even as it purposefully disengages, and large components of the network are removed for redeployment.

(2) **The objective** is to redeploy systems that are no longer needed and continue to provide communications support for the JFC and those multinational and functional component forces remaining in the operational area. The JNCC must focus on retaining and transitioning network control until the joint network no longer exists. A JNCC should remain standing whenever either of two conditions exists: there is a portion of the operational joint network where more than one subordinate command requires the communications support from another subordinate command or there exists one or more deployed joint organizations which require communications system support. During this time, the JNCC must ensure all units follow J-6 guidelines regarding deactivation of their respective communications system resources. To ensure an orderly deactivation and continued support of minimum network services, supporting components/commands/units coordinate with the JNCC prior to deactivating DISN services.

(3) **The method.** While the amount of sustainment capability and the number of redundant systems will decrease, the J-6 must maintain some communications system capabilities until the JFC no longer requires them. In the final days of redeployment activities, the communications system may look very similar to the system originally deployed.

(4) **The means.** The original commercial and government infrastructure should support as much of the communications system redeployment as possible. Lacking such an infrastructure, the last systems to redeploy are typically the mobile and easily transportable assets, such as UHF single-channel and small SHF satellite terminals.

Intentionally Blank

CHAPTER IV
INFORMATION SHARING AND SERVICES

"The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant actor perceptions, behavior, and action or inaction and to support human and automated decision making. The information function helps commanders and staffs understand and leverage ubiquitous and often unpredictable nature of informational impacts and the role of information in all military operations. This function provides JFCs [joint force commanders] the ability to integrate the generation and preservation of information while leveraging the inherent informational aspects of all military activities to achieve the commander's objectives and attain the end state."

Joint Publication 1, Volume 1, *Joint Warfighting*

1. General

a. US national security depends on the ability to share the right information, with the right people, at the right time. **Information sharing** requires sustained and responsible **collaboration** between federal, state, local, tribal, territorial, private-sector, and multinational partners. The dynamic operational environment presents challenges to continue improving information sharing and safeguarding processes and capabilities. While innovation has enhanced the ability to share, increased sharing has created the potential for vulnerabilities requiring strengthened safeguarding practices.

b. Information sharing is an increasingly important element of mission success. Joint forces must effectively exchange information among components, USG departments and agencies, multinational partners, foreign governments, and international organizations as a critical element of efforts to defend the nation and execute the national strategy. This improves unity of effort, reduces decision time, increases adaptability of forces, improves SA, and provides greater precision in mission planning and execution.

c. DOD information sharing is the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant. The *National Strategy for Information Sharing and Safeguarding* guides DOD's sharing of information within DOD and with federal, state, local, tribal, and multinational partners; foreign governments and security forces; international organizations; NGOs; and the private sector. This strategy identifies three core principles to address the challenge of improving information sharing and safeguarding processes and capabilities.

(1) Information is a national asset. USG departments and agencies have an unprecedented ability to gather, store, and use information consistent with their missions and applicable legal authorities; correspondingly, they have an obligation to make that information available to support national security missions.

(2) Information sharing and safeguarding requires shared risk management. To build and sustain the trust required to share with one another, all must work together to

identify and collectively reduce risk, rather than avoiding information loss by not sharing at all.

(3) The core premise, information informs decision making, underlies all actions, and reinforces that better decision making is the purpose of sharing information in the first place.

d. The strategy focuses on achieving five goals:

(1) Drive collective action through collaboration and accountability.

(2) Improve information discovery and access through common standards.

(3) Optimize mission effectiveness through shared services and interoperability.

(4) Strengthen information safeguarding through structural reform, policy, and technical solutions.

(5) Protect privacy, civil rights, and civil liberties through consistency and compliance.

f. **Department of Defense Information Enterprise.** DODD 8000.01, *Management of the Department of Defense Information Enterprise (DOD-IE),* provides direction on creating an information advantage for DOD personnel and mission partners and, IAW the *National Strategy for Information Sharing and Safeguarding,* provides direction for information sharing among all DOD components with mission partners.

2. Mission Partners

Joint forces must be able to integrate effectively with USG departments and agencies, partner nation militaries, and indigenous and regional stakeholders. This integration must be scalable, ranging from the ability of an individual unit to utilize the expertise of a nongovernmental partner to multinational operations. The mission partner environment information sharing capability framework has been developed using these criteria to enable assured information exchange among mission partners and consists of a combination of people, systems, policies, procedures, and processes to plan, prepare, and execute operations within a CIE.

a. **Identify Mission Partners.** The joint force must operate with all joint, interagency, international organization, and multinational mission partners. These mission partners may encompass a multitude of units and organizations. In an information sharing context, identification of mission partners should include understanding what information needs to be provided to which partners, as well as what information is desired from them. This should inform planning for releasability, as well as planning for the people, systems, and processes to enable information transmission to or from partners. The ability for all these participants to collaborate with one another is instrumental in the success or failure

of military operations. Information sharing is the foundation upon which increased collaboration with partners is enabled.

(1) **Multinational Partners.** Multinational information sharing should be facilitated by establishing a shared architecture using existing and emerging multinational mission capabilities, including Internet protocol networks. As the current DOD multinational information-sharing portion of the DODIN, multinational networks define the standards for establishing and maintaining multinational connectivity at the tactical and operational level, with reachback capability to the strategic level. Considerations for the multinational network must include the applications and services required to facilitate the utility of the network. The network must be capable of supporting communities of interest within the multinational community of interest. Additionally, information classification requirements should be clearly defined. During Operation IRAQI FREEDOM and Operation ENDURING FREEDOM, interagency, NATO, and other coalition personnel were hosted on US military facilities, sometimes in substantial numbers. The communications and information sharing needs of these partners could differ from standard military needs, particularly when hosted by smaller units. Planning for any potential hosting of significant numbers of interagency or United Nations personnel should account for these needs.

For more information, see JP 3-16, Multinational Operations.

(2) **Interagency Partners and International Organizations.** The joint force must be capable of coordinating the actions of people, organizations, and resources across great distances among diverse participants, such as USG departments and agencies, state and local authorities, and NGOs. To prevail, the JFC's decision-making and execution cycles must be consistently faster than the enemy's and be based on better information. Being faster and better requires having unfettered access to information derived from all available sources. Information sharing, cooperation, collaboration, and coordination are enabled by the information sharing environment that fully integrates interagency and international partners in a collaborative enterprise. This type of collaborative information sharing environment must be capable of generating and moving C2, intelligence, logistics, and other operational information and orders where needed in the shortest possible time. The architectures constituting a mission partner environment information sharing capability must be dynamic, flexible, and capable of providing interagency participants rapid access to appropriate data. It must facilitate the capability of the mission partners to focus on supporting the JFC and subordinate joint force components and to integrate support from non-DOD agencies and NGOs as needed.

For more information, see JP 3-08, Interorganizational Cooperation.

(3) **NGOs and Private-Sector Partners.** NGOs and other partners, such as local government representatives and civic leaders, may lack a technical capability for secure information sharing. To support more secure and readily accessible information sharing with NGOs or other partners, unclassified, but authenticated, web-based portals or other means may need to be established. Additionally, NGOs may be indirect end-users of

shared information, such as when NATO bodies serve as clearing houses for threat and hazard reporting for the local NGO community. Joint planners should be aware of how information is intended to be shared with NGO recipients in support of mission objectives.

b. **Establish Standards.** Standards facilitate integration of communications systems and networks with external mission partners at the operational and tactical levels. The joint force will most likely possess a more advanced C2 system than most mission partners. The burden thus falls on the joint force to create an information framework that will facilitate mission partner integration. This information sharing framework should leverage a federated network concept supporting the connection of multiple networks and national systems, with applications and tools, to enable information sharing at an appropriate single security classification level.

c. **The Communications System.** Whether classified or unclassified, the mission partner environment information sharing capability must be capable of securely integrating mission partner systems using mission partner communications network IT infrastructure, enterprise services, and architectures. Use of agreed upon information and data exchange standards/services enable interoperable information exchanges. The mission partner environment information sharing capability framework enables mission partners to exchange information with all participants within a specific partnership or multinational force. Mission partner communications networks assist commanders to achieve unity of effort and seamless exchange of operationally relevant information with mission partners from the operational to the tactical level. Key aspects of mission partner communications network implementation include liaisons, identification of communications network requirements, multinational communications agreements, interpreters, a coherent releasability/disclosure policy, and a sufficient number of foreign disclosure officers.

d. **Processes Planning.** The joint force should tailor policies and procedures to ensure standards for information sharing are implemented based on national- and theater-level guidance. The mission partner communications system framework facilitates mission partner collaboration and information exchange through established interfaces, protocols, and standards. A critical element of mission partner communications system is the identification of authoritative data sources and services.

e. **Agreements.** In some multinational operations or campaigns, joint forces will be able to use existing international standardization agreements (e.g., NATO) as a basis to establish rules and policies for conducting joint operations. Since each multinational operation will be unique, such agreements may have to be modified or amended based on the situation.

f. **Policies and Procedures.** Mission partner information must be protected with increased emphasis on the responsibility to coordinate integration and configuration of trusted information sharing capabilities. Care must be taken to avoid unintended negative second- and third-order effects of policy changes on national security and day-to-day operations. It is not possible to address policy in all information sharing situations a commander may face in mission partner operations. Commanders must continue to assess

risk, determine the best application of policies, and then request waivers in light of specific mission requirements and mission partners. A joint force participating in a multinational force operation develops the information sharing policy and procedures for that particular operation based on CCDR guidance and national policy. National Disclosure Policy-1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations,* provide policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance.

3. Enablers

Key benefits include, but are not limited to, achieving unity of effort across military operations; improving the speed and execution of decisions; achieving rapid adaptability across military operations; and improving the ability to anticipate events and resource needs, providing an initial situational advantage, and setting the conditions for success.

a. The five touchstones of information sharing are: culture, policy, governance, economics and resources, and technology and infrastructure. To enable the achievement of DOD information sharing objectives, the DODIN should:

(1) Promote and encourage sharing.

(2) Achieve an extended enterprise.

(3) Strengthen agility to accommodate unanticipated partners and events.

(4) Ensure trust across organizations.

b. Other enablers are global authentication, access control, directory services, and cloud services that provide any authorized user with common and portable identity credentials and visibility of, and access to, all appropriate operational, business support, or intelligence-related information, services, and applications related to their mission and communities of interest.

c. Proper use of information helps create SA as the basis for a decision and directs and coordinates actions in the execution of the decision. This information may be traditional (e.g., storyboards, presentations, voice) or shared machine-to-machine between systems or applications. A fully networked joint force enables shared SA among DOD components, all levels of USG, multinational partners, and the private sector.

d. DODIN operations enable effective information sharing. Integration of DODIN operations-essential tasks must be performed at the strategic, operational, and tactical levels and across all DOD military, intelligence, and business areas of interest to be successful. The J-6 must manage the entire network within the operational area and be cognizant of the performance of those portions of the DODIN outside of the operational

area that affect the information needs of the joint force. The three objectives of DODIN operations are:

(1) **Assured System and Network Availability.** The purpose is to provide visibility and control over system and network resources. Resources are effectively managed and problems are anticipated and mitigated. Proactive actions are taken to ensure the uninterrupted availability and protection of system and network resources. This includes providing for graceful degradation, self-healing, fail over, diversity, and elimination of critical failure points.

(2) **Assured Information Confidentiality.** The purpose is to provide a system that secures and authenticates the information passing over networks from the time it is created, stored, and cataloged until it is distributed to the users, operators, and decision makers, so that it is not disclosed to unauthorized recipients.

(3) **Assured Information Integrity.** The purpose is to provide accurate and complete information to users, operators, and decision makers in a timely manner. The networks are continuously monitored to ensure information is transferred with the correct response time, throughput, accuracy, and performance that meet user needs.

4. Other Information Considerations

a. **Information and Communications Technology.** Growing numbers and types of networked devices increase the "threat surfaces" in cyberspace. The coming years will see an increase in the number of smart devices and sensors connected to WANs. Since every device represents a potential vulnerability, this trend represents an exponential growth of targets through which a threat could access friendly force operational networks, systems information, and mission dependencies. Likewise, reliance on mobile technologies will continue to rise, with their portability potentially extending the threat surface beyond traditional boundary protections. Cybersecurity measures must keep pace with these technology trends.

b. **Insider Threat Mitigation.** Due to continued high-profile information protection failures, the JFC should take actions to better safeguard information and deter and detect malicious insider activity on the DODIN and within the joint force HQ. Safeguarding the physical workplace, information, and network systems is the responsibility of all personnel and requires daily vigilance, as well as attention and adherence to long-standing policies. The combined efforts of personnel and security measures in place, both on the network and in deterring and detecting anomalous workplace behavior, are essential to mitigating the insider threat.

c. **IC.** Intelligence provides threat assessments that are crucial to force protection and military operations for homeland defense. The timely horizontal integration and sharing of intelligence and appropriate law enforcement information among CCMDs, interagency members, and multinational partners are vital to this effort. To attain its desired end state, DOD works with DHS, the Department of the Treasury, and the Department of Justice to

arrive at a single, coherent security policy and architecture that includes personnel security policies and practices and supporting information technologies. Of particular importance to force protection is the timely sharing of counterintelligence, key leader engagement information, law enforcement information, and other actionable intelligence. Additionally, the IC provides for the integrated defense of IC systems and networks (e.g., JWICS) through the IC Security Coordination Center.

Intentionally Blank

CHAPTER V
COMMUNICATIONS SYSTEM SUPPORT TO THE PRESIDENT, THE SECRETARY OF DEFENSE, AND THE INTELLIGENCE COMMUNITY

1. National Military Command System

a. The NMCS is a system of critical command centers, C2 nodes, and underlying support systems that are a priority component of the DODIN. It is designed to support the President, SecDef, CJCS, and other senior leaders in the exercise of their responsibilities through the range of military operations. The NMCS provides the means by which the President and SecDef receive warning and intelligence that underpin accurate and timely decision making. Additionally, it provides the means by which national leaders apply the resources of the Services, assign military missions, and communicate strategic direction to CCDRs or other commanders as necessary.

b. The communication of warning and intelligence from all sources and the dissemination of decisions and commands to military forces require the NMCS to be responsive, reliable, and survivable. An enduring command structure with survivable systems is both required and fundamental to NMCS continuity of operations to ensure the integrity of national-level decision making and force execution under any condition.

c. The CJCS oversees and operates the NMCS and defines the scope of NMCS operations to meet national leadership requirements. Mobile and fixed NMCS C2 centers are continuously staffed and ready for use, linked by the DODIN and supported by warning and intelligence systems. Special capabilities within the DODIN provide for communications with strategic offensive and defensive forces and for other multinational forces that may be required for quick reaction in crises. In this case, the communications system will be designated and operated to ensure minimum elapsed time for the transmission of orders to the operating units of these forces. The NMCS also includes infrastructure connecting NMCS centers with primary and alternate command centers and interfaces with other Executive Branch departments and agencies. This construct provides effective interagency coordination necessary to address any event on a national or global scale.

2. Nuclear Command and Control System

a. The Nuclear Command and Control System (NCCS) comprises the critical core NMCS capability that enables the President to consult with SecDef, the CJCS, CCDRs, and other advisors to assess the scope and intent of a threat and direct the transfer, deployment, employment, recall, or termination of US nuclear weapons. General operational responsibility for the NCCS lies with the CJCS and is centrally directed through the Joint Staff.

b. The NCCS supports peacetime operation of nuclear forces and provides assured, unbroken connectivity between the President and the strategic deterrent forces. This

includes situation monitoring, decision making, force direction, force management, and planning functions.

3. Intelligence

a. The DODIN enables intelligence and operations information producing a common operational picture; facilitating interoperability between Service information systems; and providing assured, secure, and tailorable information. The DODIN provide the basic framework for timely dissemination of information and fused intelligence to commanders and key decision makers. The DODIN allows data collections to be communicated directly to an authorized user or processing site or platform by the most efficient path transmitted to the user as appropriate. A critical aspect of the information network is its ability to make all intelligence accessible including direct connectivity by appropriate communications system or communications relay link (landline, radio, satellite, and others as appropriate) and broadcast capability.

b. The intelligence portion of the DODIN is designed to provide an architecture that can be individually tailored to the specific needs of a joint force, ensures survivability and flexibility through distributed operations, and can be rapidly reconfigured and recovered to accommodate changing demands and responsibilities. Although intelligence organizations use a variety of sensors and other information sources to collect and analyze data and produce intelligence products, the communications system support to intelligence is normally limited to providing the communications interface and transport media required to move intelligence and related information. However, new systems and emerging requirements for terrestrial, airborne, and space communications systems will provide additional opportunities for convergence of the intelligence communications system with the DODIN.

c. **Intelligence Communications Planning**

(1) Communications system planning for intelligence must be effectively coordinated between the J-2 and the J-6. An important consideration is the management of information transmitted over communications paths. JFCs must consider intelligence requirements when prioritizing information dissemination in terms of the product, available communications paths, and time sensitivity of the product.

(2) During dissemination and integration, intelligence is delivered to and used by the consumer. The means must be determined by the needs of the user and the implications and criticality of the intelligence. Diversity of dissemination paths (e.g., network access to computer databases, direct data transfers, web pages) requires communications and computer systems interoperability among joint and multinational forces, component commands, DOD organizations, and interagency partners.

(3) A wide range of national, theater, and component intelligence and communications systems is available to a JFC. The existence of the various capabilities requires that these systems be deployed with significant planning and coordination. The

CCMD J-2 and J-6 must integrate the architecture of intelligence sensors, processors, dissemination systems, databases, in the information communications systems. Key concepts to successful intelligence systems support are joint interoperability, streamlined flow of information, and providing push and pull-down of intelligence tailored to the needs of the operating forces.

(4) JP 2-01, *Joint and National Intelligence Support to Military Operations,* identifies a methodology for effective intelligence communications planning. Step 1: J-2 identifies the type of mission, specific mission requirements, and threat's cyberspace attack capabilities; Step 2: J-2 determines specific intelligence communications support plan in the operational area; Step 3: J-2 compiles the information and intelligence that flows from step 2 into a node-to-node layout of intelligence information transactions; and Step 4: J-6 determines the communications support plan for the requirements identified in the node-to-node layout of step 3. The communications support plan should set up adequate communications for the JFC and/or subordinate joint force intelligence needs prior to deployment. The J-2 coordinates support from the J-6 for the communications system, including COMSEC, application software, and bandwidth. By the end of the planning, the J-2 and J-6 identify the frequencies, communications protocols, network security management requirements, encryption devices, and procedures for the architecture components.

d. **Department of Defense Intelligence Information System (DODIIS)**

(1) DODIIS is the aggregation of personnel, procedures, equipment, computer programs, and supporting communications of the military IC. DODIIS defines the network standards for intelligence system and application interoperability. It supports the timely and comprehensive preparation and presentation of information and intelligence to military commanders and national-level decision makers. DIA implements and manages the configuration of information, data, and communications standards for DOD intelligence systems and for IC systems that interface with, or directly support, DOD. As such, DIA establishes defense-wide intelligence priorities for achieving interoperability between the tactical, theater, and national intelligence systems and the respective communications system at each level.

(2) The DODIIS provides the interface between the CCDRs and the IC. The joint intelligence systems architecture is an integral part of the joint communications architecture and consists of an integrated network supporting voice, data, and VTC. JWICS, the Joint Deployable Intelligence Support System, and the Distributed Common Ground System are foundational elements of the SCI DODIIS. This interface consists of more than the SCI networks. DODIIS also provides the interfaces between the JWICS SCI IC systems and the SIPRNET IC systems. It is through this interface that much of the real-time intelligence gathered by the CCDRs is passed up into the national IC systems and the national intelligence products are passed back down to the CCDRs. Additionally, this interface extends multinational networks that are essential in today's missions. The DODIIS has evolved into an enterprise consisting of mission applications, communications services, and user equipment consolidated under centralized management to better serve

the CCDRs and provide more responsive intelligence. This consolidation is shaped around an enterprise approach using regional service centers. The globally linked regional service centers provide the foundation and interface for data to be managed as a single enterprise entity transparent to the users. Data will reside on, or be accessible through, the enterprise that connects the policy makers, analysts, planners, and decision makers in support of the joint force.

4. National Security and Emergency Preparedness Communications

a. DHS Office of Emergency Communications leads the national security and emergency preparedness (NS/EP) communications efforts and the office programs and services coordinate emergency communications planning, preparation, and evaluation to ensure safer, better-prepared communities nationwide. SecDef oversees the development, testing, implementation, and sustainment of NS/EP communications that are directly responsive to the national security needs and communication with or among the President, Vice President, senior national leadership, White House staff, heads of state and government, and nuclear C2 leadership; continuity of government communications; and communications among the executive, judicial, and legislative branches to support an enduring constitutional government. See Figure V-1.

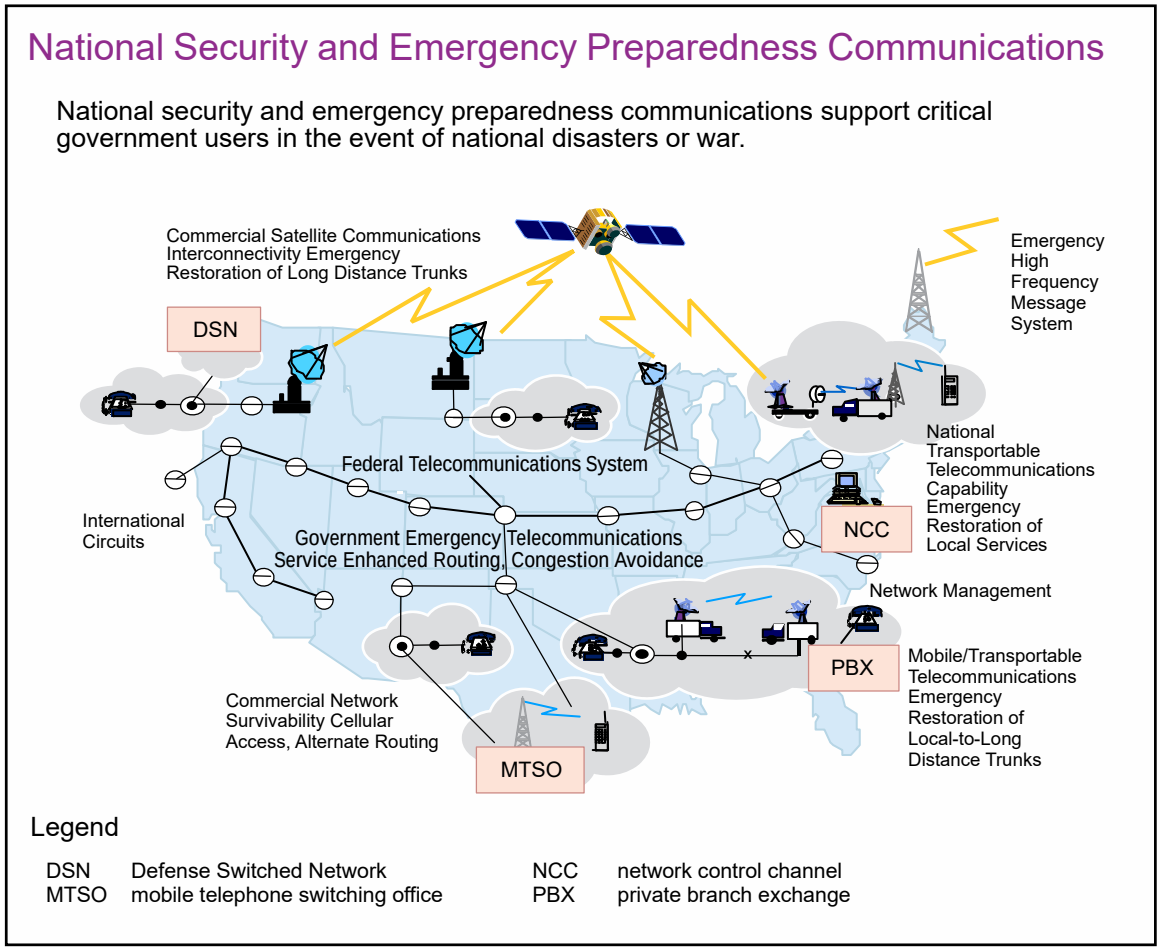


Figure V-1. National Security and Emergency Preparedness Communications

b. The addition of competitive service providers with multiple points of contact within industry for planning and service provisioning has complicated the means for satisfying NS/EP telecommunications requirements. The Joint Staff J-6 coordinates with the NS/EP Executive Committee.

Intentionally Blank

APPENDIX A
DEPARTMENT OF DEFENSE INFORMATION NETWORK TELECOMMUNICATIONS INFRASTRUCTURE COMPONENTS

DODIN is made up of several telecommunications components that provide key services:

1. Access Services

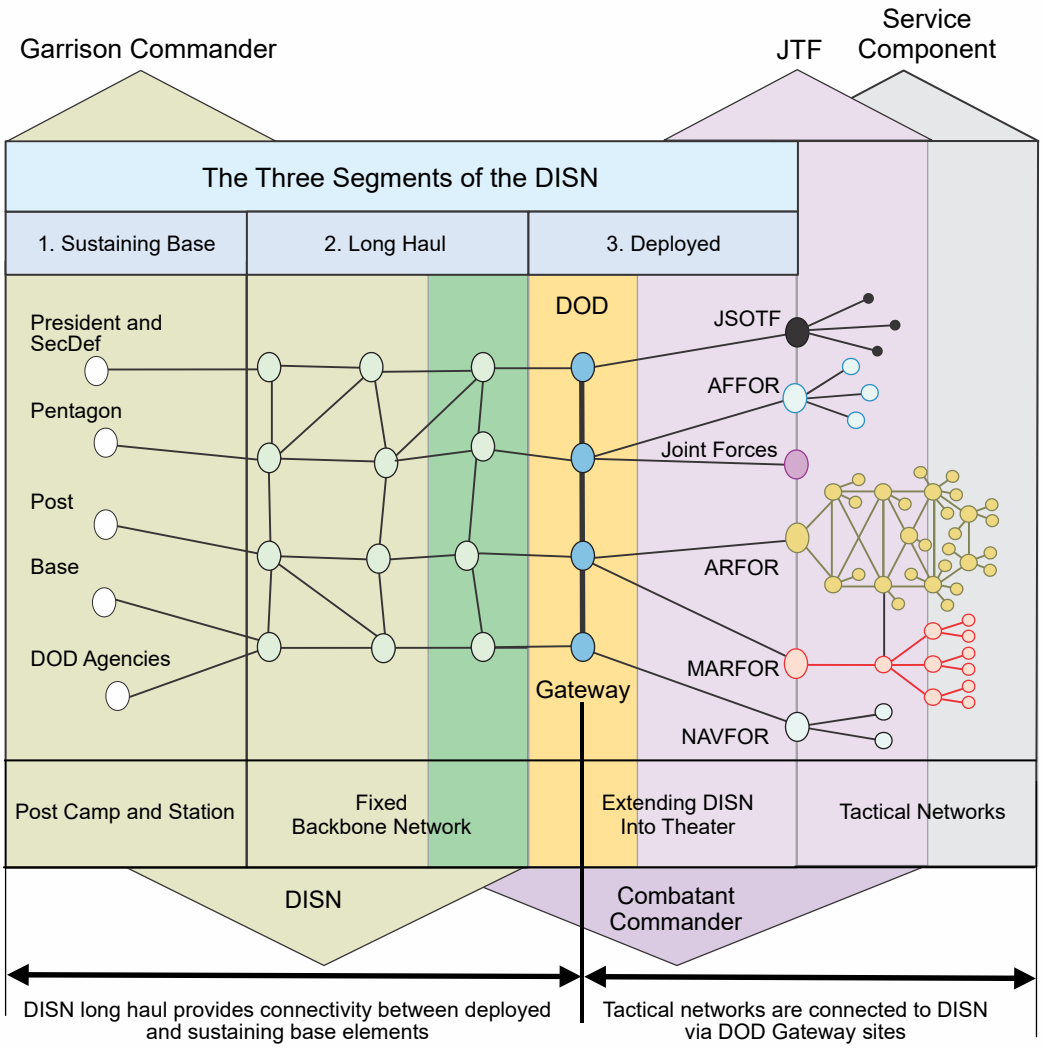
a. **DISN Interface.** The DISN is the major element of the DODIN (see Figure A-1). It has three segments: sustaining base, long haul, and deployed. It is DOD's worldwide enterprise-level telecommunications infrastructure providing end-to-end information transfer for supporting military operations. For the most part, it is transparent to the joint force. The DISN facilitates the management of information resources and is responsive to national security, as well as DOD, needs. It provides basic DODIN services to DOD installations and deployed forces. Those services include voice, data, and video, as well as ancillary enterprise services such as directories and messaging. DOD policy mandates the use of the DISN for WAN and metropolitan networks.

b. **DOD Gateway.** In concert with military and commercial communications segments that support DOD missions, the primary interface point between the sustaining base and deployed forces is called the DOD Gateway. The DOD Gateway includes the standardized tactical entry point. The Teleport upgrade, at the six core and two secondary SATCOM facilities, provide joint forces access to the gateways for the six DISN services: SIPRNET, NIPRNET, Defense Red Switch Network, Defense Switched Network, VTC, and JWICS. The DOD Gateway is designed to meet the requirement of the provisioning of pre-positioned, sustainable DISN services.

(1) The DOD Gateway program enhances the ability of the DISN to respond to the needs of the joint force. Joint and Service-level operational users rely on both military and commercial SATCOM systems to support their communications requirements. The DOD Gateway provides predefined (tailored) support packages on a predefined timeline. This support is extended via common-user transports and includes voice, data, and video services. These services are extended directly to deployed naval forces and to each component of a JTF, if employed. Voice services include access to the Defense Switched Network, and the Defense Red Switch Network Data will include access to SIPRNET and NIPRNET. Video services include access to DISN Video Services. The DOD Gateway will also support JWICS, an SCI-level data, voice, and video services network.

(2) Although the DOD Gateway is implemented globally, JFCs and their staffs play an important role in DOD Gateway employment. Entry point access and procedures are coordinated by the tactical communications system planners. DISA plays a major role in the planning process and utilizes regional contingency exercise planning branches and USCYBERCOM-operated JOC and DISA's DODIN operations center to facilitate that interaction with the joint force. DOD Gateway (see Figure A-2) has evolved to incorporate

Defense Information Systems Network Interface



Legend

AFFOR	Air Force forces	JTF	joint task force
ARFOR	Army forces	MARFOR	Marine forces
DISN	Defense Information Systems Network	NAVFOR	Navy forces
DOD	Department of Defense	SecDef	Secretary of Defense
JSOTF	joint special operations task force		

Figure A-1. Defense Information Systems Network Interface

satellite connectivity through the Teleport program. This provides greater flexibility in the use of DOD and commercial SATCOM resources. Flexibility, in this sense, does not imply additional bandwidth for the deployed joint force. However, use of quad-band terminals provides the joint force with more flexible means of SATCOM support.

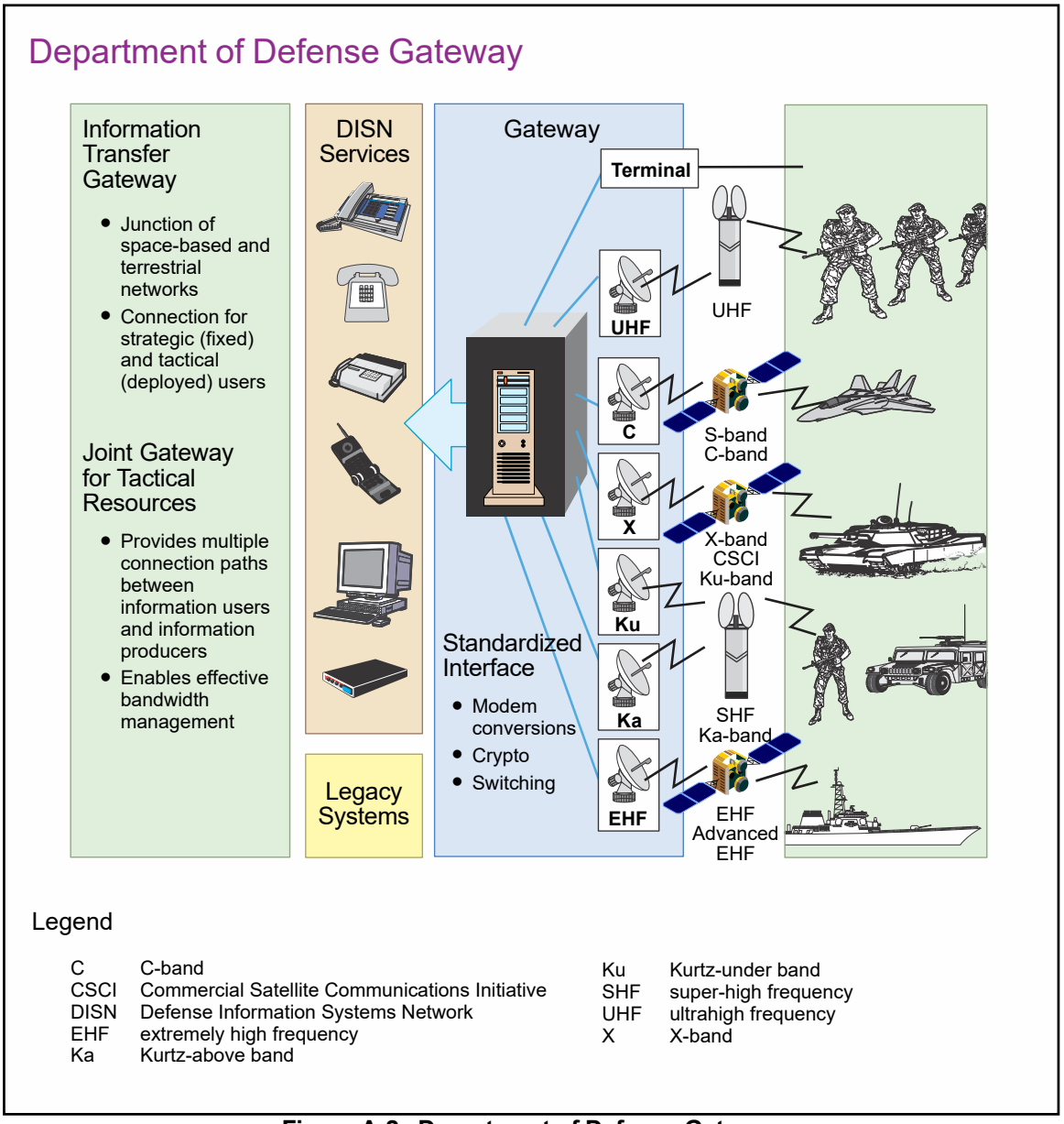


Figure A-2. Department of Defense Gateway

c. The DOD Teleport Program is an upgrade of satellite telecommunication capabilities at selected DOD gateways to improve DISN service access to the deployed joint force.

2. Voice Services

a. **Defense Switched Network.** A standard unclassified voice network supporting DOD.

b. **Defense Red Switch Network.** A classified voice network supporting DOD.

c. **Enhanced Mobile Satellite Services** (e.g., International Maritime Satellite/Iridium Satellite). Commercial, portable satellite systems capable of voice and data transmission.

d. **Tactical Voice.** Military specific switching system capable of operating in austere areas.

e. Voice over Internet protocol and voice over secure Internet protocol services.

3. Communications Services

a. **NIPRNET.** An information network for unclassified information supporting DOD.

b. **SIPRNET.** An information network for classified information (up to Secret) supporting DOD.

c. **JWICS.** An information network for classified information (up to Top Secret), including SCI, supporting DOD, the IC, and other USG departments and agencies.

d. **Multinational WAN.** An information network supporting the multinational operations that may be unclassified or classified.

e. The joint data network (JDN) carries tactical data link (TDL) and multi-sensor early warning information in support of joint operations. Information is generally passed over the JDN in near real time. The JDN consists of the multi-TDL network, ground network, intelligence network, and sensor network, along with other feeds. Effective design and implementation of the multi-TDL network are critical in managing complexities to improve the JFC's ability to engage hostile forces and prevent friendly fire.

4. Functional Services

The Global Command and Control System-Joint (GCCS-J), the Global Adaptive Planning Collaborative Information Technology Environment (GAP CITE), the theater battle management core system (TBMCS), DOD enterprise collaboration service, and the DISA organizational messaging service discussed in the following paragraphs are illustrative of applications.

a. GCCS is DOD's IT-based system of record for C2 functions. GCCS-J enables the joint force to plan, execute, and manage military operations. The system helps JFCs synchronize the actions of air, land, maritime, space, cyberspace, and special operations forces. It has the flexibility to be used in a wide range of operations, from actual combat to humanitarian assistance. GCCS-J provides CCDRs a complete picture of the operational environment and the ability to order, respond, and coordinate communications system information. GCCS-J is a comprehensive automated communications system designed to improve the JFC's ability to manage and execute joint operations. GCCS-J is interoperable with Service and agency communications systems, providing a global network of military

and commercial communications systems the JFC uses to send and obtain critical information. GCCS-J supports the exchange of information from the President/SecDef to CCDRs and their components. GCCS-J incorporates procedures, reporting structures, automated information systems, and communications connectivity to provide the information necessary to effectively plan, deploy, sustain, employ, and redeploy forces.

b. **GAP CITE** is an operational application used for US Strategic Command mission planning. GAP CITE includes a visual support tool called the Global Situational Awareness Tool, Command Dashboard and Daily Brief capability for SA, orders and messages collaborative functionality, and a configurable assessment tool. GAP CITE resides on SIPRNET and JWICS and has a SIPRNET-releasable capability.

c. **TBMCS** is used by the joint force air component commander and other component commanders to collaboratively plan, direct, and control joint air operations in support of JFC objectives. This automated system facilitates the development, deconfliction, dissemination, and execution of the air operations plan, air tasking order, airspace control order, and air defense tactical operations data message and supports collaborative target management. The system provides full support to force-level and unit-level joint forces throughout all phases of military operations and is interoperable with other DODIN systems, to include GCCS family of systems and GCSS-J/Command and Control Integrated Planning System. TBMCS is used by the US Air Force, US Navy, and US Marine Corps.

d. Current **DOD enterprise collaboration service** enables CCMDs, Services, and agencies with real-time virtual collaboration capability using instant messaging, low-bandwidth text chat, and web conferencing. Instant messaging and web conferencing both include text-based communications, while web conferencing adds shared whiteboards, desktop and application sharing, and the ability to invite non-DOD personnel into collaboration sessions.

e. The **DISA** organizational messaging service provides the Services, CCMDs, DOD agencies, USG departments and agencies, and the IC with the ability to exchange official information between organizations and to support interoperability in the strategic/fixed-base and the tactical/deployed environments.

5. Applications

a. **Defense VTC System—(Global).** An unclassified or classified (e.g., secure VTC), closed video network capable of voice, image, and data exchange supporting C2 functions of DOD. It utilizes industry standard technology for robust interoperability to commercial systems as well as legacy DOD systems.

b. **SCI-Level VTC.** A classified, closed video network capable of voice, image, and data exchange supporting intelligence and C2 functions. (Note: SCI VTC is typically carried over JWICS.)

c. **Commercial News Feed.** Commercial news feeds may be rebroadcast over the DOD communications system or received via a commercially leased terminal in support of C2 functions.

6. Aerial Layer

The aerial layer provides additional communications capacity by using manned and unmanned systems to host communications packages for continuous communications coverage of large geographic areas. The aerial layer integrates with the space and terrestrial network segments to enable advanced information exchange capabilities.

APPENDIX B
JOINT FORCE COMMUNICATIONS SYSTEM PLANNING GUIDE

1. General

This appendix provides communications system planners with an outline to assist planning.

2. Situation

The JFC has received a planning directive (e.g., CCDR's warning order, planning order). Normally, the joint planning group has been assembled, and the planning of an operation is ongoing. The J-6 develops the communications system estimate by identifying, coordinating, and integrating communications system support.

3. Developing the Communications System Estimate Analysis

The J-6 should:

a. Determine known facts, status, or conditions of communications system elements provided in the commander's planning guidance document (e.g., warning order, planning order, or alert order).

b. Understand the CCDR's mission and proposed operations/tasks to components.

(1) Mission assigned to the CCDR.

(2) Required objectives.

(3) Actions required to achieve objectives.

(4) Location of required objectives.

(5) Timing of required objectives.

(6) Operational limitations.

c. Review and describe the communications system situation.

(1) Characteristics of the operational area; emphasize factors affecting communications system activities.

(2) Adversary capabilities. Place specific emphasis on communications system matters.

(3) Friendly forces.

(a) Disposition (positions) of major units that have been provided by the CCMD for planning.

(b) Own COAs. State the proposed COAs under consideration.

(c) Probable operations/tactical developments. Review major deployments and communications system preparations necessary in all phases of the proposed campaign/major operation.

(4) The logistic situation. Review known logistic problems that may affect the communications system situation.

(5) The personnel situation. Review known or anticipated personnel problems that may influence the communications system estimate and the selection of a specific COA. Consider the requirement for and availability of JCSE support.

(6) Special features. Special aspects not covered elsewhere that may affect the communications system situation, such as the HN and its ability and willingness to allow access to/operation of communications system assets or the effects of scintillation on long-haul communications.

(7) Communications system. Consider line-of-sight communications, SATCOM, ground mobile segment, and DISN interface. Review all military, multinational partner, and commercial options.

(a) Administrative communications.

(b) Logistics and medical communications.

(c) Intelligence communications architecture.

(d) COMSEC.

(e) Communications support for combat operations:

1. Joint air operations.

2. Air-to-ground operations.

3. Naval surface fire support.

4. Other component-specific communications system.

(f) Communications control and aids for supporting operations.

(g) Interoperability of the communications system, both horizontally and vertically.

(h) Communications required for other activities (e.g., VTC).

(i) Threat and vulnerability assessment of the communications system and cyberspace.

d. Understand the deception guidance—objective, target, story, if any.

e. Understand the guidance on risk, if any.

f. Understand the desired end state.

g. Consider factors affecting communications.

(1) The topography in the operational area.

(2) The available communications resources.

(3) The communications readiness of available forces.

(4) EMS access and availability.

h. Determine limitations

(1) Restrictions placed on the JFC.

(a) Constraints. Required actions that limit freedom of action (e.g., conduct air strikes within a specific period of time).

(b) Restraints. Actions the JFC is prohibited from taking (e.g., cannot pursue the enemy forces across an international border).

(2) Imposed by higher HQ, HN, multinational force.

(3) Implied by conditions, circumstances—may be described as assumptions.

i. Develop assumptions to replace missing or unknown information. Assumptions must be valid (likely to occur) and essential for continued planning (e.g., sufficient satellite channels/bandwidth availability).

(1) Intelligence related assumptions. See the J-2.

(a) Impact of characteristics of the operational area.

(b) Enemy intentions, probable COAs, vulnerabilities.

(c) Status of friendly support.

(2) Operationally related assumptions.

(a) Status of forces at probable execution.

(b) Probability of success after the force ratio analysis.

(c) Available time.

(3) Logistic-related assumptions. See the logistics directorate of a joint staff (J-4).

(a) Logistic status of forces at probable execution.

(b) Logistic impact of characteristics of the operational area.

(c) Acquisition plan for extraordinary material and services.

(4) Communications/computer-related assumptions.

(a) Communications status at probable execution.

(b) Determine national/theater-level communications support in coordination with the CCMD J-6.

4. Receive the Joint Force Commander Planning Guidance

The JFC should provide detailed guidance at this point. Planning guidance should be disseminated to J-6 personnel and the joint force components. If needed, ask the J-3/plans directorate of a joint staff/JFC for any guidance necessary for continued planning.

5. Develop Options for Communications System Support of the Joint Force Commander's Courses of Action

a. Use analytical models or databases to determine requirements and the communications system architecture.

b. The J-6 should:

(1) Review the mission analysis and the commander's guidance and intent.

(2) Develop options for communications system support for each COA.

(a) Clearly state what is to be accomplished, including phasing of communications system support to the campaign or operation.

(b) Outline communications system support to the military deception objective and story.

(c) Specify ways (operations) and means (forces) to provide communications system support to accomplish objectives (e.g., attacking adversary centers of gravity).

(d) Outline the major communications system tasks to be performed to support the JFC, including the supporting/supported relationships by phase, and tasks to be accomplished by the supporting organizations and agencies.

(e) Outline the deployment scheme for communications system resources.

(3) Identify force requirements for communications system support.

(4) Describe C2 means and relationships for communications system support.

6. Participate in the Course of Action Analysis (Wargaming)

The J-6 should:

a. Gather tools.

(1) Identify the enemy and friendly COAs to analyze.

(2) Prepare maps of the operational area with communications system information.

(3) Join the wargaming team—normally representatives from J-2, J-3, J-4, and J-6.

(4) Depict current enemy dispositions.

b. Identify the available joint forces and augmentation from:

(1) USCYBERCOM (e.g., CO-IPEs, cyberspace mission forces).

(2) US Strategic Command (e.g., space support team, regional satellite support center).

(3) US Transportation Command (e.g., JCSE).

(4) DISA.

c. List assumptions related to communications system support.

d. Review and/or contribute to the development of known critical events and decision points—specified and implied tasks and decisions that must be made to ensure timely execution and synchronization of resources.

e. Review or contribute to selecting the wargame method. Generally use the action/reaction/counteraction sequence and assessment.

f. Participate in wargaming.

(1) Provide a perspective on communications system requirements related to friendly operations.

(2) Determine communications system objectives and integrate communications system support within the context of the COA under consideration.

(3) Identify potential adjustments to the required friendly force deployment to ensure communications system resources for the COA under consideration.

(4) Contribute refinements or modifications to the COAs and to the concepts for communications system support.

(5) Contribute to branches, sequels, or additional critical events—additional operations that might be required as a result of enemy actions not previously anticipated.

(6) Contribute to critical information.

(7) Contribute to COA(s) for the associated military deception plan.

(8) Identify major communications system tasks to the Service/functional components.

(9) Estimate the duration of communications system support requirements.

(10) Identify major requirements for communications system support of operations.

(11) Develop communications system input/information for the synchronization matrix and decision support template.

(12) Identify advantages, disadvantages of friendly COAs from the J-6 perspective of supportability.

g. Repeat for all combinations of enemy and friendly COAs.

7. Participate in the Course of Action Comparison

The J-6 tests the validity of each COA.

a. Test for suitability.

(1) Does it accomplish the mission?

(2) Does it meet the commander's intent?

(3) Does it accomplish all the essential tasks?

(4) Does it meet the conditions for the end state?

(5) Does it take into consideration the enemy and friendly centers of gravity?

b. Test for feasibility.

(1) Does the JFC have the force structure (means) to carry it out? The COA is feasible if it can be carried out with the forces, support, and technology available, within the constraints of the physical environment and against the expected enemy opposition.

(2) Although this process occurs during COA analysis and the test at this time is preliminary, it may be possible to declare a COA infeasible (e.g., resources are obviously insufficient). However, it may be possible to fill shortfalls by requesting additional support through the geographic combatant command.

c. Test for acceptability.

(1) Does it contain unacceptable risks?

(2) Does it take into account the limitations placed on the JFC (constraints [must do] and restraints [cannot do])? A COA is considered acceptable if the estimated results are worth the estimated costs. The basis of this test consists of an estimation of friendly losses in forces, time, position, and opportunity.

(3) Acceptability is considered from the perspective of the JFC and the CCDR, by reviewing the JFC's contribution to the CCDR's objective.

(4) COAs are reconciled with external restraints, particularly rules of engagement.

(5) Requires visualization of execution of the COA against each adversary capability. Although this process occurs during the COA analysis and the test at this time is preliminary, it may be possible to declare a COA unacceptable if it violates the JFC's definition of acceptable risk.

d. Test for differences or variety. Is it fundamentally different from other COAs? They can be different when considering:

(1) Focus or direction of the main effort.

(2) Scheme of maneuver.

(3) Primary mechanism for mission accomplishment.

(4) Task organization.

(5) Use of reserves.

e. Test for completeness. Does it answer the questions who, what, when, where, why, and how?

f. Provide forces and deployment requirements to the joint force deployment cell.

g. Provide conclusions.

(1) State whether the JFC's mission is supportable from a J-6 perspective.

(2) State which COA can best be supported from a J-6 standpoint.

(3) Identify the major communications system deficiencies and make recommendations to reduce or eliminate them.

(a) Are JCSE or other nonorganic capabilities required?

(b) Are en route communications required?

h. Ensure recommendations are coordinated with the J-6-equivalent at each Service/functional component and the supported CCMD J-6.

i. Recommend a COA from the J-6 perspective.

8. Receive the Joint Force Commander's Decision on the Course of Action

The JFC may select or modify the recommended COA. Based on that decision, the JFC's estimate document (or slides) will normally be sent or briefed to the supported CCDR for approval.

9. Prepare and Submit Annex K (Command, Control, Communications, and Computer Systems) to the Joint Force Plan/Order

Paragraphs 3-8 above contain most of the information needed to complete annex K. The J-6 should:

a. Identify the communications system functions required to support the proposed joint operation.

(1) Collect information based on the stated need and convert that information into the required format for annex K (Command, Control, Communications, and Computer Systems).

(2) Coordinate, as necessary, with the CCMD J-6 and the J-6-equivalents at the Service/functional components.

(3) Provide the information/annex K to the focal point for the OPLAN/OPORD, normally the joint planning group.

(4) Disseminate essential information regarding communications system and networks throughout the joint force, as required.

(5) Plan all active and passive communications system support related security measures to deny the enemy access to friendly information (e.g., COMSEC, cybersecurity).

(6) Coordinate, synchronize, and deconflict annex K with DODIN operations specific language in appendix 16 (Cyberspace Operations) to annex C (Operations).

b. Identify applicable planning guidelines/principles for the communications system support. Consider:

(1) The integration of organic and nonorganic military and commercial communications systems, so the interfaces are transparent and the systems reliable.

(2) Horizontal and vertical C2 linkages.

(3) A balance between "push" and "pull" systems to meet the information needs of the joint force.

(4) Planning considerations.

(a) Modular communications system packages.

(b) Interoperable procedures, training, and equipment permitting internal and external exchange of information.

1. What interfaces are required for multinational forces?

2. Can the Joint Interoperability Test Command assist with potential interoperability solutions?

(c) Using liaison officers/teams to facilitate interoperability.

(d) The flexibility to allow for changes in mission or to accommodate a diversity of communications schemes and equipment.

(e) Balance the need for redundancy and flexibility with the available assets.

(f) Survivable communications system architecture should include diverse communications routes, hardening and protection of equipment and communications sites, and availability of alternate modular communications system packages.

(g) Redundancy that provides diverse paths over multiple media means, with available replacement systems and repair parts.

(h) Use of available commercial networks.

1. What special interfaces are required?

2. What are the power requirements?

3. Are additional funds required?

(i) EMS assessment, deconfliction, and allocation to prevent harmful EMI. Necessary coordination with the HN for final analysis and approval via established venues. Protection of the most critical communications C2 systems through coordination and distribution of a JRFL.

(j) Security must account for users' information requirements, the vulnerability of communications system to interception, exploitation, disruption, and destruction by the adversary.

(k) Adherence to cybersecurity principles and policy must be included to minimize the danger posed by malware, hackers, and other cyberspace threats.

(l) Relevant lessons learned and best practices identified during activities in comparable operational environments.

c. Consider equipment and system characteristics necessary for proposed operations. The communications system should be designed to be interoperable, agile, trusted, and shared.

d. **Refine the concept of communications system support**

(1) Determine/refine IERs.

(a) Should be based on the consolidated requirements of the JFC.

(b) Consider communications system support to other operations/functions (e.g., military deception, military information support operations, fire support systems, airspace management, air defense).

(c) Consider the battle rhythm of the staff, reporting times, and times of critical planning meetings.

(2) Match IERs with communications system capabilities and assets.

(3) Conduct communications system planning and engineering. Design the communications system architecture.

(a) Use automated planning tools.

(b) Define the architecture in terms of communications system nodes and associated communications system, grouped into modular packages keyed to phases and deployment schedules.

(c) Describe the interconnection of modular packages to communications system and the resulting communications system networks. Compare results with mission phases and deployment schedules.

(d) Include description of supporting control centers, technical control centers, and technical control facilities.

(e) Upon validation of the requirements, input applicable information to the joint force point of contact for the TPFDD for forwarding to the supported CCMD.

(4) Program the activation of communications system links and networks.

(5) Plan for management of the EMS through CCMD JEMSOC.

(a) Ensure a trained spectrum manager is available/assigned to JEMSOC with necessary tools and resources.

(b) Use existing allocations and allotment plans, if available. ICW JFMO know HN's restrictions.

(c) Ensure systems are spectrum-supportable and certified.

(d) Plan and request an EMS survey as part of the predeployment site survey, if feasible.

(e) Develop appropriate JCEOI.

(f) As part of JEMSOC, assist in the development of the JRFL.

(6) Plan for security of communications system and networks.

(a) Transmission security.

(b) Cryptographic security.

(c) Emission security.

(7) Coordinate plan with meteorology and oceanographic observations.

e. Prepare and submit annex K (Command, Control, Communications, and Computer Systems) to the OPLAN/OPORD.

(1) Coordinate with the necessary divisions/branches to develop appendices to support annex K.

(2) Use available automated planning/annex preparation tools.

APPENDIX C
POINTS OF CONTACT

Joint Staff/J-7/Joint Doctrine Division
Website: http://www.jcs.mil/doctrine/
E-mail Support: js.pentagon.j7.jedd-support@mail.mil
Phone number: 1-703-692-7276 (DSN 222)

Joint Staff Doctrine Sponsor/J-6
Phone number: 1-757-203-8533

Intentionally Blank

APPENDIX D
REFERENCES

1. General

a. Presidential Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans.*

b. *Intelligence Community Authorized Classification and Control Markings, Register, and Manual.*

c. National Disclosure Policy-1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations.*

d. National Security Presidential Directive-54/Homeland Security Presidential Directive-23, *(U) Cybersecurity Policy.*

e. *National Strategy for Information Sharing and Safeguarding.*

2. Department of Defense Publications

a. DODD 3020.40, *Mission Assurance (MA).*

b. DODD 5105.19, *Defense Information Systems Agency (DISA).*

c. DODD 5105.77, *National Guard Bureau (NGB).*

d. DODD 5144.02, *DOD Chief Information Officer (DOD CIO).*

e. DODD S-5210.81, *(U) US Nuclear Weapons Command and Control, Safety, and Security.*

f. DODD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations.*

g. DODD 5530.3, *International Agreements.*

h. DODD 8000.01, *Management of the Department of Defense Information Enterprise (DOD IE).*

i. DODI 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum.*

j. DODI 5000.02, *Operation of the Defense Acquisition System.*

k. DODI 5015.02, *DOD Records Management Program.*

l. DODI 8170.01, *Online Information Management and Electronic Messaging*.

m. DODI 8320.02, *Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense.*

n. DODI 8320.05, *Electromagnetic Spectrum Data Sharing.*

o. DODI 8330.01, *Interoperability of Information Technology (IT), Including National Security Systems (NSS).*

p. DODI 8410.03, *Network Management (NM).*

q. DODI 8420.02, *DOD Satellite Communications (SATCOM).*

r. DODI 8500.01, *Cybersecurity.*

s. DODI 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT).*

t. DODI 8523.01, *Communications Security (COMSEC).*

u. *Department of Defense Information Sharing Strategy.*

3. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 2700.01G, *Rationalization, Standardization, and Interoperability (RSI) Activities.*

b. CJCSI 3110.10F, *(U) Communications Supplement to the Joint Strategic Capabilities Plan (JSCP).*

c. CJCSI 3150.25G, *Joint Lessons Learned Program.*

d. CJCSI 3155.01B, *Global Command and Control System-Joint (GCCS-J) Operational Framework Policy.*

e. CJCSI 3265.01A, *Command and Control Governance and Management.*

f. CJCSI 3320.01D, *(U) Joint Electromagnetic Spectrum Operations (JEMSO).*

g. CJCSI 3320.02F, *Joint Spectrum Interference Resolution.*

h. CJCSI 3320.03D, *Joint Communications Electronics Operating Instructions.*

i. CJCSI 3401.01E, *Joint Combat Capability Assessment.*

j. CJCSI 5116.05, *Military Command, Control, Communications, and Computers Executive Board.*

k. CJCSI 5721.01E, *The Defense Message System and Associated Legacy Message Processing Systems.*

l. CJCSI 6211.02D, *Defense Information System Network (DISN) Responsibilities.*

m. CJCSI 6241.04C, *Policy and Procedures for Management and Use of United States Message Text Formatting.*

n. CJCSI 6250.01F, *Department of Defense Satellite Communications.*

o. CJCSI 6251.01D, *Narrowband Satellite Communications Requirements.*

p. CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND).*

q. CJCSI 6510.06C, *Communication Security Releases to Foreign Nations.*

r. CJCSI 6731.01C, *Global Command and Control System-Joint (GCCS-J) Security Policy.*

s. CJCSI 6740.01C, *Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations.*

t. CJCSI 8010.01C, *Joint Community Warfighter Chief Information Officer.*

u. CJCSM 3122.05, *Operating Procedures for Joint Operation Planning and Execution System (JOPES) - Information Systems (IS) Governance.*

v. CJCSM 3130.03A, *Planning and Execution Planning Formats and Guidance.*

w. CJCSM 3150.01C, *Joint Reporting Structure General Instructions.*

x. CJCSM 3150.07E, *Joint Reporting Structure for Cyberspace Operations Status.*

y. CJCSM 3150.16E, *Joint Operation Planning and Execution System Reporting (JOPESREP).*

z. CJCSM 3320.01C, *Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment.*

aa. CJCSM 3320.02D, *Joint Spectrum Interference Resolution (JSIR) Procedures.*

bb. CJCSM 6120.01G, *Joint Multi-Tactical Data Link Operating Procedures Overview.*

cc. CJCSM 6231.01E, *Manual for Employing Joint Tactical Communications.*

dd. CJCSM 6510.01B, *Cyber Incident Handling Program.*

ee. JP 1, *Doctrine for the Armed Forces of the United States.*

ff. JP 3-0, *Joint Operations.*

gg. JP 3-12, *Cyberspace Operations.*

hh. JP 3-13, *Information Operations.*

ii. JP 3-13.1, *Electronic Warfare.*

jj. JP 3-14, *Space Operations.*

kk. JP 3-16, *Multinational Operations.*

ll. JP 3-33, *Joint Task Force Headquarters.*

mm. JP 4-10, *Operational Contract Support.*

nn. JP 5-0, *Joint Planning.*

oo. JP 6-01, *Joint Electromagnetic Spectrum Management Operations.*

4. Other Publication

a. US Strategic Command Instruction 714-4, *Satellite Communications (SATCOM).*

b. Chief, National Guard Bureau Instruction, 3000.04, *National Guard Bureau Domestic Operations.*

APPENDIX E
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication using the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

a. The lead agent and Joint Staff doctrine sponsor for this publication is the Director for Command, Control, Communications and Computers/Cyber and Chief Information Officer (J-6).

b. The following staff, in conjunction with the joint doctrine development community, made a valuable contribution to the revision of this joint publication: lead agent, Mr. Thomas Bauckman, Joint Staff J-6; Joint Staff doctrine sponsor, CDR Johnny Lykins, Joint Staff J-6; Mr. Mark Brown, Joint Staff J-7, Joint Doctrine Analysis Division; and LTC Josh Darling, Joint Staff J-7, Joint Doctrine Division.

3. Supersession

This publication supersedes JP 6-0, *Joint Communications System,* 10 June 2015.

4. Change Recommendations

a. To provide recommendations for urgent and/or routine changes to this publication, please complete the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil.

b. When a Joint Staff directorate submits a proposal to the CJCS that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Lessons Learned

The Joint Lessons Learned Program (JLLP) primary objective is to enhance joint force readiness and effectiveness by contributing to improvements in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy. The Joint Lessons Learned Information System (JLLIS) is the DOD system of record for lessons learned and facilitates the collection, tracking, management, sharing, collaborative

resolution, and dissemination of lessons learned to improve the development and readiness of the joint force. The JLLP integrates with joint doctrine through the joint doctrine development process by providing lessons and lessons learned derived from operations, events, and exercises. As these inputs are incorporated into joint doctrine, they become institutionalized for future use, a major goal of the JLLP. Lessons and lessons learned are routinely sought and incorporated into draft JPs throughout formal staffing of the development process. The JLLIS Website can be found at https://www.jllis.mil (NIPRNET) or http://www.jllis.smil.mil (SIPRNET).

6. Distribution of Publications

Local reproduction is authorized, and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be IAW DOD Manual 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification,* and DOD Manual 5200.01, Volume 3, *DOD Information Security Program: Protection of Classified Information.*

7. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS Joint Electronic Library Plus (JEL+) at https://jdeis.js.mil/jdeis/index.jsp (NIPRNET) and https://jdeis.js.smil.mil/jdeis/index.jsp (SIPRNET), and on the JEL at http://www.jcs.mil/Doctrine/ (NIPRNET).

b. Only approved JPs are releasable outside the combatant commands, Services, and Joint Staff. Defense attachés may request classified JPs by sending written requests to Defense Intelligence Agency (DIA)/IE-3, 200 MacDill Blvd., Joint Base Anacostia-Bolling, Washington, DC 20340-5100.

c. JEL CD-ROM. Upon request of a joint doctrine development community member, the Joint Staff J-7 will produce and deliver one CD-ROM with current JPs. This JEL CD-ROM will be updated not less than semi-annually and when received can be locally reproduced for use within the combatant commands, Services, and combat support agencies.

GLOSSARY

PART I—ABBREVIATIONS, ACRONYMS, AND INITIALISMS

ACP	Allied communications publication
AOR	area of responsibility
C2	command and control
CCDR	combatant commander
CCEB	Combined Communications-Electronics Board
CCIR	commander's critical information requirement
CCMD	combatant command
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSPACECOM	Commander, United States Space Command
CIE	collaborative information environment
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CO	cyberspace operations
COA	course of action
CO-IPE	cyberspace operations-integrated planning element
COMSEC	communications security
CPF	Cyber Protection Force
CPT	cyberspace protection team
CSSP	cybersecurity service provider
DACO	directive authority for cyberspace operations
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations-internal defensive measures
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODIIS	Department of Defense Intelligence Information System
DODIN	Department of Defense information network
EMI	electromagnetic interference
EMOE	electromagnetic operational environment
EMS	electromagnetic spectrum
GAP CITE	Global Adaptive Planning Collaborative Information Technology Environment

GCC	geographic combatant commander
GCCS	Global Command and Control System
GCCS-J	Global Command and Control System-Joint
GCSS-J	Global Combat Support System-Joint
HN	host nation
HQ	headquarters
IAW	in accordance with
IC	intelligence community
IER	information exchange requirement
IM	information management
IT	information technology
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
J-4	logistics directorate of a joint staff
J-6	communications system directorate of a joint staff
JCEOI	joint communications-electronics operating instructions
JCS	Joint Chiefs of Staff
JCSE	Joint Communications Support Element (USTRANSCOM)
JDN	joint data network
JEMSO	joint electromagnetic spectrum operations
JEMSOC	joint electromagnetic spectrum operations cell
JFC	joint force commander
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network (USCYBERCOM)
JIMB	joint information management board
JLLIS	Joint Lessons Learned Information System
JNCC	joint network operations control center
JOC	joint operations center
JP	joint publication
JRFL	joint restricted frequency list
JTF	joint task force
JWICS	Joint Worldwide Intelligence Communications System
MARS	Military Auxiliary Radio System
MC4EB	Military Command, Control, Communications, and Computers Executive Board
NATO	North Atlantic Treaty Organization
NCCS	Nuclear Command and Control System
NG JFHQ-State	National Guard joint force headquarters-state
NGO	nongovernmental organization
NIPRNET	Non-classified Internet Protocol Router Network
NMCS	National Military Command System

NOSC	network operations and security center
NS/EP	national security and emergency preparedness
NSG	National System for Geospatial Intelligence
OCO	offensive cyberspace operations
OCS	operational contract support
OPLAN	operation plan
OPORD	operation order
RM	records management
SA	situational awareness
SATCOM	satellite communications
SCI	sensitive compartmented information
SecDef	Secretary of Defense
SHF	super-high frequency
SIPRNET	SECRET Internet Protocol Router Network
TACSAT	tactical satellite
TBMCS	theater battle management core system
TDL	tactical data link
TNCC	theater network operations control center
TPFDD	time-phased force and deployment data
TTP	tactics, techniques, and procedures
UHF	ultrahigh frequency
USCYBERCOM	United States Cyber Command
USG	United States Government
USSPACECOM	United States Space Command
VTC	video teleconferencing
WAN	wide-area network

PART II—TERMS AND DEFINITIONS

command and control system. The facilities, equipment, communications, procedures, and personnel essential for a commander to plan, direct, and control operations of forces pursuant to the missions assigned. (Approved for incorporation into the DOD Dictionary.)

commonality. A quality that applies to materiel or systems: (1) possessing like and interchangeable characteristics enabling each to be utilized, or operated and maintained, by personnel trained on the others without additional specialized training; (2) having interchangeable repair parts and/or components; and (3) applies to consumable items interchangeably equivalent without adjustment. (Approved for incorporation into the DOD Dictionary.)

communications network. An organization of stations capable of intercommunications, but not necessarily on the same channel. Also called **COMNET.** (DOD Dictionary. Source: JP 6-0)

communications security. Actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study. Also called **COMSEC.** (Approved for incorporation into the DOD Dictionary.)

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. (Approved for incorporation into the DOD Dictionary.)

Defense Information Systems Network. The integrated network, centrally managed and configured by the Defense Information Systems Agency, to provide dedicated, point-to-point, switched voice and data, imagery, and video teleconferencing services for all Department of Defense activities. Also called **DISN.** (Approved for incorporation into the DOD Dictionary.)

Defense Switched Network. The component of the Defense Communications System that handles Department of Defense voice, data, and video communications. Also called **DSN.** (DOD Dictionary. Source: JP 6-0)

Department of Defense information network. The set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. Also called **DODIN.** (Approved for incorporation into the DOD Dictionary.)

emission security. Actions designed to deny unauthorized persons information of value as a result of intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems. (Approved for incorporation into the DOD Dictionary.)

Global Command and Control System. A deployable system supporting forces for joint and multinational operations across the range of military operations with compatible, interoperable, and integrated communications systems. Also called **GCCS.** (Approved for incorporation into the DOD Dictionary.)

interoperability. 1. The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. (JP 3-0) 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. (DOD Dictionary. Source: JP 6-0)

joint communications network. The aggregation of the joint multichannel trunking and switching system and the joint command and control communications system(s) in a theater. Also called **JCN.** (DOD Dictionary. Source: JP 6-0)

joint network operations control center. An element of the communications system directorate of a joint staff established as the single control agency for the management and direction of the joint force communications system. Also called **JNCC.** (Approved for incorporation into the DOD Dictionary.)

message. 1. Any thought or idea expressed briefly in a plain or secret language and prepared in a form suitable for transmission by any means of communication. (JP 6-0) 2. A narrowly focused communication directed at a specific audience to support a specific theme. Also called **MSG.** (DOD Dictionary. Source: JP 3-61)

minimize. A condition wherein normal message and telephone traffic is drastically reduced so messages connected with an actual or simulated emergency shall not be delayed. (Approved for incorporation into the DOD Dictionary.)

National Communications System. None. (Approved for removal from the DOD Dictionary.)

National Military Command System. The priority component of the Global Command and Control System designed to support the President, Secretary of Defense, and Joint Chiefs of Staff in the exercise of their responsibilities. Also called **NMCS.** (DOD Dictionary. Source: JP 6-0)

node. 1. A location in a mobility system where a movement requirement is originated, processed for onward movement, or terminated. (JP 3-17) 2. In communications and computer systems, the physical location that provides terminating, switching, and gateway

access services to support information exchange. (JP 6-0) 3. An element of a system that represents a person, place, or physical thing. (DOD Dictionary. Source: JP 3-0)

operational data. Information created by, used in, or used in support of a military operation by the headquarters, its components, and operating forces that supports planning, analysis, and assessment of friendly, adversary, and enemy activity. (Approved for inclusion in the DOD Dictionary.)

physical security. None. (Approved for removal from the DOD Dictionary.)

SECRET Internet Protocol Router Network. None. (Approved for removal from the DOD Dictionary.)

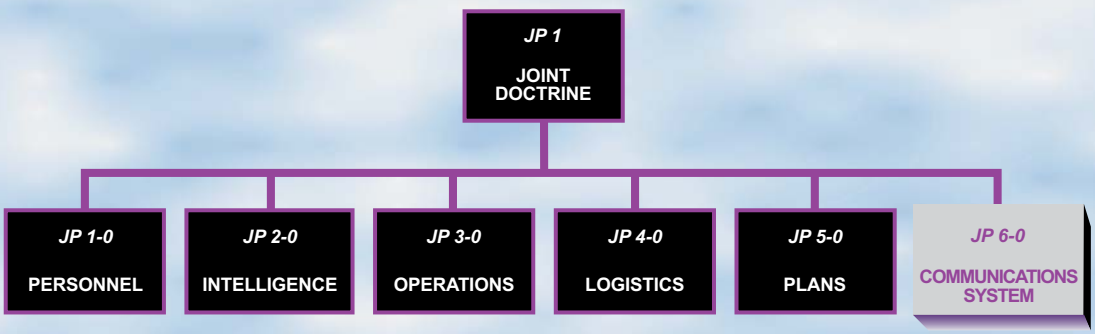
signal operating instructions. A series of orders issued for technical control and coordination of the signal communication activities of a command. Also called **SOI.** (Approved for incorporation into the DOD Dictionary.)

tactical data link. A Joint Staff-approved, standardized communication link used for the transmission of digital information via a single or multiple network architecture and multiple communication media for exchange of tactical information. Also called **TDL.** (Approved for incorporation into the DOD Dictionary.)

telecommunications. Any transmission, emission, or reception of various forms of information by wire, radio, visual, or other electromagnetic systems. (Approved for incorporation into the DOD Dictionary.)

transmission security. Actions designed to protect communications from interception and exploitation by means other than cryptoanalysis. Also called **TRANSEC.** (Approved for incorporation into the DOD Dictionary.)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



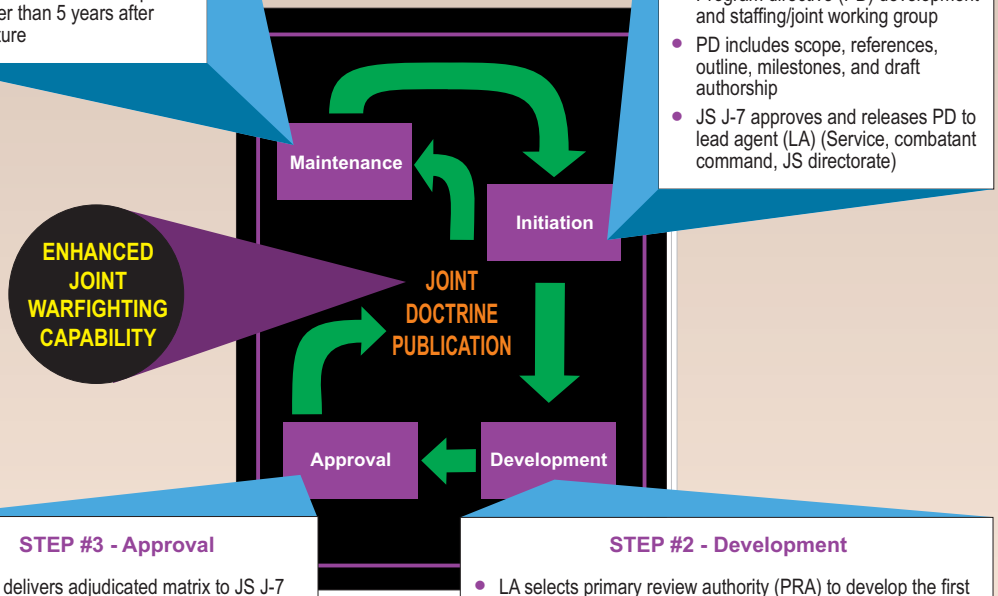
All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 6-0** is in the **Communications System** series of joint doctrine publications. The diagram below illustrates an overview of the development process:

STEP #4 - Maintenance

- JP published and continuously assessed by users
- Formal assessment begins 24-27 months following publication
- Revision begins 3.5 years after publication
- Each JP revision is completed no later than 5 years after signature

STEP #1 - Initiation

- Joint doctrine development community (JDDC) submission to fill extant operational void
- Joint Staff (JS) J-7 conducts front-end analysis
- Joint Doctrine Planning Conference validation
- Program directive (PD) development and staffing/joint working group
- PD includes scope, references, outline, milestones, and draft authorship
- JS J-7 approves and releases PD to lead agent (LA) (Service, combatant command, JS directorate)



STEP #3 - Approval

- JSDS delivers adjudicated matrix to JS J-7
- JS J-7 prepares publication for signature
- JSDS prepares JS staffing package
- JSDS staffs the publication via JSAP for signature

STEP #2 - Development

- LA selects primary review authority (PRA) to develop the first draft (FD)
- PRA develops FD for staffing with JDDC
- FD comment matrix adjudication
- JS J-7 produces the final coordination (FC) draft, staffs to JDDC and JS via Joint Staff Action Processing (JSAP) system
- Joint Staff doctrine sponsor (JSDS) adjudicates FC comment matrix
- FC joint working group


JOINT
CHIEFS OF STAFF