# Joint Publication 6-0

# Joint Communications System

10 June 2015

This publication is the keystone document for communications system support to joint operations, providing guidelines to commanders regarding information systems and networks.

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.

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.

Martin E Dempsey

MARTIN E. DEMPSEY
General, U.S. Army
Chairman of the Joint Chiefs of Staff

# PREFACE

## 1. Scope

This publication is the keystone document for the communications system series of publications. It provides the doctrinal foundation for communications system support to joint operations and provides a comprehensive approach to the support of joint force command and control through the integration of joint communications and information systems across the range of military operations.

## 2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS). It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for US military coordination with other US Government departments and agencies during operations and for US military involvement in multinational operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall objective.

## 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, and combat support agencies.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. 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, has provided 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.

Intentionally Blank

# SUMMARY OF CHANGES
## REVISION OF JOINT PUBLICATION 6-0
## DATED 10 JUNE 2010

- **Synchronizes related terminology with Joint Publication 3-12, *Cyberspace Operations,* including replacing "Global Information Grid" with "Department of Defense information network."  Replaces "information assurance" with "cybersecurity."**

- **Updates organizational relationships and describes command and support relationships for Department of Defense information network operations.**

- **Discusses the joint information environment.**

- **Updates communications planning considerations for operations with mission partners.**

- **Discusses information sharing and services.**

- **Updates information on National Security and emergency preparedness communications.**

- **Corrects and updates factual errors due to procedural and organizational changes.**

Intentionally Blank

# TABLE OF CONTENTS

PAGE

CHAPTER V

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

APPENDIX

GLOSSARY

FIGURE

# 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

***All joint functions—command and control (C2), intelligence, fires, movement and maneuver, protection, and sustainment—depend on responsive and available communications systems that tie together all aspects of joint operations and allow the joint force commanders and their staffs to initiate, direct, monitor, question, and react.***

A joint communications system is comprised of the networks and services that enable joint and multinational capabilities. The objective of the joint communications system is to 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's (DOD's) end-to-end communications system supporting the JFC is the Department of Defense information network (DODIN). 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.

***Elements of the C2 System***

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

There are two 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 in the execution of the decision.

***Information Management***

Improved technology in mobility, weapons, sensors, and communications continues to reduce reaction time, increase the operating tempos, and generate large amounts of information. If information is not properly managed, the abilities of commanders, decision makers, and, ultimately, the joint force may be degraded. It is essential that the joint communications system complement human capabilities and reduce or eliminate anticipated or known limitations to mission accomplishment.

***The Role of the Communications System***

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

***Cyberspace***

Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

***Department of Defense Information Network (DODIN) Operations***

The DODIN consists of all networks and information systems owned or leased by DOD. This includes common enterprise service networks (classified and unclassified), intelligence networks operated by DOD components of the intelligence community, closed mission system and battlefield networks, and other special purpose networks.

***Communications System Functions***

Information system components that make up the communications system normally have the capabilities to acquire, process, store, transport, control, protect, disseminate, and present information.

***Communications System Principles***

To provide the flexibility to dynamically meet mission objectives, the communications system must be interoperable, agile, trusted, and shared. Networked joint forces increase operational effectiveness by allowing 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.

## The Information Environment

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

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 full spectrum 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.

***DODIN Operations***

DODIN operations are the means by which DOD manages the flow of information over its information networks.

DODIN operations include proactive actions which address the entire DODIN, including configuration control and patching, cybersecurity measures and user training, physical security and secure architecture design, intrusion detection, bandwidth management/spectrum management, operation of host-based security systems and firewalls, and encryption of data. DODIN operations require centralized coordination because they have the potential to impact the integrity and operational readiness of the DODIN; however, execution is generally decentralized.

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 IT infrastructure, information services, data, policies, standards, and procedures must support the operational forces in all of their assigned missions.

***Roles and Responsibilities***

Commander, United States Strategic Command (CDRUSSTRATCOM) is responsible for directing DOD information networks operations and defense. For operational effectiveness, CDRUSSTRATCOM has delegated DODIN operations, security, and defense to United States Cyber Command (USCYBERCOM). CCDRs, Services, and DOD agencies will coordinate with USCYBERCOM to ensure global impacts to the DODIN are properly considered. USCYBERCOM focuses on military cyberspace operations. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the security, operations, and defense of the DODIN.

## Joint Force Communication, System Operations, and Management Planning

***Planning and Management Organizations***

The **Joint Network Operations Control Center** (JNCC) is used to manage all deployed communications systems. The JNCC, through component/Service control facilities, exercises control over many deployed communications systems and serves as a control agency for the management of joint communications networks under JFC authority and USCYBERCOM's directive authority for cyberspace operations.

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.

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

***Planning and Management Structure***

The CCDR, through the Joint Cyberspace Center (JCC) and J-6, provides communications system guidance and priorities that support the commands and the components through the 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.

The JCC functions as the nexus for the CCDR's cyberspace enterprise, serving as the staff to provide SA, planning, intelligence, and readiness functions for all three cyberspace missions—DODIN operations, defensive cyberspace operations, and offensive cyberspace operations.

***Communications Planning and Management***

Communications system planners ensure that 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 a host nation. 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, communications available, and how they are employed.

***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.
- Commercial Capabilities.
- Training.
- Discipline.

- Timelines.
- Simultaneous Planning.

## Information Sharing and Services

Joint forces must effectively exchange information among components, United States Government (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. The DOD Information Sharing Strategy guides DOD's sharing of information within DOD and with federal, state, local, tribal, and multinational partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector.

***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.

***Establish Standards***

Standards facilitate integration of communications systems and networks with external mission partners at the operational and tactical levels.

***Communications Systems***

Whether classified or unclassified, the mission partner communications network must be capable of securely integrating mission partners' systems using the mission partner communications network IT infrastructure, enterprise services, and architectures. Use of agreed upon information and data exchange standards/services that enable interoperable information exchanges.

Key aspects of mission partner communications network implementation include liaisons, identification of communications network requirements, multinational communications agreements, US interpreters, and a coherent releasability/disclosure policy.

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

***National Military Command System***

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, the Secretary of Defense (SecDef), the Chairman of the Joint Chiefs of Staff (CJCS), and other senior leaders in the exercise of their responsibilities through the range of military operations and during all levels of conflict.

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.

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.

***Nuclear C2***

The Nuclear Command and Control System supports peacetime operation of nuclear forces and provides assured, unbroken connectivity between the President and the strategic deterrent forces in stressed environments. It includes the emergency action message dissemination systems and those systems used for tactical warning/attack assessment, conferencing, force report-back, reconnaissance, retargeting, force management, and requests to use nuclear weapons.

***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 (OEC) leads the national security and emergency preparedness (NS/EP) communications efforts. OEC's programs and services coordinate emergency communications planning, preparation and evaluation, to ensure safer, better-prepared communities nationwide. The SecDef oversees the development, testing, implementation, and sustainment of NS/EP communications that are directly responsive to the national security needs of the President, Vice President, and senior national leadership.

## Conclusion

This publication provides the doctrinal foundation for communications system support to joint operations and provides a comprehensive approach to the support of joint force command and control through the integration of joint communications and information systems across the range of military 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,* c. 500 BC**

### 1. Introduction

a. A joint communications system is comprised of the networks and services that enable joint and multinational capabilities. The objective of the joint communications system is to 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's (DOD's) end-to-end communications system supporting the JFC is the Department of Defense information network (DODIN). 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. Cyberspace operations (CO) include offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DODIN operations. This publication addresses primarily the DODIN operations mission and elements of the DCO mission within CO. It also includes reference to initial defensive cyberspace operations-internal defensive measures (DCO-IDM), as the same forces often coordinate the activities of both missions. The DODIN conceptually unifies DOD's information systems and networks into a real-time information system of systems 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, policy, 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, transport, process, share, and protect 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. All joint functions—C2, intelligence, fires, movement and maneuver, protection, and sustainment—depend on responsive and available communications systems that tie together all aspects of joint operations and allow the 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 the DOD cooperates to achieve national goals. 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; multinational 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.

## 2. Command and Control

a. **Elements of the C2 System.** The first element of a C2 system is **people**—people who acquire information, make decisions, take action, communicate, and collaborate with one another to accomplish a common goal. Human beings—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 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 two 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 in the execution of the decision. In one way or another, effective C2 is inherently dependent on information: getting it, evaluating its accuracy, judging its value, processing it into useful form, acting on it, and sharing it with those who need it in the most expeditious, secure manner. The C2 system must present information in a form that is both quickly understood and useful to the recipient at every required level of warfare—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 the quality of information is as important as other military tasks. Good IM makes accomplishment of other tasks less complex. Automation and standardization of communications system processes and procedures improve IM and assist the commander's effectiveness and speed of C2. Improved technology in mobility, weapons, sensors, and communications continues to reduce reaction time, increase the operating tempos, and generate large amounts of information. If information is not properly managed, the abilities of commanders, decision makers, and, ultimately, the joint force may be degraded. It is essential that the joint communications system complement human capabilities and reduce or eliminate anticipated

### Information Quality Attributes

Accuracy

- Information that conveys the true situation

Relevance

- Information that applies to the mission task or situation ahead

Timeliness

- Information that is available in time to make decisions

Usability

- Information that is understandable and is in commonly understood format and displays

Completeness

- All necessary information required by the decision maker

Brevity

- Information that has only the level of detail required

Security

- Information that has been afforded adequate protection where required

**Figure I-1. Information Quality Attributes**

or known limitations 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 context of current and future operations. The value of technology, organization, and strategy is diminished in the absence of a professional force to leverage their value. A comprehensive and thoroughly rehearsed set of operational procedures is crucial to developing that required degree of proficiency. 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.

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

## 3. The Role of the Communications System

a. A secure, robust, and reliable communications system gives the JFC the means to assimilate information and to exercise authority and direct forces over large geographic areas and a wide range of conditions. A communications system that provides connectivity throughout the operational area from the strategic to tactical levels is vital to plan, conduct, sustain operations, and enable information superiority. The JFC should maintain reliable, resilient, jam-resistant, and secure communications with higher, supported, supporting, and subordinate commands during all phases of an operation and in all types of degraded environments. Operations at all levels routinely require long-range, mobile communications. Consideration must be made for en route, intra-theater, and inter-theater communications. In addition, the communications system must be prepared to interface mission partners. 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 flow of information.

b. The communications system is the JFC's principal tool to collect, monitor, transport, process, protect, and disseminate information. Given the criticality of information, the security of the communications system is paramount to ensuring the JFC can trust the information it provides. Effective C2, through the exchange of information, integrates joint force components and allows them to function effectively across vast distances, in austere or complex environments, and in all weather conditions. The mission and structure of the joint force drives specific information flow and processing requirements. The location and information requirements of the joint force drive the configuration and capabilities of the communications system. The goal 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 allowing the use of remote staffs to develop and coordinate an operation plan (OPLAN) and execute an operation order (OPORD). It 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) **Operational Reach.** The communications system supports the synchronization of military capabilities, allowing commanders to locate and identify friendly forces in the operational environment and support the conduct of over-the-horizon operations with beyond line-of-sight communications and communications on the move.

(4) **Tactical Flexibility.** The communications system allows 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 adversary—to the joint force enables more effective decentralized execution.

(5) **Network-Enabled Operations**

(a) The modern communications system allows 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 widely 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 adversaries will seek to exploit. The joint force's ability to use the EMS is a key to success in the future operational environment. See Chapter III, "Joint Force Communication, System Operations, and Management Planning," for more on EMS.

(6) **Information Superiority**

(a) Information superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. The communications system must facilitate information superiority and IM. Information superiority and IM lie at the core of every military activity. Information superiority is more than just having an information edge over an adversary or sustaining the information needs of our own forces. It also involves denying an adversary's ability to do the same.

(b) The power of superiority in the information environment mandates that the US advocate for it as a first priority even before hostilities begin. This requires DOD to develop 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 all 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 US Government, multinational partners, and, when authorized, the private sector.

d. **Cyberspace.** Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace threats from state and non-state actors are a real and imminent danger to all operations. Information is a critical instrument of national power, thus the ability to achieve and maintain an advantage in cyberspace is crucial to national security.

e. **DODIN Operations.** The DODIN consists of all networks and information systems owned or leased by DOD. This includes common enterprise service networks (classified and unclassified), intelligence networks operated by DOD components of the intelligence community (IC), closed mission system and battlefield networks, and other special purpose networks (e.g., "edu" domains operated by the Service academies). When properly secured, operated, and defended, the DODIN collects, processes, stores, manages, and disseminates information on demand to the joint force, policy makers, and support personnel. DODIN operations are the means by which DOD designs, builds, configures, secures, operates, maintains, and sustains communications and networks in support of military operations. DOD shares cyberspace with enemies and adversaries seeking to exploit our weaknesses on a daily basis. US joint forces, mission partners, and first responders require communications that are not only secure, but also flexible enough to meet the ever-changing needs of joint and multinational operations.

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

f. **EMS**

(1) The EMS is essential to control the operational environment during all military operations. Information and data exchange between platforms and capabilities will at some point rely on the EMS for transport. The EMS is constrained by both military and civil users as well as adversary attempts to deny its use. The EMS transcends all physical domains and the information environment and extends beyond defined borders and boundaries.

(2) Statutory requirements and the variety of agencies and authorities present within the homeland make EMS management for domestic operations very different than EMS management conducted in support of operations overseas. Defense support of civil authorities operations typically begin at the local and state level. An operation may progress through several legal authorities, depending on the severity of the situation, and the actions of state and national leaders. It is critical that continuity of EMS management be maintained as the forces responding to an incident transition to other legal authorities.

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

g. **DCO-IDM.** Internal defensive measures are those DCO that are conducted within the DODIN. They include actively hunting for advanced internal threats as well as the internal responses to these threats. Internal defensive measures respond to unauthorized activity or alerts/threat information within the DODIN, and leverage intelligence, counterintelligence (CI) law enforcement (LE), and other military capabilities as required. While DODIN operations are primarily concerned with the security and performance of the DODIN, DCO-IDM are concerned with its defense. DODIN operations and DCO-IDM are intrinsically linked activities, sharing many common activities and practitioners. There are four basic components of DCO-IDM:

(1) **Organic Defenses.** These include the infrastructure and administrators of the DODIN in general. Activities associated with organic defense include emergency patching, reconfiguration in the face of a specific threat, and monitoring.

(2) **Dedicated Defenses.** These include infrastructure dedicated to DCO and activities, such as intrusion sensors, gateway security stacks, and other boundary defenses.

(3) **Enterprise Defenders.** These include personnel performing enterprise network defense activities, as well as network defense units organized to secure the DODIN but who also provide basic DODIN defenses.

(4) **Cyberspace Protection Teams.** These are mobile cyberspace defense units assigned to United States Cyber Command (USCYBERCOM) for the purpose of mission assurance to provide secondary defenses and to target advanced threats.

## 4. 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 communications system normally have the capabilities to acquire, process, store, transport, control, protect, disseminate, and present information (see Figure I-2).

## 5. Communications System Principles

a. A joint force that is linked and synchronized in time and purpose is considered networked. 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. To provide the flexibility to dynamically meet mission objectives, the communications system must be interoperable, agile, trusted, and shared (see Figure I-3). Networked joint forces increase operational effectiveness by

### Communications System Functions

Acquire

- The introduction of information into the communications system

Process

- Specified sequence of operations performed on well-defined inputs to produce a specified output

Store

- Retention, organization, and disposition of data, information, or knowledge to facilitate sharing and retrieval

Transport

- End-to-end information exchange and dissemination in a global environment

Control

- The function of directing, monitoring, and regulating communications system functions to fulfill operational requirements within specific performance parameters

Protect

- Information integrity, secure processing, and transmission with access only by authorized personnel

Disseminate

- Distributing processed information to the appropriate users

Present

- Information provided to the user in the method that best facilitates understanding and use

**Figure I-2. Communications System Functions**

allowing 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. A networked force has the ability to expand its operational reach by allowing dispersed elements to use the information services of other organizations and integrate information from across the operational environment.

c. 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 of the JFC's OPLANs, OPORDs, or campaign plans.

d. The DODIN is a global enterprise enabling all combatant command (CCMD) missions and Service core functions. Commander, United States Strategic Command (CDRUSSTRATCOM), through Commander, United States Cyber Command (CDRUSCYBERCOM), is the supported commander for global DODIN operations and DCO-IDM, including those operations that span multiple CCMDs. CDRUSCYBERCOM

### Communications System Principles

**Interoperable**

- When information can be exchanged between communications systems/equipment directly and satisfactorily between them and/or their users. Facilitated by:
    - Common equipment
    - Compatibility of equipment
    - Standardization
    - Liaison

**Agile**

- System agility attributes
    - Responsiveness
    - Flexibility
    - Innovation
    - Adaptation

**Trusted**

- Trusted communications attributes
    - Survivability
    - Security
    - Sustainability

**Shared**

- Mutual use of information, services, or capabilities

**Figure I-3. Communications System Principles**

delegates this authority to Commander, Joint Force Headquarters (JFHQ) for DODIN operations and DCO-IDM to establish the global priorities to secure, operate, and defend the DODIN for operational planning, direction, and monitoring of tactical execution. Geographic combatant commanders (GCCs) are the supported commanders for theater DODIN operations and DCO-IDM within their assigned area of responsibility (AOR). The GCCs establish regional priorities for mission assurance, which will drive theater DODIN operations and DCO-IDM. CO will be deconflicted through the synchronization of USCYBERCOM and CCMD operational processes, principally through the cyberspace tasking cycle.

Intentionally Blank

# CHAPTER II
## THE INFORMATION ENVIRONMENT

> *"In order to create an IT [information technology] environment that enables mission command, requires us to adapt how we approach information technology, including the structure and function of our information systems, and also how we use them."*
>
> **General Martin E. Dempsey**
> **Chairman of the Joint Chiefs of Staff**
> **Joint Information Environment White Paper, January 2013**

### 1. General

a. The information environment is one that continues to evolve and adapt. The information 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 manage and operate 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 full spectrum 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.

> **The JIE [joint information environment] will be an important evolution in our information environment. It will change the way we assemble, configure, and use new and legacy information technologies. It will consist of networked operations centers, a consolidated set of core data centers, and a global identity management system with cloud-based applications and services. The JIE framework will provide the information environment to flexibly create, store, disseminate, and access data, applications, and other computing services when and where needed. It will better protect the integrity of information from unauthorized access while increasing the ability to respond to security breaches coherently across the system as a whole.**
>
> **Source: Chairman of the Joint Chiefs of Staff**
> **Joint Information Environment White Paper**
> **22 January 2013**

### 2. Operational Construct

a. The DODIN supports DOD missions and functions and is central to joint operations. Joint operations span military engagement, security cooperation, deterrence activities, crisis response, limited contingency operations, and major operations and campaigns from phase 0 through phase V. 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 mission partners to securely and seamlessly share required information.

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 allows 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. To achieve this information advantage, everyone in DOD must be able to access the information they require to perform their assigned functions from the point of need, consistent with security and required access restrictions. 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.

## 3. Department of Defense Information Network Operations

a. DODIN operations are operations to design, build, configure, secure, operate, maintain, and sustain DOD information networks. Since all actions taken for the sake of performance impact security and vice versa, DODIN operations and DCO-IDM are intrinsically linked activities.

(1) DODIN operations are the means by which DOD manages the flow of information over its information networks. The purpose of DODIN operations is assured system and network availability, assured information protection, and assured information delivery, which protect and maintain freedom of action for DOD missions within cyberspace. DODIN operations include proactive actions which address the entire DODIN, including configuration control and patching, cybersecurity measures and user training, physical security and secure architecture design, intrusion detection, bandwidth management/spectrum management, operation of host-based security systems and firewalls, and encryption of data. DODIN operations require centralized coordination because they have the potential to impact the integrity and operational readiness of the DODIN; however, execution is generally decentralized. The aggregate effect of DODIN operations activities establishes the security framework on which all DOD missions ultimately depend.

(2) Joint force DODIN operations are those activities occurring within a theater that have the potential to impact only operations in that theater. Examples include operations on mission networks, the timing of centrally directed network configuration, establishing minimal procedures to limit outbound traffic flow, or other prioritization of joint force resources. DODIN operations underlie nearly every aspect of the JFC's operations throughout the operational environment, and its activities are the foundation of cyberspace (SA). Therefore, DODIN operations are fundamental to the JFC's SA of the operational

environment. Besides physical protection of key cyberspace infrastructure, the JFC's primary defense-in-depth in cyberspace is DODIN operations.

(3) The remainder of this publication addresses DODIN operations and their application to the joint communications system.

b. DODIN is detailed more in Appendix A, "Department of Defense Information Network Components."

*For further information, see JP 3-12,* Cyberspace Operations.

## 4. The Tactical Level

US forces at the tactical level often operate at a communications disadvantage. 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 by, 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 adversaries. As such, commanders should implement clear measures to ensure tactical information is accurate, timely, and adequately protected at all times. The tactical network environment may be supported with joint communications nodes (JCNs). A JCN 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., Nonsecure 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 transitions between administrative, movement of forces, and tactical networks. As such, the need to delineate network operations and 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 24/7 persistence. Each system needs tailored network management systems, lines of control, and authority requirements to meet operational needs.

*For additional information on the roles of the joint network data officer, refer to CJCSM 3115.01,* Joint Data Network (JDN) Operations, *as it pertains to converging requirements to plan, analyze, and manage tactical C2 networks.*

## 6. Operations in Degraded and Denied Environments

a. Enemies and adversaries may seek to 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 target for adversaries.

b. The growth of anti-access (A2) and area denial (AD) 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 may see the adoption of an A2/AD strategy against the US as a favorable course of action (COA) for them. Those able to field layered and fully integrated A2/AD capabilities may 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 may deliberately attempt to deny friendly use of the EMS, space, cyberspace, and/or terrestrial systems. Due to heavy joint reliance on advanced communications systems, such an attack may be a central element of any enemy or adversary A2/AD strategy, requiring a higher degree of protection for friendly C2 systems and planning for operations in a denied or degraded environment.

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.

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 allowing operations to continue uninterrupted.

## 7. Roles and Responsibilities

a. The attainment of information superiority requires unity of effort in command, control, and management of the DODIN. As a practical matter, unity of effort is necessary due to the vast number of IT resources required to support worldwide DODIN operations. 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 that are deployed or operate 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. In accordance with (IAW) the Unified Command Plan (UCP), CDRUSSTRATCOM is responsible for directing DOD information networks operations and defense. For operational effectiveness, CDRUSSTRATCOM has delegated DODIN operations, security, and defense to USCYBERCOM. CCDRs, Services, and DOD agencies will coordinate with USCYBERCOM to ensure global impacts to the DODIN are properly considered. USCYBERCOM focuses on military CO. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the security, operations, and defense of the DODIN. 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 SecDef**

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

1. The DOD CIO serves as the DOD's principal staff assistant for IM, and consequently develops and issues the DOD information resource management strategic plan. The DOD CIO is the DODIN architect and develops, maintains, and enforces compliance with the DODIN architecture. The DOD CIO also consults with comparable IC authorities on matters of policy, implementation, and operation. The DOD CIO is responsible to enforce standards for interoperability, cybersecurity, 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 pertaining to the DODIN. The DOD CIO Executive Board provides advice and information to the DOD CIO on the full range of statutory and regulatory matters related to information and DOD IT. Chaired by the DOD CIO, the board is composed of CIOs and/or senior communicators from the Services, the Joint Staff, the IC, United States Strategic Command (USSTRATCOM), 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 the SecDef in developing information security policy and guidance. Concerning joint communications, The Undersecretary of Defense for Intelligence advises and assists the DOD CIO on the acquisition programs that significantly affect intelligence, CI, 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. CJCS exercises operational oversight over those portions of the DODIN utilized for such communications.

(b) CJCS is responsible for the operation of the National Military Command System (NMCS) for SecDef to meet the needs of the President, SecDef, and the Joint Chiefs of Staff; it establishes operational policies and procedures for all components of the NMCS and ensures their implementation.

(c) 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 communications systems 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, 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 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 United States. 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. As the only joint combined organization focused entirely on communications system matters, it is positioned to provide leadership within the combined and joint environment. 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 that enable the exchange of information in the combined environment including Allied communications publications (ACPs).

(3) **CCDRs**

(a) GCCs oversee and coordinate DODIN planning and employment within their AORs. They exercise authority over DODIN assets assigned to their commands. Through their joint cyberspace center (JCC), they utilize the USCYBERCOM cyberspace support element (CSE) and the Defense Information Systems Agency (DISA) DODIN Operations Center hierarchy, 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), and USSTRATCOM to create and maintain visibility over theater and global networks.

(b) CCDRs report on the readiness of 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 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 by operational phase:

1. **Phase 0 (Shape).** The CCDR's network consists of the system infrastructure, much of which is globally connected. Phase 0 operations are characterized by well-secured networks that are prepared to support CCDR's campaign and contingency plans.

2. **Phase I (Deter).** The network begins to transition into a more decentralized capability; the CCDR postures network capabilities and authority for eventual delegation to one or more JFCs.

3. **Phase II (Seize Initiative).** The CCDR begins decentralization/transition of network capability/authority to subordinate commanders.

4. **Phase III (Dominate).** The CCDR increases the rate of decentralization.

5. **Phase IV (Stabilize).** The CCDR completes decentralization of network capability/authority to subordinate commanders.

6. **Phase V (Enable Civil Authority).** Commanders initiate the transition of network capabilities/authority back to a 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 theater 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, intergovernmental organizations (IGOs), 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 joint electromagnetic spectrum operations (JEMSO) to gain control of their electromagnetic operational environment and therefore enable DODIN capabilities to operate as they are intended. JEMSO requires significant joint EMS management operations (i.e., HN coordination, frequency management, and joint spectrum interference resolution), as well as electronic warfare, to enable freedom of operation 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/intelligence information 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 (communications supplement/instructions) 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 in order to identify operational procedures, coordination with USCYBERCOM and other DOD and non-DOD mission partners, and provide joint training.

(4) **Military Departments (MILDEPs) and Services.** IAW guidelines and direction from SecDef, each MILDEP 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, managers, or executive agents, extend DODIN common services, to include voice, data, and video, to their organizations within the sustaining base.

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

(d) Provide spectrum engineering and management within their respective MILDEPs 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) **CDRUSSTRATCOM**

(a) CDRUSSTRATCOM is responsible for the security, operation, and defense of the DODIN, which it executes through its subordinate unified command, USCYBERCOM. USSTRATCOM secures, operates, and defends the DODIN as part of its overall responsibility for CO. USSTRATCOM, through its USCYBERCOM component, executes the DOD missions of DODIN operations, OCO, and DCO. USSTRATCOM advocates for national requirements and standards, and in coordination with other CCDRs, assesses the operational readiness of the DODIN. In addition, USSTRATCOM's Joint Functional Component Command for intelligence, surveillance, and reconnaissance (ISR) identifies processing, exploitation, and dissemination and shortfalls in ISR-related communications architecture. The Joint Functional Component Command for ISR also monitors the development of ISR capabilities and reviews CCMD integrated priority lists and advocates for processing, exploitation, and dissemination capabilities and capacity necessary to conduct future ISR operations.

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

(c) CDRUSCYBERCOM exercises directive authority for CO over all DOD components not assigned to USSTRATCOM. Directive authority for CO is vested in CDRUSSTRATCOM and delegated to 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 directive authority for cyberspace operations in total or in part for specific times and purposes, in order to ensure the timely and efficient security, operation, and defense of the DODIN. The ability of CDRUSCYBERCOM to exercise directive authority for CO 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 has established a joint task force (JTF) for the DODIN operations and DCO-IDM missions to exercise directive authority for CO over all DOD components for operational and tactical planning, execution, and oversight while enabling USCYBERCOM to focus on the operational and strategic levels of the mission. This JTF ensures the effective C2 of DODlN operations and DCO-IDM. See Figure II-1, for DODIN C2 illustration.

(d) CDRUSSTRATCOM has space operations authorities and responsibilities tasked by the UCP. Space operations include satellite communications (SATCOM) operations as a segment of the DODIN, and positioning, navigation, and timing operations, which heavily supports the DODIN. IAW the UCP, CDRUSSTRATCOM plans and conducts space operations and advocates for capabilities to meet CCMD, Service, and DOD agency operational requirements and strategic planning.

*For further information, see JP 3-14,* Space Operations.

(e) Additionally, CDRUSSTRATCOM 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. CDRUSSTRATCOM 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.

(6) **Joint Communications Support Element (JCSE)**

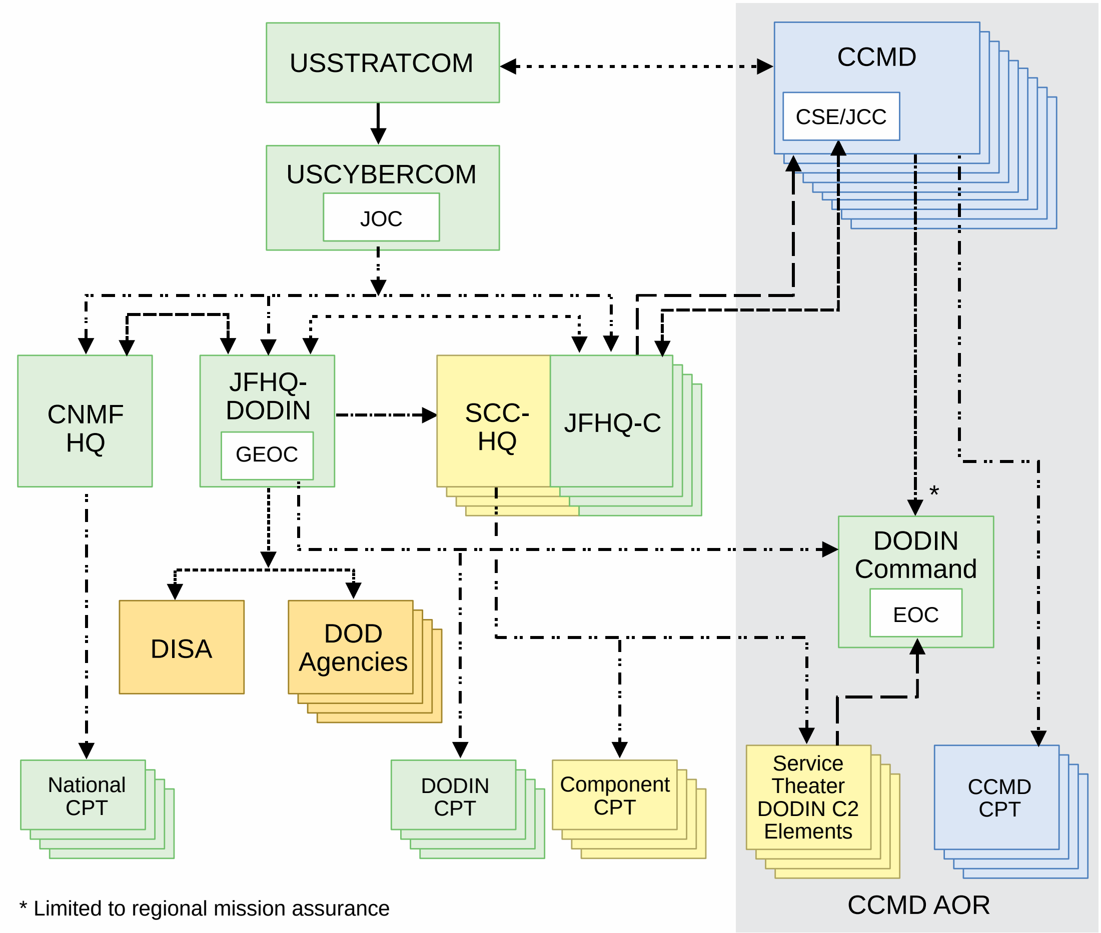
(a) The JCSE provides rapid, deployable, and scalable, en-route early entry communications capabilities across the full spectrum of operations in order to enable rapid employment of the joint force.

(b) JCSE, headquartered at MacDill Air Force Base, FL, is composed of joint active duty, National Guard, and reserve personnel who can globally deploy within hours of notification to provide communications packages tailored to the specific needs of a JTF, headquarters (HQ), and a joint special operations task force.

(7) **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).

## Command and Support Relationships for Department of Defense Information Network Operations



* Limited to regional mission assurance

### Legend

| | |
|---|---|
| AOR | area of responsibility |
| C2 | command and control |
| CCMD | combatant command |
| CNMF | Cyber National Mission Force |
| CPT | cyberspace protection team |
| CSE | cyberspace support element |
| DISA | Defense Information Systems Agency |
| DOD | Department of Defense |
| DODIN | Department of Defense information network |
| EOC | enterprise operations center |
| GEOC | Global Enterprise Operations Center |
| HQ | headquarters |
| JCC | joint cyberspace center |
| JFHQ-C | joint force headquarters-cyberspace |
| JFHQ-DODIN | Joint Force Headquarters-Department of Defense information network |
| JOC | joint operations center |
| SCC-HQ | Service cyberspace component-headquarters |
| USCYBERCOM | United States Cyber Command |
| USSTRATCOM | United States Strategic Command |

| | |
|---|---|
| ──────► | combatant command (command authority) |
| ◄- - - - - - -► | coordinating authority |
| ···············► | directive authority for cyberspace operations |
| — — — — ► | direct support |
| - ·· - ·· - ·· ► | operational control |
| ◄·············► | supporting/supported |
| -·-·-·-·-·-► | tactical control |

**Figure II-1. Command and Support Relationships for Department of Defense Information Network Operations**

(b) The J-6:

1. Publishes communications system plans, annexes, and operating instructions to support the assigned mission. In so doing, the J-6 (in coordination with the JCC) directs subordinate commands to provide communications system assets required to support the JFC. This may include assigning primary responsibility for communications to a subordinate or component command. The J-6 also assigns responsibility for 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 operational control of the EMS through the joint frequency management office.

(8) **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 the DOD IM strategic plan and 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 attaining interoperability between tactical, theater, and national intelligence-related systems, and between intelligence-related systems and tactical, theater, and national elements of the DODIN. The 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. NSG produces geospatial intelligence in an integrated multi-intelligence environment. The NSG community consists of members of the IC, MILDEPs, 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** 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.

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

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

3. 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.

4. Provides standards, interoperability testing, spectrum support and deconfliction, and integrated architecture development for the DOD net-centric enterprise information environment.

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

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

7. Provides acquisition leadership for the implementation of the net-centric vision. 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. Air National Guard units submit through the Air Force Spectrum Management Office.

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

> *"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

Joint communications system management involves the employment and technical control of assigned communications systems. Communications system management allows the planners to maintain an accurate and detailed status of the network and all networked assets. 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 joint force J-6 responds to the JFC for all communication system issues required to accomplish the overall mission. The JNCC is used to manage all deployed communications systems. The JNCC, through component/Service control facilities, exercises control over many deployed communications systems and serves as a control agency for the management of joint communications networks under JFC authority and USCYBERCOM's directive authority for CO. Functional components and subordinate JFCs may establish a network operations and security center (NOSC) to serve as their single point of contact for communications system issues. The JNCC performs planning, execution, technical direction, and management over all deployed communications systems as discussed in detail in the CJCSM 6231.01, *Manual for Employing Joint Tactical Communications*.

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. It is chaired by that individual designated the IM officer. 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.

d. The JCC functions as the nexus for the CCMD's CO. The JCC, supported by a USCYBERCOM CSE, will provide SA, planning, preparation, direction, intelligence, and readiness functions in support of CO. The JCC serves as the CCDR's staff/component for planning and oversight of CCMD DODIN operations, DCO, and OCO.

*For more information on the JCC and CO, see JP 3-12,* Cyberspace Operations.

## 2. Planning and Management Structure

a. **Executive Agent for Communications.** SecDef or Deputy Secretary of Defense may designate the head of a component as an executive agent for specific responsibilities and authority prescribed at the time of assignment. This is done when no existing means to accomplish the DOD objectives exists and DOD resources need to be focused on a specific AOR.

b. **CCMD J-6.** The CCDR, through the JCC 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 JCC to support CO planning, DODIN operations, DCO-IDM, information dissemination management, and to share SA of CCDR's communication systems. The TNCC, in conjunction with the JCC, 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 GCC's orders and direction. The CCMD J-6, in coordination with the JCC and J6, identifies defense critical infrastructure DODIN assets IAW DODD 3020.40, *DOD Policy and Responsibilities for Critical Infrastructure,* within the CCMD's AOR.

c. **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 a subordinate command's communications control center, commonly referred to as 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 SPECTRUM XXI. SPECTRUM XXI is an automated spectrum management tool that supports operational planning as well as real time management of the radio frequency spectrum, with emphasis on assigning compatible frequencies and performing spectrum engineering tasks.

*For additional information, see JP 3-0,* Joint Operations, *and JP 3-33,* Joint Task Force Headquarters.

(4) The J-6 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, neutral/civil emitters and receivers. The J-6 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.

d. **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 DODIN tactical communication and DCO-IDM deployed during operations and exercises. The JNCC, like the JCC and 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.

e. **JCC.** The JCC functions as the nexus for the CCDR's cyberspace enterprise, serving as the staff to provide SA, planning, intelligence, and readiness functions for all three cyberspace missions—DODIN operations, DCO, and OCO. The functions of the JCC encompass elements of the J-2, J-3, and J-6. While the CCDR may elect to align the JCC with any of these three depending upon the nature of the mission and AOR, the J-6 has a significant contribution due to the DODIN operations and DCO-IDM missions of the JCC. The JCC:

(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 JFHQ-Cyber, Enterprise Operations Center, and cyberspace protection teams.

(3) Should be integrated with the CCMD's boards, centers, cells, and working groups.

(4) Coordinates CO within the CCMD in order 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 CSE to obtain CCMD required cyberspace effects in theater and to establish AOR cyberspace shared SA.

f. **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 cannot unilaterally decide the priority of support. It must coordinate with the JNCC to prioritize its activities. 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 gain technical and/or interoperability assistance.

**JOINT CYBERSPACE CENTERS UNDER JOINT FORCE HEADQUARTERS-DEPARTMENT OF DEFENSE INFORMATION NETWORK**

**With the establishment of Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN), the Commander, JFHQ-DODIN will have operational control over each Department of Defense information network (DODIN) command for global DODIN/defensive cyberspace operations-internal defensive measures (DCO-IDM) activities supporting United States Cyber Command's global DODIN mission. The DODIN commands are tactical level headquarters, which include an enterprise operations center (EOC), supporting both global and regional combatant command (CCMD) mission needs. CCMD Joint Cyberspace Centers (JCCs) have tactical control of assigned DODIN commands for those DODIN and DCO-IDM activities supporting their regional CCMD missions.**

**As the cyberspace command and control construct continues to evolve and the combatant commanders receive additional manpower in their respective JCCs, the JCCs are likely to subsume many of the joint network operations control center roles and responsibilities.**

**A JNCC, in coordination with the JCC, provides the appropriate EOC with:**

- **Local situational awareness information (directly to EOC) on all relevant DODIN and DCO-IDM events**
- **Mission impact assessments of system and network events**
- **DODIN and DCO-IDM requirements beyond the commander's current assets or authority**
- **Key friendly terrain in cyberspace**

**The EOC directs network updates, policy changes, security updates, etc., in coordination with the JCC to synchronize and standardize DODIN and DCO-IDM activities.**

**Joint Information Environment<br>Operations Concept of Operations (JIE Operations CONOPS)<br>Version 2.0, 18 September 2014.**

## 3. Communications Planning and Management

a. **Systems Requirements.** The mission C2 organization and location of forces assigned to the JFC determine the essential elements of the communications systems employed. Specific command relationships and the organization of units and staffs drive the interconnecting communications methods and means. The communications system supports and provides 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 in order to enable common awareness, speed decision making, and to integrate actions of the joint force. In a fast-paced and highly technical environment, it is critical that the communications system also accommodate information exchanges at tactical levels.

b. **Adaptive Planning and Execution (APEX).** APEX applies to the development and implementation of campaign plans, OPLANs, and OPORDs prepared in response to requirements from the President, SecDef, or CJCS. It is a system of policies, procedures, processes, and reporting structures—supported by communications and IT that is 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. APEX provides for orderly and coordinated problem solving and decision making in two related but distinct categories—**deliberate planning and crisis-action planning**—which differ primarily in the amount of available planning time.

*For additional information on APEX, see JP 5-0,* Joint Operation Planning, *and CJCSM 3130.03,* Adaptive Planning and Execution (APEX) Planning Formats and Guidance.

(1) The joint planning and execution community uses deliberate planning to develop 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 APEX process is highly structured to support iterative, concurrent, and parallel deliberate planning throughout the planning community to produce thorough and fully coordinated contingency plans in noncrisis situations when time permits. Communications planners must understand commander's concept of operations, intent, and have a clear picture of the overall C2 structure.

(2) While deliberate planning is conducted in anticipation of future events, crisis action planning is based on the actual circumstances that exist at the time planning occurs. Within the context of APEX, crisis action planning responds to an incident or situation involving a threat that typically develops rapidly and creates a condition of such diplomatic, economic, political, 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 that 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 a 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, communications available, and how they are employed.

d. The J-6 plans and establishes the communications system and the communications estimate of supportability (see Appendix B, "Joint Force Communications System Estimate

Preparation Guide") during COA development and selection under the crisis action 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, the TNCC, the JCC, 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 and authorizes communications system networks. The authorizing official will assign a security control assessor within each component. For all other networks, the J-6 must consolidate system risk management requirements, validate their correctness, and forward a consolidated network security authorization package to the next higher joint force J-6.

*For more information on the accreditation process, see Department of Defense Instruction (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) **Cybersecurity.** Achieving and maintaining an effective cybersecurity posture involves the employment of secure configuration, comprehensive security training for all DODIN users, monitoring, detection, and restoration capabilities to shield and preserve information and information systems. Cyberspace defense is necessary to regain the security of the DODIN once it is lost and is focused on actions to protect, detect, characterize, counter, and mitigate unauthorized activity and vulnerabilities on DODIN. Planning for cyberspace defense to resecure information and information systems is paramount to the success of the mission when we know that there will occasionally be breaches of security. It is a part of the defense-in-depth strategy.

(2) **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 in an operational environment. Once the JFC establishes the specific C2 organization for a joint or multinational operation, the information exchange requirements (IERs) and information services are established as communications system planning begins. Planning considerations include network federation, governance and management of a federated network, EMS management; 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 (video teleconferencing [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 joint and 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 Identification of Communications System Requirements Early.** The demand for information often exceeds the capabilities of the communications system within joint and multinational commands. It is crucial that the JFC identify early communications system requirements that are external to the command or require support from national, multinational, and host-nation resources (e.g., space-based systems support, US Transportation Command-controlled JCSE, North Atlantic Treaty Organization [NATO] standing communications system equipment pool, and EMS). Multinational communications system planning must include the early establishment and incorporation of multinational networks. Resources need to be identified and planned for accordingly. Identification of the primary, secondary, and tertiary means to transport all required services is a critical planning responsibility.

3. **Standardized 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 area of concern is increasingly important. DODIN operations, including activities conducted to secure our networks, must be evaluated in the context of 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.

5. **Provide/Acquire Interpreters.** To ensure US interests are adequately protected, DOD provides or acquires its own interpreters.

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 intelligence information 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 Criteria System Firewall.** All established networks that involve multinational communications systems operations must include firewalls with security classification and restrictions IAW all the pertinent DOD security policy directives and instructions. The scope of the firewall must be specified with no ambiguity among multinational communications system participants.

8. **Identify Criteria Cross Network Domain.** Information flow between different network security domains (e.g., between US and foreign mission partner information systems) requires the use of a cross network domain solution. The DOD Information Security Risk Management Council authorizes or delegates authority for cross network domain service or authorizes the use of a cross network domain solution to access or transfer information between different interconnected network security domains.

9. **Comply with USC 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.

*For more information on sharing classified military information or national intelligence, refer to National Security Decision Memorandum 119,* Disclosure of Classified US Military Information to Foreign Governments and International Organizations, *and to National Disclosure Policy-1,* National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations.

10. **Provide Training On Communication System Services.** Communication system services express the functionalities that a communication system offers to the user. The concept of service permits the user to avoid having to know or deal with the circumstances or characteristics that are required on how the service is offered. What is important are the capabilities the system can provide for the user. This approach facilitates and simplifies communication system analysis, planning, and design. There are three main types of user communication system services:

a. **Communications Services.** Communications services are the services the communication systems provides related mainly with the transfer of information directly from user to user by conventional means not related with computer terminals (voice, data, video teleconference applications, configuration management, etc.).

b. **Core Services.** Core services are tools that provide generic computer information processing functionalities to the user (e.g., directory, file storage, printing, email, web browsing, and web hosting services).

c. **Functional Services.** Functional services are tools that provide support to a specific staff function, service, or process. For instance, a functional service could be a decision support tool, a planning tool, or any other type of capability required by the staffs. A functional service will, in general, be oriented towards a specific staff function such as intelligence or logistics. However, its implementation must take into account the complete staff process that is not necessarily constrained by organizational boundaries. For instance, while a particular functional service might support joint operations or transport/movement planning, it must also recognize and support lateral relationships with other mission areas thereby avoiding the development of stovepipe sub-systems.

(b) Commanders and planners must rapidly determine what is shared, when, and with whom. Communication 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, and concept of operations. 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 that 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:

<u>1.</u> Use system-to-system compatibility to ensure interoperability. The US may have to provide communications system resources to multinational partners to achieve this status.

<u>2.</u> Establish and manage an interface between incompatible communications system through a combination of interface hardware, software, and TTP to ensure interoperability.

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

*CJCSI 2700.01,* International Military Agreements for Rationalization, Standardization, and Interoperability (RSI) Between the United States, Its Allies, and Other Friendly Nations, *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. There are approximately 65 ACPs (basic and supplements) used by more than 90 nations. The CCEB is the only joint combined organization focused entirely on communications system matters. 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.

(3) **Support to Intelligence.** The communications system planned by the J-6 is the primary means through which intelligence information 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, the SecDef, and the Intelligence Community.")

(4) **Interagency Organization, IGO, and NGO Communications.** Of increasing importance to joint operations is effective connectivity to non-DOD departments and agencies and NGOs and IGOs. 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, IGOs, and NGOs. JFCs need to identify interagency 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 can pose a risk to DOD information networks. JFC's may need to set up separate communications networks for these users outside the DOD information network for boundary protection consisting of appropriate devices such as gateways, routers, firewalls, guards, or cross network domain solutions.

(5) **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 adversary threats to communications networks in theater. Wireless networks in particular must be closely managed due to security risks.

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

(7) **Support to Homeland Security and Defense Support of Civil Authorities.** DOD protects the United States and its citizens through homeland defense and, when SecDef approves a request, through homeland security and defense support of civil authorities. DOD is the lead federal agency for homeland defense. 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 the SecDef. DOD's involvement in homeland security and support to 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 suite or similar commercial collaboration tools, JTF owned deployable commercial voice switching, secure VTC in each governor's office, radio cross-banding so that land mobile radios, tactical satellite (TACSAT) radios, high frequency radios, and cell phones can communicate with each other, and links to national laboratories and other subject matter experts. United States Northern Command (USNORTHCOM) units include JTF-Civil Support, Joint Force HQ-National Capital Region, JTF-Alaska, JTF-North, and USNORTHCOM Domestic Operations Division. US Army North will also establish up to two regional task forces, as required. Another option is the dual-status commander. A dual-status commander is a commissioned officer of the Active Component Army or Air Force or a federally recognized Army National Guard or Air National Guard officer authorized, pursuant to Title 32, United States Code, Section 315 or 325 by SecDef, with the consent of the applicable governor of a state, to exercise command on behalf of, and receive separate orders from, a state chain of command.

(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 the DOD. For example, the JTF J-6 may need to rapidly gather information on the commercial communications infrastructure from the National Communication System and/or the National Response Framework Emergency Support Function-2 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 in order 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.

(8) **World Wide Web/Public Internet.** Communications planning and execution is dependent upon persistent access to the public portion of cyberspace. As the world's population increasingly gets its information from the public 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 public access websites for informing critical, worldwide audiences as part of a global information campaign.

(9) **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."

(10) **SATCOM Planning and Management.** SATCOM provides users with beyond the line of sight transmission 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.** The Joint Staff J-6 adjudicates allocation conflicts that cannot be resolved through USSTRATCOM's arbitration process at the respective CCMD or DOD agency, or by USSTRATCOM.

(b) **CDRUSSTRATCOM.** CDRUSSTRATCOM 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 the DOD. Directs operations of DOD SATCOM resources to provide global SATCOM support as operations and evolving requirements dictate. It also 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 Satellite Communications Support Center (RSSC) Functions.** The RSSCs provide general support to CCMDs, Services, USG departments and agencies, and international partners in the allocation of SATCOM resources as directed by CDRUSSTRACOM.

(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 has been granted and authority to radiate on that satellite channel frequency is not specifically included, failure to obtain HN authorization to radiate on the satellite channel access frequency may preclude use of the satellite link.

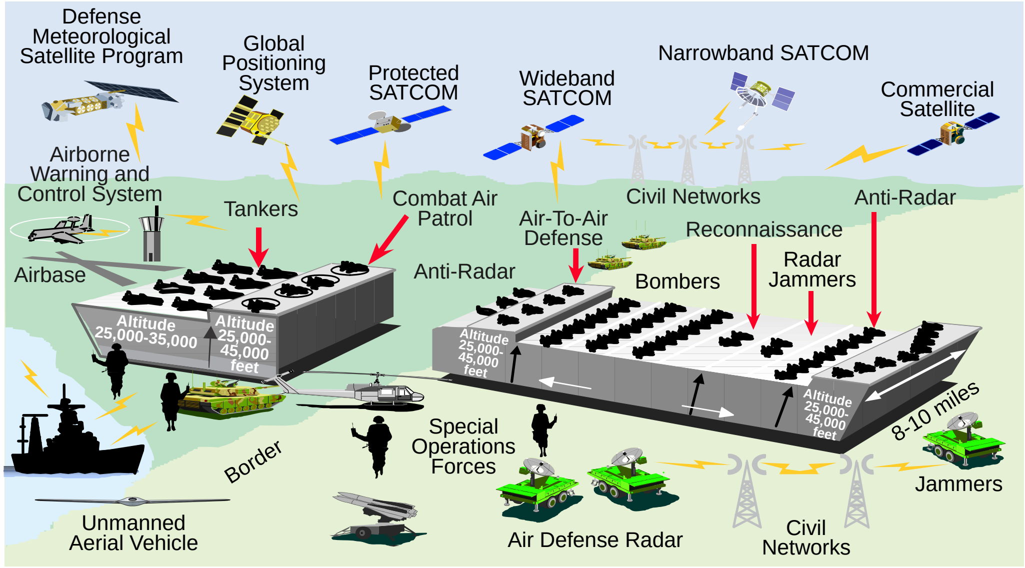
*For additional details on SATCOM, see CJCSI 6250.01,* Satellite Communications.

(11) **EMS**

(a) The EMS is a highly regulated and increasingly congested and contested natural resource. The EMS is a fundamental component of military operations and must be considered during each phase of operational planning and execution. The rapid, ever-increasing growth of highly sophisticated weapons systems, as well as operational, intelligence, and communications systems, will increase EMS demand (see Figure III-1). Gaining and maintaining EMS control necessitates an understanding of both military and civilian systems that operate within the EMS. Primarily, personnel assigned to the J-2, J-3, and J-6 staff sections plan, coordinate, and control joint military use of the EMS. With the increasingly constrained spectrum resources, the practical way of supporting the joint mission is sharing the spectrum to the maximum extent among the users of spectrum-dependent equipment.

(b) One goal of the JFC is to shape and control the electromagnetic operational environment in order to enable the secure, dependable operations of EMS-dependent capabilities (of which DODIN is key). However, the EMS transcends all physical domains and the information environment. It extends beyond defined borders or boundaries, thus complicating JEMSO. JEMSO activities consist of electronic warfare and joint EMS

Department of Defense Electromagnetic Spectrum Use



Legend

SATCOM satellite communications

**Figure III-1. Department of Defense Electromagnetic Spectrum Use**

management operations used to exploit, attack, protect, and manage the electromagnetic operational environment to achieve the commander's objectives.

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

## 4. 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, C2 task organization, commander's critical information requirements (CCIRs), and the C2 structure. 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, mission statement, intent, CCIRs, and concept of operations and support of it. Using foundational knowledge of the C2 organization and communications system capabilities, planners translate the concept of operations, concept of support, CCIRs, and operational environment 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 requirements of who needs to communicate with whom, and by what means/systems; and identifies requirements for what products—and volume of those products—will be 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 organization necessitate the increase or decrease of the IERs, or new exchange requirements. Planners make adjustments to the IERs as appropriate.

*For a more detailed discussion of IERs, refer to Joint Capabilities Integration and Development System Manual series,* Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS), *NIPRNET: https://www.intelink.gov/wiki/JCIDS_Manual*.

(3) **Interoperability, Compatibility, and Supportability Analysis.** This analysis identifies technical protocols, formats, 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 match information needs with capabilities/assets; and identifies specific communication 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 and during all phases of the operation. In the joint environment, the CCMD J-6 will plan to provide organic communications systems 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 exists 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 systems are 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 and 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 command should maintain C2 of their organic communications units as the mission allows. Mission requirements may dictate some task organization of communications system units in order 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, commercial communications systems and networks, multinational communications systems and networks, and the Service communications system.

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

b. **Planning Tools.** Automated planning and management tools are available to 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, 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 [CEOI], 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) Asynchronous transfer mode planning and engineering.

(c) Voice network planning.

(d) Data network planning.

(e) Video network planning and engineering.

(f) Automated message handling system (AMHS) planning and engineering.

(g) Message switch planning and engineering.

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

(i) Radio network planning and engineering.

(j) Engineering plans and orders.

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

(l) 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 electromagnetic interference resolution.

(18) Display regional communications system cyberspace defensive 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,* Adaptive Planning and Execution (APEX) Planning Formats and Guidance. *See also CJCSM 6231.01,* Manual for Employing Joint Tactical Communications—Joint Network Management and Control.

c. **Development of the Network Plan.** Planners use automated and manual planning tools to integrate all communications system resources to ensure unity of effort, exploitation of total force capabilities, the fusion of information, and proper positioning of critical 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.

## 5. Communications Planning Factors

a. The J-6 should be brought into the overall operation 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 (confidentiality, integrity, etc.) and incorporate them into communication systems planning efforts. Incremental development, deployment, and employment of plans and initial communication 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 may 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, communication planners should rely on agreed to standards and TTP to support the mission. In a complex network environment, unplanned changes and new approaches can have significant consequences if not fully tested and planned for. 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. As the mission and assets allow, 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 in an incremental fashion.

(6) **Modular Packaging.** Based on the mission, the commander's intent, the OPLAN, the capabilities, limitations, and 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. The joint CEOI and COMSEC must be coordinated with Service CEOI/signal operating instructions and COMSEC must also be coordinated.

(8) **Standardization** should be evident in the planned communications system. Planners should ensure equipment and system configurations are standardized throughout 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 in a timely manner to variations in the initial mission. 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) **Commercial Capabilities.** 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 may allow planners to 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.

(11) **Training.** The level of training of managers and operators of the communications system should be addressed. 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. If possible, units should also conduct language training prior to deployment and in the operational area.

(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) **Timelines.** 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 operations). 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 phase 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.** Range is a factor in connecting nodal points and networks. Consideration of equipment capabilities and the distance between nodal points is key to network connectivity.

(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. 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 use the tools and systems and educated to understand the advantages and power of a collaborative information environment (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 vulnerabilities.

(b) Connectivity issues and outages.

(c) 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 interference, ROE, 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) Unauthorized disclosure of sensitive but unclassified (SBU) information.

(3) In order to reduce overall risk to operations, skilled communications planner(s) need to be an integral part of the original operational planning team in order to assist in defining the problem, developing the plan, and allowing for sufficient lead time to coordinate with outside communications support providers, and reduce risk of operational planning teams devoid of communications expertise developing an unsupportable plan and 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).

## 6. 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 joint operations in a campaign are highly situation-and-mission dependent. Timelines between phases may be severely compressed. Phases may not follow each other in sequence; they 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, share, and collaboratively resolve lessons learned from operations, exercises, and events. Consideration of JLLIS 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 USSTRATCOM) to evaluate the existing communications infrastructure in theater to determine the strategic and tactical communications assets required. It is imperative that communications system plans 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 exclusively 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 incrementally in support of the build-up in 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 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, low frequency/very low frequency radio assets, 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 allows for 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 needs to provide 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 goal 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 allowing 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. Super-high frequency (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 the needs of the 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 communications systems 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 JSCE-controlled assets. Continued attention to preventive and routine maintenance, adequacy of stocks of spare and/or repair parts, and consumables is also 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 redraft the plan. In many cases, although major operations cease, a residual communications capability is required. Transition planning should consider both the transition of communication 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. To execute the transition plan, the J-6 needs 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 the communications system is not reduced too rapidly so it may continue to support the JFC's follow-on mission. The planner 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) As during predeployment activities, **planning is the most important part of the redeployment.** 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 unnecessary systems 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.

# CHAPTER IV
## INFORMATION SHARING AND SERVICES

> *"Sharing of information is an increasingly important element of Departmental mission success. It is imperative to effectively exchange information among components, Federal agencies, coalition partners, foreign governments and international organizations as a critical element of our efforts to defend the nation and execute national strategy."*
>
> **Department of Defense Information Sharing Strategy, 4 May 2007**

### 1. General

a. US national security depends on the ability to share the right information, with the right people, at the right time. This **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 allows 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 DOD Information Sharing Strategy 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.

d. The National Strategy for Information Sharing and Safeguarding identifies three core principles in order to address the challenge of improving information sharing and safeguarding processes and capabilities.

(1) USG departments and agencies have achieved 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. In order 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.

e. The National Strategy for Information Sharing and Safeguarding 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.

*For more information, see* National Strategy for Information Sharing and Safeguarding.

## 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 environment that enables assured information sharing among mission partners consists of a combination of people, systems, policies, procedures, and processes by which mission partners plan, prepare, and execute operations.

a. **Identify Mission Partners.** The joint force must operate with all joint, interagency, intergovernmental, and multinational mission partners. These mission partners may encompass a multitude of units, organizations, and actors. The ability for all these players to collaborate with one another is instrumental in the success or failure of military operations.

(1) **Planning.** Joint operation planning is the overarching process that guides CCDRs in developing plans for the employment of military power within the context of national strategic objectives and national military strategy to shape events, meet contingencies, and respond to unforeseen crises. Planning for the people, systems, and processes to execute information sharing in support of joint operations must be taken into account. These planning factors and considerations can be found in Chapter III, "Joint Force Communication, System Operations, and Management Planning."

(2) **Interagency and Intergovernmental.** 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 intergovernmental 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 supporting this type of environment 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 Coordination During Joint Operations.

(3) **Multinational.** 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.

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

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 almost any potential mission partner. The burden thus falls on the joint force to create an information framework that will facilitate mission partner integration. This framework leverages 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. **Communications Systems.** Whether classified or unclassified, the mission partner communications network must be capable of securely integrating mission partners' systems using the mission partner communications network IT infrastructure, enterprise services, and architectures. Use of agreed upon information and data exchange standards/services that enable interoperable information exchanges. The capability provides the ability for mission partners to share their information with all participants within a specific partnership or multinational force beginning in phase 0 (Shape) and transitioning to execution of phase I (Deter) operations. Mission partner communications network assists commanders in their effort to achieve unity of effort and seamless exchange of operational 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, US interpreters, and a coherent releasability/disclosure policy.

d. **Processes Planning.** The joint force must tailor policies and procedures to ensure standards for information sharing are effectively implemented for operations 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 IAW the DOD Sharing Data, Information, and IT Services Strategy.

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 exercise their authority to assess risk, determine the best application of policies, and the need for waivers in light of specific mission requirements and mission partners. A joint force participating in a multinational force develops the information sharing policy and procedures for that particular operation based on CCDR guidance and national policy. National Security Decision Memorandum 119 and 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

Improving the joint force's ability to share information **enables** DOD to realize the power of information as a strategic asset. 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 *DOD Information Sharing Strategy* establishes five touchstones of information sharing: culture, policy, governance, economics and resources, and technology and infrastructure. The joint stakeholder community shall improve these five areas to enable the realization of the overall goals of this strategy. To enable the achievement of DOD information sharing goals the DODIN should:

(1) Promote, encourage, and incentivize sharing.

(2) Achieve an extended enterprise.

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

(4) Ensure trust across organizations.

b. Other enablers are global authentication, access control, and directory services that allow any authorized user, with common and portable identity credentials, to have 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 to help create SA as the basis for a decision and direct and coordinate actions in the execution of the decision. A fully networked joint force to achieve shared SA among DOD components, all levels of US Government, multinational partners, and the private sector.

d. According to Chapter 1, "Joint Communications Systems Overview," there are seven criteria that enable information quality. These are accuracy, relevance, timeliness, usability, completeness, brevity, and security.

e. 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. To meet these goals, 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 goals of DODIN operations are:

(1) **Assured System and Network Availability.** The purpose is to provide visibility and control over the 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 the system and network resources. This includes providing for graceful degradation, self-healing, fail over, diversity, and elimination of critical failure points.

(2) **Assured Information Protection.** The purpose is to provide protection for the information passing over networks from the time it is stored and catalogued until it is distributed to the users, operators, and decision makers.

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

## 4. The National Information Exchange Model

In order to comply with US national guidance, DOD has adopted the National Information Exchange Model as the best suited option for standards-based data exchanges.

**NATIONAL INFORMATION EXCHANGE MODEL**

**The National Information Exchange Model (NIEM) is a community-driven, government-wide, standards-based approach to exchanging information. NIEM connects communities of people who share a common need to exchange information in order to advance their mission. NIEM is not a database, system, software, technology stack, or a silver bullet.**

**In order to comply with United States national guidance, the Department of Defense (DOD) has adopted the NIEM standards based framework as the basis for DOD's data exchange strategy. Given the Clinger-Cohen Act mandates and current fiscal pressures, DOD must adopt a DOD-wide sustainable business model for information sharing that supports the DOD data strategy. This adoption requires organizations to first consider NIEM for their information sharing solutions when deciding which data exchange standard or specification meets their mission and operational needs.**

**NIEM exchanges are being developed to allow for a more efficient and consistent method of sharing important public health and safety information, representing a significant first step in the development of a borderless network of information exchange between the United States, Canada, and Mexico.**

**Various Sources**

*For more information, see DOD CIO Memorandum,* Adoption of the National Information Exchange Model within the Department of Defense, *March 28, 2013.*

## 5. Cybersecurity

a. Cyberspace is composed of all computers, servers, routers, switches, and wired and wireless links that allow critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to national security. Securing DOD's portion of cyberspace is a strategic challenge that requires a coordinated and focused effort.

b. Cybersecurity is integral to DODIN operations and is the foundation for a strong cyberspace defense. Cybersecurity involves applying a number of security paradigms and best practices across a very broad and heterogeneous network environment or environments. The focus incorporates the security aspects of operating in cyberspace—how are the JFC's systems comprised and configured, are the systems sufficiently protected from threats and vulnerabilities, can the JFC trust the network on which the force relies for information and data exchange, and are personnel sufficiently trained to secure, operate, and defend the JFC's portion of the DODIN? The construct for cyberspace is much more complex than operating as a single information system on a network.

c. A variety of malicious actors in cyberspace threaten critical information infrastructures. Of primary concern is the threat of organized cyberspace attacks capable of denying DOD forces access to critical infrastructures or compromising security.

d. Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona. Each of these represents a level on which CO may be conducted. From the perspective of cybersecurity, these layers reveal specific avenues of approach for protecting against cyberspace threats.

*For a detailed discussion of the layers in cyberspace, see JP 3-12,* Cyberspace Operations.

e. **Support to Additional Cyberspace Operations**

(1) **DODIN Operations.** The number and complexity of networks and other information capabilities in DOD, including diverse technology implementations and varying standards, makes the securing of all the DODIN exceptionally difficult. Secure networks and other information capabilities are the foundation of the JFCs' confidence, not only in their communications pathways, but in their weapon systems and their very ability to engage and defeat adversaries when required.

(2) **Routine Operations in Cyberspace.** All uses of cyberspace by DOD personnel not conducting OCO, DCO, or DODIN operations are considered routine uses of cyberspace. But routine is not synonymous with unimportant. These cyberspace operations range, on the most mundane end, from sending an administrative announcement via e-mail to, on the strategic end, nuclear C2. DOD personnel undertaking these tasks often take for granted the availability, confidentiality, and integrity of the networks they use. Threats to the security of the DODIN are numerous and complex. The level of effort required to stay abreast of them is significant. While some information capabilities, particularly those used for tactical operations, may be harder for an adversary to exploit due to their isolation from the Internet and their encryption and requirement for specialized hardware, some DOD missions are coordinated and sometimes executed across the Internet. Therefore the importance of sound cybersecurity policy and uncompromising cybersecurity training and oversight of users cannot be overemphasized.

(3) **Information and Communications Technology.** Information and communications technology is rapidly evolving, forcing governments and militaries to rethink the context in which they operate. From around-the-clock news to blogs, social networking, and text messaging, the rapid flow of information has changed the social fabric of the world. The ability of social networks in cyberspace to incite popular support and to spread ideology is not geographically limited, and the continued proliferation of information and communications technology will have profound implications for US national security.

f. **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.

g. **Intelligence Community.** 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, the DOD works with the 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 CI, key leader engagement information, law enforcement information, and other actionable intelligence regarding threats from terrorism, weapons of mass destruction, adversary IO, and CO.

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

> *"Sharing of information is an increasingly important element of Departmental mission success. It is imperative to effectively exchange information among components, Federal agencies, coalition partners, foreign governments and international organizations as a critical element of our efforts to defend the nation and execute national strategy."*
>
> ***Department of Defense Information Sharing Strategy,*** **4 May 2007 Title 10, United States Code, Section 153**

### 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 and during all levels of conflict. 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 a CIE that is 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 communication 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 systems 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

a. The Nuclear Command and Control System (NCCS) comprises the critical core NMCS capability that enables the President to consult with the SecDef, CJCS, CCDRs, and other advisors to assess the scope and intent of a threat, and direct the transfer, deployment, employment 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 in stressed environments. It includes the emergency action message dissemination systems and those systems used for tactical warning/attack assessment, conferencing, force report-back, reconnaissance, retargeting, force management, and requests to use nuclear weapons.

## 3. Intelligence

a. The DODIN enables intelligence and operations information and schematics producing a common operational picture, facilitating interoperability between Service information systems, and providing assured, secure, and tailorable information. The communications networks and information processing, storage, and management systems comprised in 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 and sets 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 layer communications systems will provide additional opportunities for convergence of intelligence communications systems with the DODIN.

c. **Intelligence Communications Planning**

(1) Communications system planning for intelligence must be effectively coordinated between the J-6 and the J-2. 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 (network access to computer databases, direct data transfers, web pages, etc.) requires communications and

computer systems interoperability among joint and multinational forces, component commands, DOD organizations, and the interagency community.

(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 intelligence and communications systems be deployed with significant planning and coordination. The CCMD J-6 and J-2 must sufficiently and effectively understand current systems to tailor an integrated architecture of intelligence sensors, processors, dissemination systems, databases, information systems, and 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 and specific mission requirements; Step 2: J-2 determines specific intelligence communications support plan; Step 3: J-2 compiles the intelligence information that flows from step 2 into a node-to-node layout, including IERs; 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 paths for the JFC and/or subordinate joint force intelligence needs prior to deployment. The J-2 coordinates support from the J-6 for the necessary communications systems, COMSEC, application software, and communications bandwidth needed. By the end of the planning process, the joint force 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 intelligence information to military commanders and national-level decision makers. The 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 attaining interoperability between the tactical, theater, and national intelligence systems and the respective communications system at each level.

(2) In a technical sense, DODIIS is the SCI portion of the DODIN that provides the interface between the CCDRs and the IC. The joint intelligence systems architecture is an integral part of the DODIN, and consists of an integrated network supporting voice, data, and VTC. The JWICS, the Joint Deployable Intelligence Support System, and the Distributed Common Ground System currently form the foundation of the SCI portion of the DODIN. 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 partners 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.

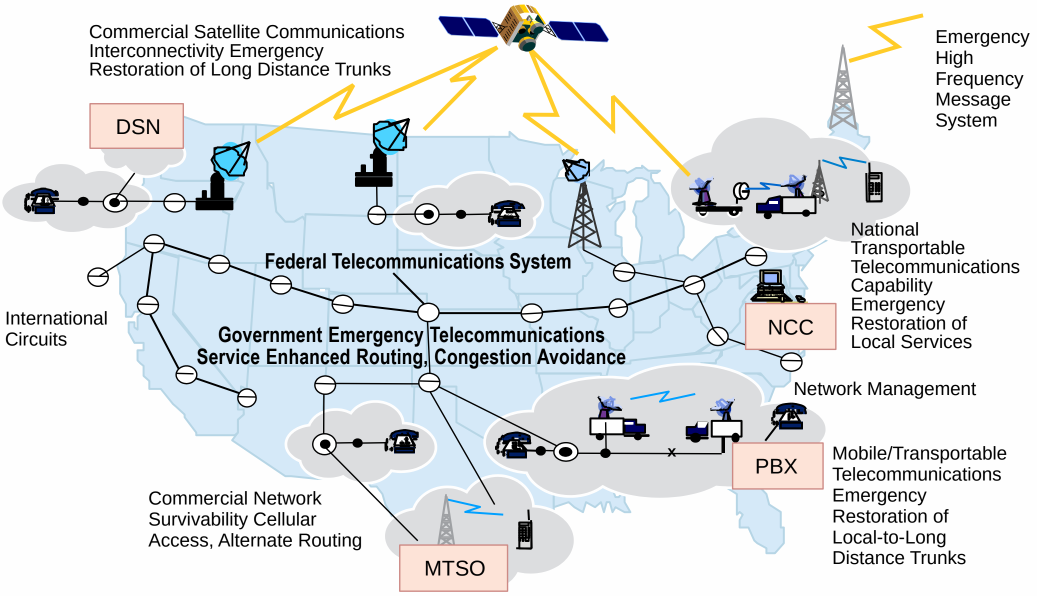
## 4. National Security and Emergency Preparedness Communications

a. DHS Office of Emergency Communications (OEC) leads the national security and emergency preparedness (NS/EP) communications efforts. OEC's programs and services coordinate emergency communications planning, preparation and evaluation, to ensure safer, better-prepared communities nationwide. The SecDef oversees the development, testing, implementation, and sustainment of NS/EP communications that are directly responsive to the national security needs of the President, Vice President, and senior national leadership, including communications with or among the President, Vice President, 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.

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 NSEP telecommunications requirements. To help manage how service providers are selected, the National Security Telecommunications Advisory Committee (NSTAC) was established in 1982 by Executive Order 12382, President's NSTAC. Composed of chief executives from major telecommunications and IT-related companies, the NSTAC provides the President with a unified source of national security telecommunications policy expertise unobtainable solely within the US Government. While the NS/EP Executive Committee serves as the mechanism for federal interagency coordination, the NSTAC and its working group structure are the means for the NS/EP Executive Committee to work with industry to address the range of NSEP telecommunications issues. The Joint Staff J-6 coordinates with the NS/EP Executive Committee through participation on the NSTAC.

## National Security and Emergency Preparedness Communications

National Security and Emergency Preparedness Communications support critical government users in the event of national disasters or war.



Legend

| | | | |
|---|---|---|---|
| DSN | Defense Switched Network | NCC | network control channel |
| MTSO | mobile telephone switching office | PBX | private branch exchange |

**Figure V-1. National Security and Emergency Preparedness Communications**

Intentionally Blank

# APPENDIX A
# DEPARTMENT OF DEFENSE INFORMATION NETWORK COMPONENTS

## 1. Department of Defense Information Network

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

a. **Access Services**

(1) **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.

(2) **DOD Gateway.** In concert with military and commercial communication segments that support DOD missions, the primary interface point between the sustaining base and deployed forces is called the DOD Gateway. The DOD Gateway may include the standardized tactical entry point and upgrades called the Teleport, and the Modernization of Enterprise Terminal programs. The DOD Gateway provides robust worldwide ground entry interface to SATCOM resources and DISN services. The DOD Gateway is designed to meet the requirement of the provisioning of pre-positioned, sustainable DISN services. An equally important result of this upgrade to the DISN has been the improvement and standardization (facilitating interoperability) of the JFC's access to the DISN.

(a) 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 Switched Network. Data will include access to the SIPRNET and the NIPRNET. Video services include access to DISN Video Services. It will also support the JWICS, a SCI-level data, voice, and video services network.

(b) Although the DOD Gateway is implemented globally under a single executive agent, 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 satellite connectivity through the Teleport program. This

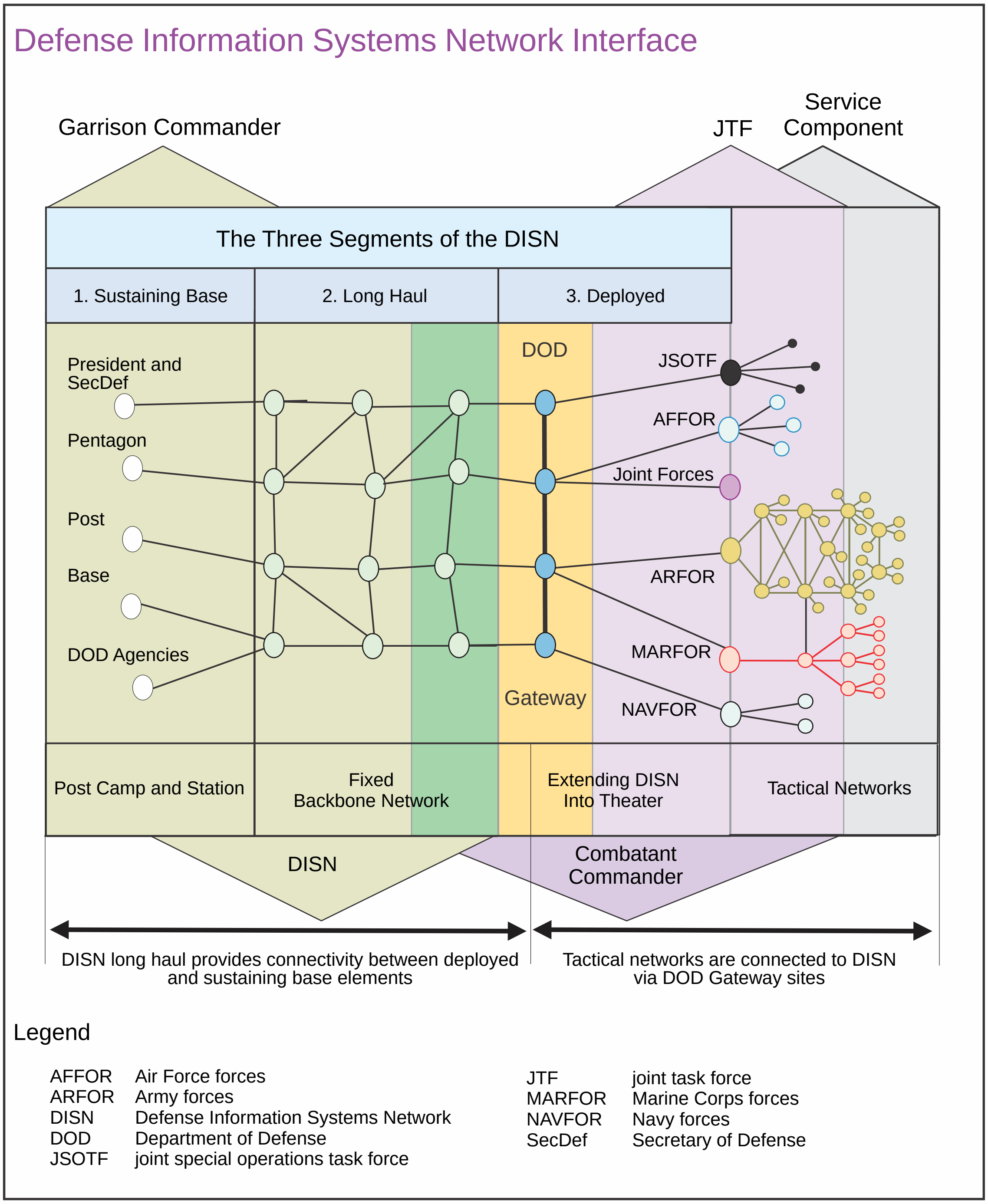
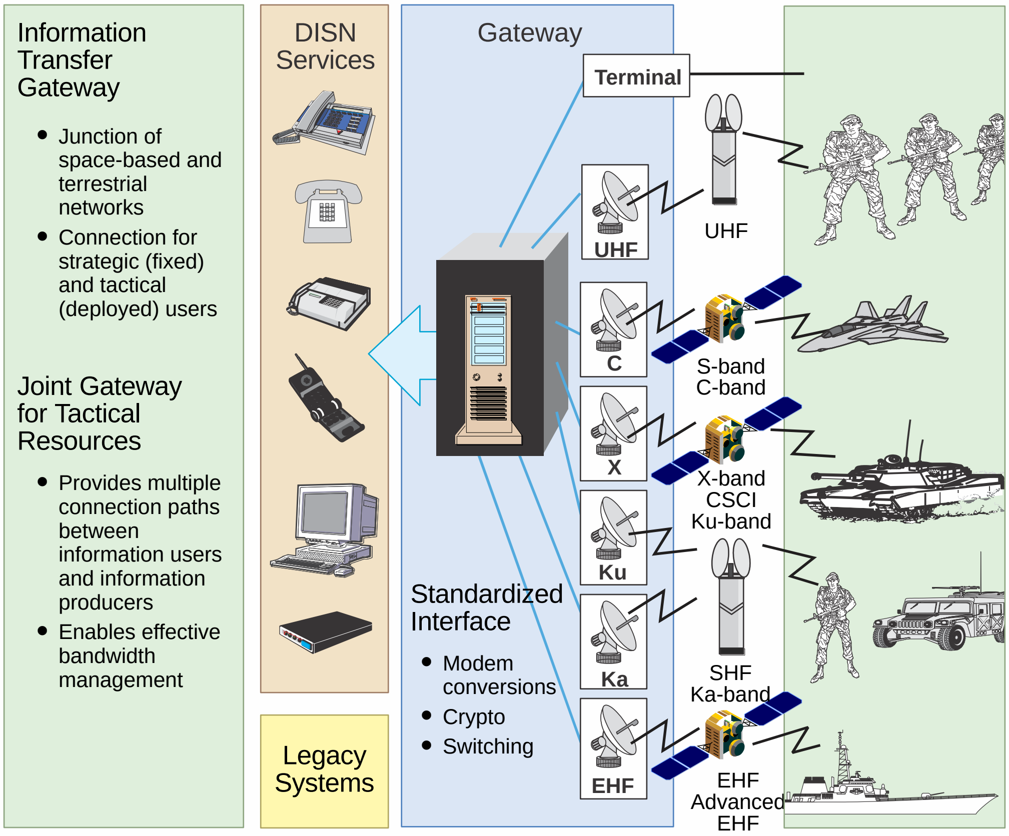

Defense Information Systems Network Interface
Garrison Commander
JTF
Service Component
The Three Segments of the DISN
1. Sustaining Base
2. Long Haul
3. Deployed
President and SecDef
Pentagon
Post
Base
DOD Agencies
DOD
Gateway
JSOTF
AFFOR
Joint Forces
ARFOR
MARFOR
NAVFOR
Post Camp and Station
Fixed Backbone Network
Extending DISN Into Theater
Tactical Networks
DISN
Combatant Commander
DISN long haul provides connectivity between deployed and sustaining base elements
Tactical networks are connected to DISN via DOD Gateway sites
Legend
AFFOR Air Force forces
ARFOR Army forces
DISN Defense Information Systems Network
DOD Department of Defense
JSOTF joint special operations task force
JTF joint task force
MARFOR Marine Corps forces
NAVFOR Navy forces
SecDef Secretary of Defense

**Figure A-1. Defense Information Systems Network Interface**

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.

Department of Defense Gateway


Information Transfer Gateway
• Junction of space-based and terrestrial networks
• Connection for strategic (fixed) and tactical (deployed) users
Joint Gateway for Tactical Resources
• Provides multiple connection paths between information users and information producers
• Enables effective bandwidth management
DISN Services
Legacy Systems
Gateway
Terminal
Standardized Interface
• Modem conversions
• Crypto
• Switching
UHF
C
X
Ku
Ka
EHF
UHF
S-band
C-band
X-band
CSCI
Ku-band
SHF
Ka-band
EHF
Advanced
EHF

Legend

| | | | |
|---|---|---|---|
| CSCI | Commercial Satellite Communications Initiative | Ku | Kurtz-under band |
| C | C-band | S | S-band |
| DISN | Defense Information Systems Network | SHF | super-high frequency |
| EHF | extremely high frequency | UHF | ultrahigh frequency |
| Ka | Kurtz-above band | X | X-band |

**Figure A-2. Department of Defense Gateway**

(3) 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.

b. **Voice Services**

(1) **Defense Switched Network.** A standard unclassified voice network supporting DOD.

(2) **Defense Red Switched Network.** A classified voice network supporting DOD.

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

(4) **Tactical Voice.** Military specific switching system capable of operating in austere areas.

(5) Voice over Internet protocol and voice over secure Internet protocol services.

c. **Transport Services**

(1) **NIPRNET.** An information network for SBU information supporting DOD.

(2) **SIPRNET.** A information network for classified information (up to SECRET) supporting DOD.

(3) **JWICS.** An information network for classified information (up to TOP SECRET), including SCI, supporting DOD.

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

(5) 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.

d. **Applications.** The Global Command and Control System-Joint (GCCS-J), the Theater Battle Management Core Systems (TBMCS), the Army Battle Command System, DOD enterprise collaboration service, and the AMHS discussed in the following paragraphs are illustrative of applications.

(1) GCCS-J is the DOD's computerized system of record for strategic 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 that 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.

(2) **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, Navy, and Marine Corps.

(3) The Army Battle Command System is the Army system-of-information-systems that provides commanders and staffs the ability to execute mission command across echelons during Army and joint operations. Its purpose is to give commanders at brigade/brigade combat team and below a common picture of the operational environment and to facilitate synchronization of combat forces in joint environments.

(4) 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.

(5) **AMHS** is a multilevel secure, high mission assurance system for transmission of record message traffic in support of DOD.

e. **Video Services**

(1) **Defense VTC System—Global.** A classified, 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.

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

(3) **Commercial News Feed.** Commercial news feeds may be rebroadcast over DOD communications systems or received via a commercially leased terminal in support of C2 functions.

f. **SATCOM** is a critical segment of the DODIN that provides the ability to establish or augment the communications system in regions of the world that lack suitable terrestrial infrastructure, such as polar regions, open ocean, and remote areas of the world. SATCOM is detailed more in JP 3-14, *Space Operations.*

g. **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 ESTIMATE PREPARATION 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 communications system planner will develop the communications system estimate by identifying, coordinating, and integrating communications system support.

## 3. Developing the Communications System Estimate Analysis

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 results.

(3) Actions required to achieve results.

(4) Location of required results.

(5) Timing of required results.

(6) Limitations on freedom of action.

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 tactical air operations.

2. Air-to-ground operations.

3. Naval surface fire support operations.

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., video teleconference).

(i) Threat and vulnerability assessment of communications systems 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, etc.

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

i. Develop assumptions to replace missing or unknown information. NOTE: 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. See J-3/plans directorate of a joint staff (J-5) (operations/plans).

(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/J-5/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 assist in determining requirements and the communications system architecture.

b. For combat operations:

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

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

(a) State clearly 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.

c. For noncombat operations:

(1) Review the mission analysis and JFC's guidance (e.g., commander's intent).

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

(a) Clearly state what is to be accomplished.

(b) Specify ways (operations) and means (forces) to provide communications system support to accomplish objectives.

(c) 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.

(3) Identify the force requirements for communications system resources.

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

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

a. Gather tools.

(1) Identify the adversary 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 adversary dispositions.

b. Identify the available joint forces and augmentation from:

(1) USSTRATCOM (e.g., CSE, cyberspace mission forces, space support team, RSSC).

(2) DISA (e.g., Joint Spectrum Center).

(3) JCSE/ United States Transportation Command controlled assets.

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 allow 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 adversary 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 adversary and friendly COAs.

## 7. Participate in the Course of Action Comparison

Test 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 adversary and friendly centers of gravity?

b. Preliminary 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. Preliminary 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. Preliminary 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 non-organic capabilities required?

(b) Are en route communications required?

h. Ensure that 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

Note: Steps 1-6 above contain most of the information needed to complete annex K.

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.

(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 adversary 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 that permits the 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) The use of liaison officers/teams to provide a means to facilitate interoperability during different tactical phases of an operation.

(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 that includes a diversity of communications routes, hardening and protection of equipment and communications sites, and availability of alternate modular communications system packages.

(g) Redundancy that provides diversity of paths over multiple media means, with available replacement systems and repair parts. The goal is timely, reliable information flow.

(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 electromagnetic interference. 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) Cybersecurity principles must be included to minimize the threats posed by computer viruses, hackers, and cyberspace attacks.

(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 command 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 operational IERs with communications system capabilities and assets.

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

(a) Use available automated planning tools.

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

(c) Describe the interconnection of modular packages to communications system and the resulting communications system networks. Consider using an automated planning tool, then comparing 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.

(a) Ensure a trained spectrum manager is available with necessary tools and resources.

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

(c) Ensure that spectrum-dependent 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 joint CEOI.

(f) Coordinate with the J-2/J-3 to plan in developing 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.

Intentionally Blank

# APPENDIX C
## REFERENCES

### 1. General Publications

a. 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, Cybersecurity Policy.

e. National Strategy for Information Sharing and Safeguarding.

### 2. Department of Defense Publications

a. DODD 3020.40, *DOD Policy and Responsibilities for Critical Infrastructure.*

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

f. DODD 5530.3, *International Agreements.*

g. DODD 8000.01, *Management of the Department of Defense Information Enterprise.*

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

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

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

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

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

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

n. DODI 8500.01, *Cybersecurity.*

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

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

q. DODI 8550.01, *DOD Internet Services and Internet-Based Capabilities.*

r. Department of Defense Information Sharing Strategy.

## 3. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 2700.01E, *International Military Agreements for Rationalization, Standardization, and Interoperability (RSI) Between the United States, Its Allies, and Other Friendly Nations.*

b. CJCSI 3150.25, *Joint Lessons Learned Program.*

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

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

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

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

g. CJCSI 3320.03C, *Joint Communications Electronics Operating Instructions.*

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

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

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

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

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

m. CJCSI 6250.01E, *Satellite Communications.*

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

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

p. CJCSI 6510.06C, *Communications Security Releases to Foreign Nations.*

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

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

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

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

u. CJCSM 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance.*

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

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

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

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

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

aa. CJCSM 6120.01F, *Joint Multi-Tactical Data Link Operating Overview*.

bb. CJCSM 6231.01D, *Manual for Employing Joint Tactical Communications.*

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

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

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

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

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

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

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

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

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

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

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

## 4. Other Publication

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

# APPENDIX D
## ADMINISTRATIVE INSTRUCTIONS

### 1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Joint Staff J-7, Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

### 2. Authorship

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

### 3. Supersession

This publication supersedes JP 6-0, *Joint Communications System*, 10 June 2010.

### 4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J-7-JED//

b. Routine changes should be submitted electronically to the Deputy Director, Joint Education and Doctrine, ATTN: Joint Doctrine Analysis Division, 116 Lake View Parkway, Suffolk, VA 23435-2697, and info the lead agent and the Director for Joint Force Development, J-7/JED.

c. 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. 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.*

## 6. 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 http://jdeis.js.smil.mil/jdeis/index.jsp (SIPRNET), and on the JEL at http://www.dtic.mil/doctrine (NIPRNET).

b. Only approved JPs are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified JP to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to Defense Intelligence Agency, ATTN: 7400 Pentagon, Office of Partnership Engagement, OPE, Washington, DC 20301-7400.

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 AND ACRONYMS

| | |
|---|---|
| A2 | antiaccess |
| ACP | Allied communications publication |
| AD | area denial |
| AMHS | automated message handling system |
| AOR | area of responsibility |
| APEX | Adaptive Planning and Execution |
| 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 |
| CDRUSSTRATCOM | Commander, United States Strategic Command |
| CEOI | communications-electronics operating instructions |
| CI | counterintelligence |
| 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 |
| COMSEC | communications security |
| CSE | cyberspace support element |
| 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 |
| EMS | electromagnetic spectrum |
| 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 |
| | |
| HQ | headquarters |
| | |
| IAW | in accordance with |
| IC | intelligence community |
| IER | information exchange requirement |
| IGO | intergovernmental organization |
| IM | information management |
| ISR | intelligence, surveillance, and reconnaissance |
| 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-5 | plans directorate of a joint staff |
| J-6 | communications system directorate of a joint staff |
| JCC | joint cyberspace center |
| JCN | joint communications node |
| JCSE | Joint Communications Support Element (USTRANSCOM) |
| JDN | joint data network |
| JFC | joint force commander |
| JFHQ | joint force headquarters |
| 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 |
| | |
| LE | law enforcement |
| | |
| MARS | Military Auxiliary Radio System |
| MC4EB | Military Command, Control, Communications and Computers Executive Board |
| MILDEP | Military Department |
| | |
| NATO | North Atlantic Treaty Organization |
| NCCS | Nuclear Command and Control System |
| NG JFHQ-State | National Guard joint force headquarters-state |
| NGO | nongovernmental organization |
| NIPRNET | Nonsecure 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 |
| NSS | national security system |
| NSTAC | National Security Telecommunications Advisory Committee |
| | |
| OCO | offensive cyberspace operations |
| OEC | Office of Emergency Communications (DHS) |
| OPLAN | operation plan |
| OPORD | operation order |
| | |
| RSSC | regional satellite communications support center |
| | |
| SA | situational awareness |
| SATCOM | satellite communications |
| SBU | sensitive but unclassified |
| 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 |
| | |
| UCP | Unified Command Plan |
| UHF | ultrahigh frequency |
| USCYBERCOM | United States Cyber Command |
| USG | United States Government |
| USNORTHCOM | United States Northern Command |
| USSTRATCOM | United States Strategic Command |
| | |
| VTC | video teleconferencing |
| | |
| WAN | wide-area network |

## PART II—TERMS AND DEFINITIONS

**active communications satellite**. None. (Approved for removal from JP 1-02.)

**capstone requirements document**. None. (Approved for removal from JP 1-02.)

**command and control system.** The facilities, equipment, communications, procedures, and personnel essential for a commander to plan, direct, and control operations of assigned and attached forces pursuant to the missions assigned. (Approved for incorporation into JP 1-02.)

**commonality.** A quality that applies to materiel or systems: a. possessing like and interchangeable characteristics enabling each to be utilized, or operated and maintained, by personnel trained on the others without additional specialized training; b. having interchangeable repair parts and/or components; and c. applying to consumable items interchangeably equivalent without adjustment. (JP 1-02. SOURCE: JP 6-0)

**communicate.** None. (Approved for removal from JP 1-02.)

**communications network.** An organization of stations capable of intercommunications, but not necessarily on the same channel. Also called **COMNET.** (Approved for incorporation into JP 1-02.)

**communications satellite.** None. (Approved for removal from JP 1-02.)

**communications security.** The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called **COMSEC.** (JP 1-02. SOURCE: JP 6-0)

**computer security.** None. (Approved for removal from JP 1-02.)

**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. Also called **CM.** (Approved for incorporation into JP 1-02.)

**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 JP 1-02.)

**defense message system.** None. (Approved for removal from JP 1-02.)

**Defense Switched Network.** The component of the Defense Communications System that handles Department of Defense voice, data, and video communications. Also called **DSN.** (Approved for incorporation into JP 1-02.)

**Department of Defense information network.** The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Also called **DODIN.** (Approved for replacement of "Department of Defense information networks" and its definition in JP 1-02.)

**emission security.** The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. (JP 1-02. SOURCE: JP 6-0)

**frequency management.** None. (Approved for removal from JP 1-02.)

**Global Command and Control System.** A deployable command and control system supporting forces for joint and multinational operations across the range of military operations with compatible, interoperable, and integrated communications systems. Also called **GCCS.** (JP 1-02. SOURCE: JP 6-0)

**Global Information Grid.** None. (Approved for removal from JP 1-02.)

**Global Network Operations Center.** None. (Approved for removal from JP 1-02.)

**immediate message.** None. (Approved for removal from JP 1-02.)

**interoperability.** 1. The ability to operate in synergy in the execution of assigned tasks. (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. (JP 6-0) (Approved for incorporation into JP 1-02.)

**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.** (Approved for incorporation into JP 1-02.)

**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 systems. Also called **JNCC.** (Approved for incorporation into JP 1-02.)

**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.** (JP 3-61) (Approved for incorporation into JP 1-02.)

**Military Affiliate Radio System.** None. (Approved for removal from JP 1-02.)

**minimize.** A condition wherein normal message and telephone traffic is drastically reduced in order that messages connected with an actual or simulated emergency shall not be delayed. (JP 1-02. SOURCE: JP 6-0)

**National Communications System.** The telecommunications system that results from the technical and operational integration of the separate telecommunications systems of the several executive branch departments and agencies having a significant telecommunications capability. Also called **NCS.** (JP 1-02. SOURCE: JP 6-0)

**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.** (JP 1-02. SOURCE: JP 6-0)

**network operations.** None. (Approved for removal from JP 1-02.)

**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. (JP 1-02. SOURCE: JP 3-0)

**physical security.** 1. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 3-0) 2. In communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JP 1-02. SOURCE: JP 6-0)

**SECRET Internet Protocol Router Network.** The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called **SIPRNET.** (JP 1-02. SOURCE: JP 6-0)

**signal operating instructions.** A series of orders issued for technical control and coordination of the signal communication activities of a command. In Marine Corps usage, these instructions are designated communication operation instructions. Also called **SOI.** (Approved for incorporation into JP 1-02.)

**tactical data link.** A Joint Staff-approved, standardized communication link suitable for transmission of digital information, which interfaces two or more command and control or weapons systems via a single or multiple network architecture and multiple communication media for exchange of tactical information. Also called **TDL.** (Approved for incorporation into JP 1-02.)

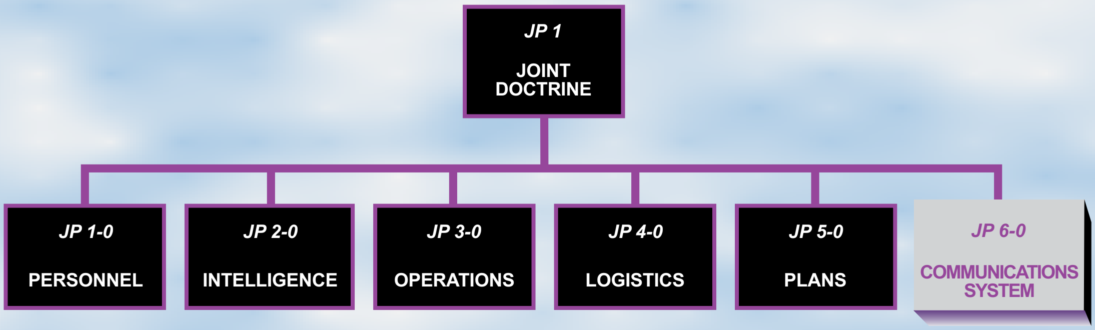
**telecommunications.** Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. (JP 1- 02. SOURCE: JP 6-0)

**traffic flow security.** None. (Approved for removal from JP 1-02.)

**transmission security.** The component of communications security that results from all measures designed to protect communications from interception and exploitation by means other than cryptanalysis. Also called **TRANSEC.** (Approved for incorporation into JP 1-02.)

Intentionally Blank

# JOINT DOCTRINE PUBLICATIONS HIERARCHY



*JP 1*

JOINT DOCTRINE

*JP 1-0*

PERSONNEL

*JP 2-0*

INTELLIGENCE

*JP 3-0*

OPERATIONS

*JP 4-0*

LOGISTICS

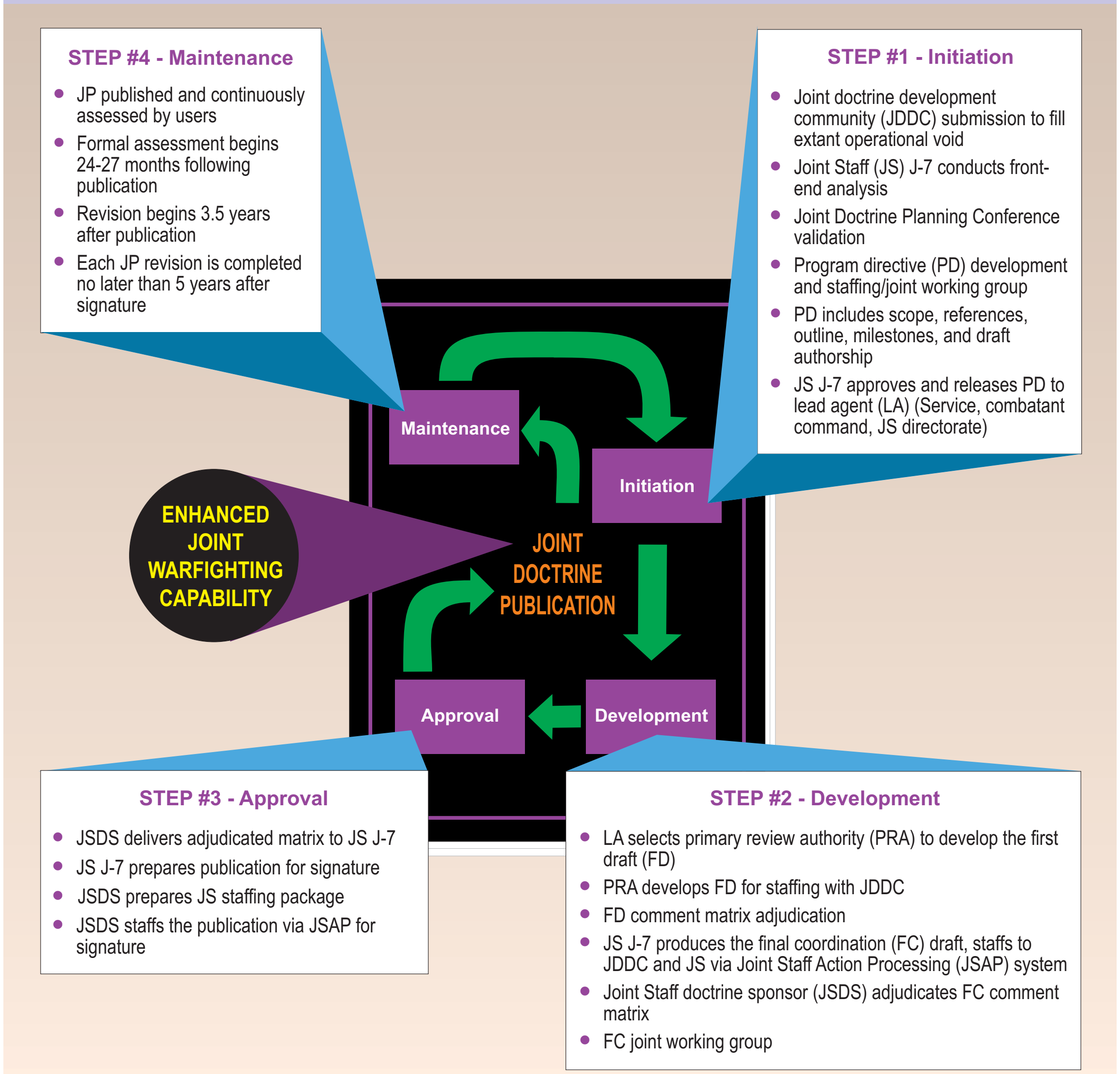
*JP 5-0*

PLANS

*JP 6-0*

COMMUNICATIONS SYSTEM

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)

Maintenance

Initiation

ENHANCED JOINT WARFIGHTING CAPABILITY

JOINT DOCTRINE PUBLICATION

Approval

Development

### 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