Joint Publication 3-12

Cyberspace Operations

8 June 2018

PREFACE

1. Scope

This publication provides joint doctrine to plan, execute, and assess cyberspace 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 it provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners. 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 and executing their plans and orders. 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 objectives.

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 US, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

KEVIN D. SCOTT
Vice Admiral, USN
Director, Joint Force Development

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-12
DATED 05 FEBRUARY 2013

- **Changes the format from a classified publication to an unclassified publication with a classified appendix.**
- **Reflects United States Cyber Command as a functional combatant command.**
- **Incorporates discussion of the Cyber Mission Force.**
- **Expands the discussion of command and control of cyberspace operations (CO).**
- **Includes discussion of information as a joint function.**
- **Enhances the discussion of CO planning considerations.**

Intentionally Blank

TABLE OF CONTENTS

APPENDIX

GLOSSARY

FIGURE

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses the Nature of Cyberspace**
- **Describes how to integrate Cyberspace Operations with Other Operations**
- **Discusses Cyberspace Operations Forces**
- **Outlines Challenges to the Joint Force's Use of Cyberspace**
- **Describes Cyberspace Operations Core Activities**
- **Outlines Authorities, Roles, and Responsibilities related to Cyberspace Operations**
- **Discusses Planning, Coordination, Execution, and Assessment of Cyberspace Operations**

Overview of Cyberspace and Cyberspace Operations

Cyberspace operations (CO) is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

This publication focuses on military operations in and through cyberspace; explains the relationships and responsibilities of the Joint Staff (JS), combatant commands (CCMDs), United States Cyber Command (USCYBERCOM), the Service cyberspace component (SCC) commands, and combat support agencies; and establishes a framework for the employment of cyberspace forces and capabilities.

The Nature of Cyberspace

Relationship with the Physical Domains. Cyberspace, while part of the information environment, is dependent on the physical domains of air, land, maritime, and space.

CO use links and nodes located in the physical domains and perform logical functions to create effects first in cyberspace and then, as needed, in the physical domains. Actions in cyberspace, through carefully controlled cascading effects, can

enable freedom of action for activities in the physical domains.

Cyberspace Layer Model. To assist in the planning and execution of CO, cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona.

Department of Defense (DOD) Cyberspace. The Department of Defense information network (DODIN) is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

Connectivity and Access. Gaining access to operationally useful areas of cyberspace, including targets within them, is affected by legal, policy, or operational limitations. For all of these reasons, access is not guaranteed. Additionally, achieving a commander's objectives can be significantly complicated by specific elements of cyberspace being used by enemies, adversaries, allies, neutral parties, and other United States Government (USG) departments and agencies, all at the same time.

The operational environment (OE) is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and impact the decisions of the commander assigned responsibility for it. The information environment permeates the physical domains and therefore exists in any OE.

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

Given that cyberspace is wholly contained within the information environment and the chief purpose of information operations (IO) is to create effects in the information environment, there is significant interdependency between IO and CO.

Integrating Cyberspace Operations with Other Operations

During joint planning, cyberspace capabilities are integrated into the joint force commander's (JFC's) plans and synchronized with other operations across the range of military operations. While not the norm, some military objectives can be achieved by CO alone. Commanders conduct CO to obtain or retain freedom of maneuver in cyberspace, accomplish JFC objectives, deny freedom of action to the threat, and enable other operational activities.

Cyberspace Operations Forces

Commander, United States Cyber Command (CDRUSCYBERCOM), commands a preponderance of the cyberspace forces that are not retained by the Services. USCYBERCOM accomplishes its missions within three primary lines of operation: secure, operate, and defend the DODIN; defend the nation from attack in cyberspace; and provide cyberspace support as required to combatant commanders (CCDRs).

The Services man, train, and equip cyberspace units and provide them to USCYBERCOM through the SCCs.

Challenges to the Joint Force's Use of Cyberspace

Threats. Cyberspace presents the JFC's operations with many threats, from nation-states to individual actors to accidents and natural hazards.

Anonymity and Difficulties with Attribution. To initiate an appropriate defensive response, attribution of threats in cyberspace is crucial for any actions external to the defended cyberspace beyond authorized self-defense.

Geography Challenges. In cyberspace, there is no stateless maneuver space. Therefore, when US military forces maneuver in foreign cyberspace, mission and policy requirements may require they

maneuver clandestinely without the knowledge of the state where the infrastructure is located.

Technology Challenges. Using a cyberspace capability that relies on exploitation of technical vulnerabilities in the target may reveal its functionality and compromise the capability's effectiveness for future missions.

Private Industry and Public Infrastructure. Many of DOD's critical functions and operations rely on contracted commercial assets, including Internet service providers (ISPs) and global supply chains, over which DOD and its forces have no direct authority.

Globalization. The combination of DOD's global operations with its reliance on cyberspace and associated technologies means DOD often procures mission-essential information technology products and services from foreign vendors.

Mitigations. DOD partners with the defense industrial base (DIB) to increase the security of information about DOD programs residing on or transiting DIB unclassified networks.

Cyberspace Operations Core Activities

CO comprise the military, national, and ordinary business operations of DOD in and through cyberspace. Although commanders need awareness of the potential impact of the other types of DOD CO on their operations, the military component of CO is the only one guided by joint doctrine and is the focus of this publication. CCDRs and Services use CO to create effects in and through cyberspace in support of military objectives. Military operations in cyberspace are organized into missions executed through a combination of specific actions.

Military Operations In and Through Cyberspace

Cyberspace Missions. All actions in cyberspace that are not cyberspace-enabled activities are taken as part of one of three cyberspace missions: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), or DODIN

operations. These three mission types comprehensively cover the activities of the cyberspace forces. The successful execution of CO requires integration and synchronization of these missions.

DODIN Operations. The DODIN operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN.

DCO. DCO missions are executed to defend the DODIN, or other cyberspace DOD cyberspace forces have been ordered to defend, from active threats in cyberspace.

OCO. OCO are CO missions intended to project power in and through foreign cyberspace through actions taken in support of CCDR or national objectives.

National Intelligence Operations In and Through Cyberspace

National-level intelligence organizations conduct intelligence activities in, through, and about cyberspace in response to national intelligence priorities. This intelligence can support a military commander's planning and preparation.

Department of Defense Ordinary Business Operations In and Through Cyberspace

Ordinary business operations in and through cyberspace are "cyberspace-enabled activities" that comprise those non-intelligence and non-warfighting capabilities, functions, and actions used to support and sustain DOD forces and components.

The Joint Functions and Cyberspace Operations

Command and Control (C2). Cyberspace provides communications pathways, planning and decision-support aids, and cyberspace-related intelligence to enable timely decision making and execution of those decisions. This provides the commander the advantage of controlling the timing and tempo of operations.

Intelligence. Understanding the OE is fundamental to all joint operations, including CO. Intelligence may be derived from information

gained during military operations in cyberspace or from other sources.

Fires. Cyberspace attack capabilities create fires in and through cyberspace and are often employed with little or no associated physical destruction. However, modification or destruction of computers that control physical processes can lead to cascading effects (including collateral effects) in the physical domains.

Movement and Maneuver. Cyberspace operations enable force projection without the need to establish a physical presence in foreign territory. Maneuver in the DODIN or other blue cyberspace includes positioning of forces, sensors, and defenses to best secure areas of cyberspace or engage in defensive actions as required. Maneuver in gray and red cyberspace is a cyberspace exploitation action and includes such activities as gaining access to adversary, enemy, or intermediary links and nodes and shaping this cyberspace to support future actions.

Sustainment. From the perspective of cyberspace-enabled activities in support of global logistics, DOD relies on protected DODIN and commercial network segments to coordinate sustainment of forces.

Protection. Protection of the DODIN and other critical US cyberspace includes the continuous and synchronized integration of cyberspace security and, when required, cyberspace defense actions.

Information. The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence perceptions, behavior, action or inaction, and human and automated decision making.

Authorities, Roles, and Responsibilities

Under the authorities of the Secretary of Defense (SecDef), DOD uses cyberspace capabilities to shape cyberspace and provide integrated offensive

and defensive options for the defense of the nation. USCYBERCOM coordinates with CCMDs, the JS, and the Office of the Secretary of Defense; liaises with other USG departments and agencies; and, in conjunction with the Department of Homeland Security, DOD's Department of Defense Cyber Crime Center, and the Defense Security Service, liaises with members of the DIB. Similarly, as directed, DOD deploys necessary resources to support efforts of other USG departments and agencies, and allies.

Authorities

Authority for CO actions undertaken by the US Armed Forces is derived from the US Constitution and federal law. Key laws that apply to DOD include Title 10, United States Code (USC), *Armed Forces;* Title 50, USC, *War and National Defense;* and Title 32, USC, *National Guard.*

Authorities for specific types of military CO are established within SecDef policies, including DOD instructions, directives, and memoranda, as well as in execute orders and operation orders authorized by the President or SecDef and subordinate orders issued by commanders approved to execute the subject missions.

Roles and Responsibilities

SecDef. Directs the military, intelligence, and ordinary business operations of DOD in cyberspace.

Chairman of the Joint Chiefs of Staff (CJCS). As the global integrator advises the President and SecDef on operational policies, responsibilities, and programs.

Service Chiefs. Provide appropriate administration of and support to cyberspace forces, including Service-retained forces and forces assigned or attached to CCMDs.

Chief, National Guard Bureau (NGB). Advises CDRUSCYBERCOM on NGB matters pertaining to CCMD CO missions, and supports planning and coordination for such activities as requested by the CJCS or the CCDRs.

CDRUSCYBERCOM. As the coordinating authority for CO, plans, coordinates, integrates, synchronizes, and conducts activities to:

- Direct the security, operations, and defense of the DODIN.
- Prepare to, and when directed, conduct military CO external to the DODIN, including in gray and red cyberspace, in support of national objectives.

Other CCDRs. Secure, operate, and defend tactical and constructed DODIN segments within their commands and areas of responsibility.

Director, Defense Information Systems Agency (DISA). Complies with the commander of Joint Force Headquarters-Department of Defense Information Network's direction to execute DODIN operations and defensive cyberspace operations-internal defensive measures (DCO-IDM) missions at the global and enterprise level, within DISA-operated portions of the DODIN.

Director, National Security Agency/Chief, Central Security Service. Provides signals intelligence support and cybersecurity guidance and assistance to DOD components and national customers.

Director, Defense Intelligence Agency. Provides timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policy makers.

Legal Considerations

DOD conducts CO consistent with US domestic law, applicable international law, and relevant USG and DOD policies. The laws that regulate military actions in US territory also apply to cyberspace. Therefore, DOD cyberspace forces that operate outside the DODIN, when properly authorized, are generally limited to operating in gray and red cyberspace only, unless they are issued different rules of engagement or conducting defense support of civil authorities (DSCA) under appropriate authority. Since each CO mission has

unique legal considerations, the applicable legal framework depends on the nature of the activities to be conducted, such as OCO or DCO, DSCA, ISP actions, law enforcement and counterintelligence activities, intelligence activities, and defense of the homeland.

Planning, Coordination, Execution, and Assessment

Joint Planning Process and Cyberspace Operations

Commanders plans should address how to effectively integrate cyberspace capabilities, counter adversaries' use of cyberspace, identify and secure mission-critical cyberspace, access key terrain in cyberspace, operate in a degraded environment, efficiently use limited cyberspace assets, and pair operational requirements with cyberspace capabilities.

Cyberspace Operations Planning Considerations

While many elements of cyberspace can be mapped geographically, a full understanding of an adversary's disposition and capabilities in cyberspace involves understanding the target, not only at the underlying physical network layer but also at the logical network layer and cyber-persona layer, including profiles of system users and administrators and their relationship to adversary critical factors.

Characteristics of Cyberspace Capabilities. While cyberspace is complex and ever changing, cyberspace capabilities, whether devices or computer programs, must reliably create the intended effects. However, cyberspace capabilities are developed based on environmental assumptions and expectations about the operating conditions that will be found in the OE.

Cascading, Compounding, and Collateral Effects. Overlaps among military, other government, corporate, and private activities on shared networks in cyberspace make the evaluation of probable cascading, compounding, and collateral effects particularly important when targeting for CO.

DODIN operations underpin nearly every aspect of military operations, and this reliance on cyberspace

is well understood by our adversaries. However, a commander's reliance on specific segments of the DODIN is often not considered during plans development, but planning for DODIN resiliency is essential. JFC planning staffs should incorporate DCO-IDM branches and sequels for any operations that pose an increased threat to the DODIN.

Intelligence and Operational Analytic Support to Cyberspace Operations Planning

Intelligence requirements (IRs). During mission analysis, the joint force staff identifies significant information gaps about the adversary and other relevant aspects of the OE. After gap analysis, the staff formulates IRs, which are general or specific subjects upon which there is a need for the collection of information or the production of intelligence.

Targeting

Three fundamental aspects of CO require consideration in the targeting processes: recognizing cyberspace capabilities are a viable option for engaging some designated targets; understanding a CO option may be preferable in some cases, because it may offer low probability of detection and/or no associated physical damage; and higher-order effects on targets in cyberspace may impact elements of the DODIN, including retaliation for attacks attributed to the joint force.

Command and Control of Cyberspace Forces

The complex nature of CO, where cyberspace forces can be simultaneously providing actions at the global level and at the theater or joint operations area level, requires adaptations to traditional C2 structures. Joint forces principally employ centralized planning with decentralized execution of operations. CO require constant and detailed coordination between theater and global operations, creating a dynamic C2 framework that can adapt to the constant changes, emerging threats, and unknowns. Certain CO functions, including protection of the DODIN's global networks and pursuit of global cyberspace threats, lend themselves to centralized planning and execution to meet multiple, near-instantaneous requirements for response. Centrally controlled CO should be integrated and synchronized with the CCDR's regional or local CO, conducted by forces assigned or attached to the CCDR, or in support of the CCDR.

Synchronization of Cyberspace Operations

The pace of CO requires significant pre-operational collaboration and constant vigilance after initiation, for effective coordination and deconfliction throughout the OE. Keys to this synchronization are maintaining cyberspace situational awareness and assessing the potential impacts to the joint force of any planned CO, including the protection posture of the DODIN, changes from normal network configuration, or observed indications of malicious activity.

Assessment of Cyberspace Operations

The assessment process for external CO missions begins during planning and includes measures of performance and measures of effectiveness of fires and other effects in cyberspace, as well as their contribution to the larger operation or objective. Historically, combat assessment has emphasized the battle damage assessment (BDA) component of measuring physical and functional damage, but this approach does not always represent the most complete effect, particularly with respect to CO. CO effects are often created outside the scope of battle and often do not create physical damage. Assessing the impact of CO effects requires typical BDA analysis and assessment of physical, functional, and target system components.

CONCLUSION

This publication provides joint doctrine to plan, execute, and assess cyberspace operations.

Intentionally Blank

CHAPTER I
OVERVIEW OF CYBERSPACE AND CYBERSPACE OPERATIONS

"... the United States (US) Department of Defense (DOD) is responsible for defending the US homeland and US interests from attack, including attacks that may occur in cyberspace. ... the DOD seeks to deter attacks and defend the US against any adversary that seeks to harm US national interests during times of peace, crisis, or conflict. To this end, the DOD has developed capabilities for cyberspace operations and is integrating those capabilities into the full array of tools that the US government uses to defend US national interests…"

***The Department of Defense Cyber Strategy*, April 2015**

1. Introduction

a. Most aspects of joint operations rely in part on cyberspace, which is the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations (CO) is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

b. This publication focuses on military operations in and through cyberspace; explains the relationships and responsibilities of the Joint Staff (JS), combatant commands (CCMDs), United States Cyber Command (USCYBERCOM), the Service cyberspace component (SCC) commands, and combat support agencies (CSAs); and establishes a framework for the employment of cyberspace forces and capabilities. Cyberspace forces are those personnel whose primary duty assignment is to a CO mission.

c. **The Impact of Cyberspace on Joint Operations**

(1) Cyberspace capabilities provide opportunities for the US military, its allies, and partner nations (PNs) to gain and maintain continuing advantages in the operational environment (OE) and enable the nation's economic and physical security. Cyberspace reaches across geographic and geopolitical boundaries and is integrated with the operation of critical infrastructures, as well as the conduct of commerce, governance, and national defense activities. Access to the Internet and other areas of cyberspace provides users operational reach and the opportunity to compromise the integrity of critical infrastructures in direct and indirect ways without a physical presence. The prosperity and security of our nation are significantly enhanced by our use of cyberspace, yet these same developments have led to increased exposure of vulnerabilities and a critical dependence on cyberspace, for the US in general and the joint force in particular.

(2) Although it is possible for CO to produce stand-alone tactical, operational, or strategic effects and thereby achieve objectives, commanders integrate most CO with other

operations to create coordinated and synchronized effects required to support mission accomplishment.

(3) Permanent global cyberspace superiority is not possible due to the complexity of cyberspace. Even local superiority may be impractical due to the way IT is implemented; the fact US and other national governments do not directly control large, privately owned portions of cyberspace; the broad array of state and non-state actors; the low cost of entry; and the rapid and unpredictable proliferation of technology. Therefore, commanders should be prepared to conduct operations under degraded conditions in cyberspace. Commanders can manage resulting risks using threat mitigation actions; post-impact recovery measures; clear, defensive priorities; primary/secondary/tertiary communication means; and other measures to accomplish their mission and ensure critical data reliability. Once one segment of a network has been exploited or denied, the perception of data unreliability may inappropriately extend beyond the compromised segment due to uncertainty about how networks interact. Therefore, it is imperative commanders be well informed of the status of the portions of cyberspace upon which they depend and understand the impact to planned and ongoing operations.

2. The Nature of Cyberspace

a. **Relationship with the Physical Domains.** Cyberspace, while part of the information environment, is dependent on the air, land, maritime, and space physical domains. Much as operations in the physical domains rely on physical infrastructure created to take advantage of naturally occurring features, operations in cyberspace rely on networked, stand-alone, and platform-embedded IT infrastructure, in addition to the data that resides on and is transmitted through these components to enable military operations in a man-made domain. CO use links and nodes located in the physical domains and perform logical functions to create effects first in cyberspace and then, as needed, in the physical domains. Actions in cyberspace, through carefully controlled cascading effects, can enable freedom of action for activities in the physical domains. Likewise, activities in the physical domains can create effects in and through cyberspace by affecting the electromagnetic spectrum (EMS) or the physical infrastructure. The relationship between space and cyberspace is unique in that virtually all space operations depend on cyberspace, and a critical portion of cyberspace bandwidth can only be provided via space operations, which provide a key global connectivity option for CO. These interrelationships are important considerations during planning. While domains are useful constructs for visualizing and characterizing the physical environment in which operations are conducted (i.e., the operational area [OA]), the use of the term “domain” is not meant to imply or mandate exclusivity, primacy, or command and control (C2) in any domain.

b. **Cyberspace Layer Model.** To assist in the planning and execution of CO, cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona (see Figure I-1). Each layer represents a different focus from which CO may be planned, conducted, and assessed.

(1) The **physical network layer** consists of the IT devices and infrastructure in the physical domains that provide storage, transport, and processing of information within

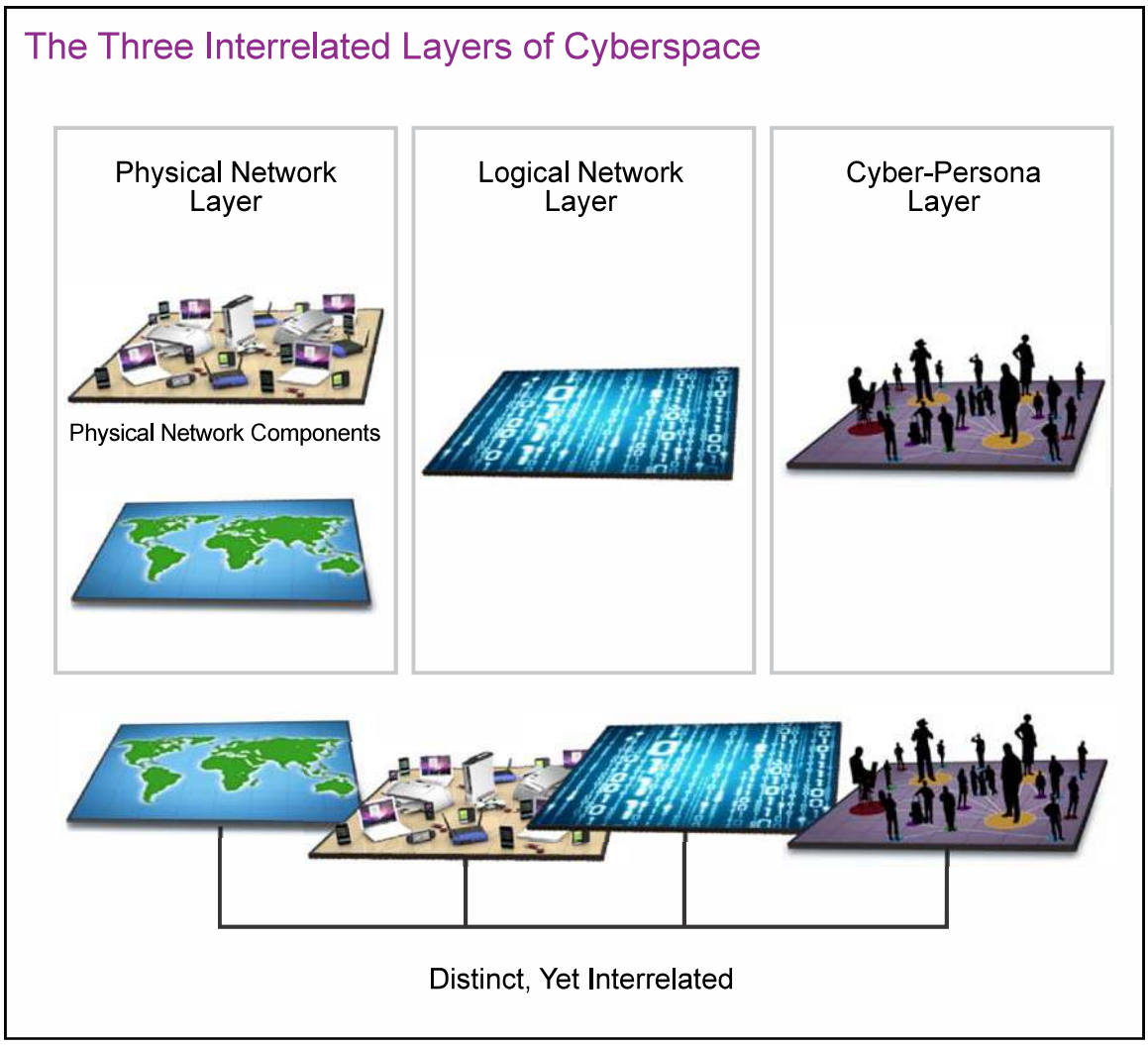


Figure I-1. The Three Interrelated Layers of Cyberspace

cyberspace, to include data repositories and the connections that transfer data between network components. The physical network components include the hardware and infrastructure (e.g., computing devices, storage devices, network devices, and wired and wireless links). Components of the physical network layer require physical security measures to protect them from physical damage or unauthorized physical access, which may be leveraged to gain logical access. The physical network layer is the first point of reference CO use to determine geographic location and appropriate legal framework. While geopolitical boundaries can easily and quickly be crossed in cyberspace, there are still sovereignty issues tied to the physical domains. Every physical component of cyberspace is owned by a public or private entity, which can control or restrict access to their components. These unique characteristics of the OE must be taken into consideration during all phases of planning.

(2) The **logical network layer** consists of those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components (i.e., the relationships are not

necessarily tied to a specific physical link or node, but to their ability to be addressed logically and exchange or process data). Individual links and nodes are represented in the logical layer but so are various distributed elements of cyberspace, including data, applications, and network processes not tied to a single node. An example is the Joint Knowledge Online Website, which exists on multiple servers in multiple locations in the physical domains but is represented as a single URL [uniform resource locator] on the World Wide Web. More complex examples of the logical layer are the Department of Defense's (DOD's) Non-classified Internet Protocol Router Network (NIPRNET) and SECRET Internet Protocol Router Network (SIPRNET), global, multi-segment networks that can be thought of as a single network only in the logical sense. For targeting purposes, planners may know the logical location of some targets, such as virtual machines and operating systems, that allow multiple servers or other network functions with separate Internet protocol (IP) addresses to reside on one physical computer, without knowing their geographic location. Logical layer targets can only be engaged with a **cyberspace capability:** a device or computer program including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

(3) The **cyber-persona layer** is a view of cyberspace created by abstracting data from the logical network layer using the rules that apply in the logical network layer to develop descriptions of digital representations of an actor or entity identity in cyberspace (cyber-persona). The cyber-persona layer consists of network or IT user accounts, whether human or automated, and their relationships to one another. Cyber-personas may relate directly to an actual person or entity, incorporating some personal or organizational data (e.g., e-mail and IP addresses, Web pages, phone numbers, Web forum log-ins, or financial account passwords). One individual may create and maintain multiple cyber-personas through use of multiple identifiers in cyberspace, such as separate work and personal e-mail addresses, and different identities on different Web forums, chat rooms, and social networking sites, which may vary in the degree to which they are factually accurate. Conversely, a single cyber-persona can have multiple users, such as multiple hackers using the same malicious software (malware) control alias, multiple extremists using a single bank account, or all members of the same organization using the same e-mail address. The use of cyber-personas can make attributing responsibility for actions in cyberspace difficult. Because cyber-personas can be complex, with elements in many virtual locations not linked to a single physical location or form, their identification requires significant intelligence collection and analysis to provide enough insight and situational awareness to enable effective targeting or to create the joint force commander's (JFC's) desired effect. Like the logical network layer, complex changes to cyber-personae can happen very quickly compared to similar changes in the physical network layer, complicating actions against these targets without detailed change tracking.

c. **Viewing Cyberspace Based on Location and Ownership.** Maneuver in cyberspace is complex and generally not observable. Therefore, staffs that plan, execute, and assess CO benefit from language that describes cyberspace based on location or ownership in a way that aids rapid understanding of planned operations. The term "blue cyberspace" denotes areas in cyberspace protected by the US, its mission partners, and other areas DOD may be ordered to protect. Although DOD has standing orders to protect only the Department of Defense information network (DODIN), cyberspace forces prepare,

on order, and when requested by other authorities, to defend or secure other United States Government (USG) or other cyberspace, as well as cyberspace related to critical infrastructure and key resources (CI/KR) of the US and PNs. The term "red cyberspace" refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, "controlled" means more than simply "having a presence on," since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others. All cyberspace that does not meet the description of either "blue" or "red" is referred to as "gray" cyberspace.

d. **DOD Cyberspace.** The DODIN is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. The DODIN comprises all of DOD cyberspace, including the classified and unclassified global networks (e.g., NIPRNET, SIPRNET, Joint Worldwide Intelligence Communications System) and many other components, including DOD-owned smartphones, radio frequency identification tags, industrial control systems, isolated laboratory networks, and platform information technology (PIT). PIT is the hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems, including weapon systems. Nearly every military and civilian employee of DOD uses the DODIN to accomplish some portion of their mission or duties.

e. **Connectivity and Access.** Cyberspace consists of myriad different and often overlapping elements to include networks, nodes, links, interrelated applications, user data, and system data. Even though cyberspace continues to become increasingly interconnected, some elements are intentionally isolated or subdivided into enclaves using access controls, encryption, unique protocols, or physical separation. With the exception of actual physical isolation, none of these approaches eliminate the underlying physical connectivity; instead, they limit access to the logical network. Access, whether authorized or unauthorized, can be gained through a variety of means. Although CO require timely and effective connectivity and access, the USG may not own, control, or have access to the infrastructure needed to support US military operations. For CO, access means a sufficient level of exposure to, connectivity to, or entry into a device, system, or network to enable further operations. While some accesses can be created remotely with or without permission of the network owner, access to closed networks and other systems that are virtually isolated may require physical proximity or more complex, time-consuming processes. In addition, gaining access to operationally useful areas of cyberspace, including targets within them, is affected by legal, policy, or operational limitations. For all of these reasons, access is not guaranteed. Additionally, achieving a commander's objectives can be significantly complicated by specific elements of cyberspace being used by enemies, adversaries, allies, neutral parties, and other USG departments and agencies, all at the same time. Therefore, synchronization and deconfliction of CO access is critical to successful operations of all types.

f. **The OE.** The OE is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and impact the decisions of the commander assigned responsibility for it. The information environment permeates the physical domains and therefore exists in any OE. The continuing advancement of IT has significantly reduced its cost of acquisition and cost of use, leading to the rapid proliferation of cyberspace capabilities, considerably complicating an already challenging OE. For instance, CO from moving platforms requires transmission through the EMS, which can be significantly affected by congestion (i.e., interference from commercial and military use), atmospheric conditions, and enemy electronic attack (EA). The decision to use CO to create effects may be affected by the political climate or even a single individual's use of cyberspace. Understanding the relationship of cyberspace to the physical domains and the information environment is essential for planning military operations in cyberspace.

(1) The pervasiveness of mobile IT is forcing governments and militaries to re-evaluate the impact of the information environment on operations. The nature of global social interaction has been changed by the rapid flow of information from around-the-clock news, including from nontraditional and unverifiable sources such as social networking, media sharing and broadcast sites, online gaming networks, topical forums, and text messaging. The popularity of these information sources enables unprecedented interaction among global populations, much of which is increasingly relevant to military operations. The ability of social networks in cyberspace to incite popular support (whether factually based or not) and to spread ideology is not geographically limited, and the continued proliferation of IT has profound implications for the joint force and US national security.

(2) State and non-state threats use a wide range of advanced technologies, which represent an inexpensive way for a small and/or materially disadvantaged adversary to pose a significant threat to the US. The application of low-cost cyberspace capabilities can provide an advantage against a technology-dependent nation or organization. This can provide an asymmetric advantage to those who could not otherwise effectively oppose US military forces. Additionally, organized crime or other non-state, extralegal organizations often make sophisticated malware available for purchase or free, allowing even non-sophisticated threats to acquire advanced capabilities at little to no cost. Because of the low barriers to entry and the potentially high payoff, the US can expect an increasing number of adversaries to use cyberspace threats to attempt to negate US advantages in military capability.

(3) **Key terrain in cyberspace** is analogous to key terrain in the physical domains in that holding it affords any combatant a position of marked advantage. In cyberspace, it may only be necessary to maintain a secure presence on a particular location or in a particular process as opposed to seizing and retaining it to the exclusion of all others. Note that it is possible for the US and an adversary to occupy the same terrain or use the same process in cyberspace, potentially without knowing of the other's presence. An additional characteristic of terrain in cyberspace is that these localities have a virtual component, identified in the logical network layer or even the cyber-persona layer. Key terrain identification is an essential component of planning. The military aspects of terrain (obstacles, avenues of approach, cover and concealment, observation and fields of fire, and

key terrain) provide a way to visualize and describe a network map. Obstacles in cyberspace may include firewalls and port blocks. Avenues of approach can be analyzed by identifying nodes and links, which connect endpoints to specific sites. Cover and concealment may refer to hidden IP addresses or password protected access. Cyberspace observation and fields of fire refer to areas where network traffic can be monitored, intercepted, or recorded. Examples of potential key terrain in cyberspace include access points to major lines of communications (LOCs), key waypoints for observing incoming threats, launch points for cyberspace attacks, and mission-relevant cyberspace terrain related to critical assets connected to the DODIN. Operators, planners, and intelligence staff work together to match plans' objectives with terrain analysis to determine key terrain in blue, gray, and red cyberspace for each plan. Correlating plan or mission objectives with key terrain ensures mission dependencies in cyberspace are identified and prioritized for protection in a standard manner across DOD. In many cases, the systems, networks, and infrastructure that support a mission objective will be interdependent. These complex interdependencies may require in-depth analysis to develop customized risk mitigation methodologies.

g. **The Information Environment.** The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. Since all CO require the creation, processing, storage, and/or transmission of information, cyberspace is wholly contained within the information environment. The information environment is broken down into the physical, informational, and cognitive dimensions and includes many types of information not in cyberspace. Although the types of information excluded from cyberspace continue to dwindle, there remain individuals and organizations that handle their information requirements outside of cyberspace, particularly when security, durability, cost, and scope factors are significant.

h. **The Relationship of CO to Operations in the Information Environment**

(1) Cyberspace is wholly contained within the information environment. CO and other information activities and capabilities create effects in the information environment in support of joint operations. Their relationship is both an interdependency and a hierarchy; cyberspace is a medium through which other information activities and capabilities may operate. These activities and capabilities include, but are not limited to, understanding information, leveraging information to affect friendly action, supporting human and automated decision making, and leveraging information (e.g., military information support operations [MISO] or military deception [MILDEC]) to change enemy behavior. CO can be conducted independently or synchronized, integrated, and deconflicted with other activities and operations.

(2) While commanders may conduct CO specifically to support information-specific operations, some CO support other types of military objectives and are integrated through appropriate cells and working groups. The lack of synchronized CO with other military operations planning and execution can result in friendly force interference and may counter the simplicity, agility, and economy of force principles of joint operations.

Refer to Joint Publication (JP) 3-0, Joint Operations, *for information on the primary activities that support the information joint function.*

3. Integrating Cyberspace Operations with Other Operations

a. During joint planning, cyberspace capabilities are integrated into the JFC's plans and synchronized with other operations across the range of military operations. While not the norm, some military objectives can be achieved by CO alone. Commanders conduct CO to obtain or retain freedom of maneuver in cyberspace, accomplish JFC objectives, deny freedom of action to the threat, and enable other operational activities.

b. The importance of CO support to military operations grows in direct proportion to the joint force's increasing reliance on cyberspace. Issues that may need to be addressed to fully integrate CO into joint planning and execution include centralized CO planning for DODIN operations and defense and other global operations; the JFC's need to integrate and synchronize all operations and fires across the entire OE, including the cyberspace aspects of joint targeting; deconfliction requirements between government entities; PN relationships; and the wide variety of authorities and legal issues related to the use of cyberspace capabilities. This requires all members of the commander's staff who conduct planning, execution, and assessment of operations to understand the fundamental processes and procedures for CO, including the organization and functions of assigned or supporting cyberspace forces.

c. Effective integration of CO with operations in the physical domains requires the active participation of CO planners and operators in each phase of joint operations on every staff supported by cyberspace forces. The physical and logical boundaries within which joint forces execute CO, and the priorities and restrictions on its use, should also be identified by the JFC, in coordination with other USG departments and agencies and national leadership. In particular, creation of effects in foreign cyberspace may have the potential to impact other efforts of the USG. Where the potential for such impact exists, national policy requires DOD coordination with interagency partners.

Refer to Chapter IV, "Planning, Coordination, Execution, and Assessment," for more information about planning, synchronization, integration, and interorganizational coordination of CO.

4. Cyberspace Operations Forces

a. Commander, United States Cyber Command (CDRUSCYBERCOM), commands a preponderance of the cyberspace forces that are not retained by the Services. USCYBERCOM accomplishes its missions within three primary lines of operation: secure, operate, and defend the DODIN; defend the nation from attack in cyberspace; and provide cyberspace support as required to combatant commanders (CCDRs). The Services man, train, and equip cyberspace units and provide them to USCYBERCOM through the SCCs. Per the *Memorandum of Agreement Between The Department of Defense and The Department of Homeland Security Regarding Department of Defense and US Coast Guard Cooperation on Cyberspace Security and Cyberspace Operations,*

the Commandant of the Coast Guard retains operational control (OPCON) of US Coast Guard Cyberspace forces when employed in support of DOD. USCYBERCOM uses a mission alignment process to make requirements-driven, risk-informed, Cyber Mission Force (CMF)-alignment recommendations and task assignments to assigned or attached cyberspace units to perform CO utilizing cyberspace capabilities to achieve objectives.

b. **CMF.** The Secretary of Defense (SecDef) and Chairman of the Joint Chiefs of Staff (CJCS) established the CMF to organize and resource the force structure required to conduct key cyberspace missions. CDRUSCYBERCOM exercises combatant command (command authority) (COCOM) of the CMF, which is a subset of the DOD's total force for CO. Various Service tactical cyberspace units, assigned to CDRUSCYBERCOM, comprise the three elements of the CMF:

(1) **Cyber Protection Force (CPF).** The CPF conducts CO for internal protection of the DODIN or other blue cyberspace when ordered. The CPF consists of cyberspace protection teams (CPTs) organized, trained, and equipped to defend assigned cyberspace in coordination with and in support of segment owners, cybersecurity service providers (CSSPs), and users.

(2) **Cyber National Mission Force (CNMF).** The CNMF conducts CO to defeat significant cyberspace threats to the DODIN and, when ordered, to the nation. The CNMF comprises various numbered national mission teams (NMTs), associated national support teams (NSTs), and national-level CPTs for protection of non-DODIN blue cyberspace.

(3) **Cyber Combat Mission Force (CCMF).** The CCMF conducts CO to support the missions, plans, and priorities of the geographic and functional CCDRs. The CCMF comprises various numbered combat mission teams (CMTs) and associated combat support teams (CSTs).

Refer to Chapter II, "Cyberspace Operations Core Activities," for more information about the operations of CMF units.

c. **USCYBERCOM Subordinate Command Elements.** Subordinate headquarters (HQ) of USCYBERCOM execute C2 of the CMF and other cyberspace forces. These include the Cyber National Mission Force-Headquarters (CNMF-HQ), the Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN), the joint force headquarters-cyberspace (JFHQ-C), and the SCC HQs. Each of the SCC commanders is dual-hatted by CDRUSCYBERCOM as a commander of one of the four JFHQs-C to enable synchronization of CO C2. In addition, there are other centers and staff elements that further enable unity of command for CO. Figure I-2 describes the organizational and subordination relationships of these command elements and the units of the CMF.

Refer to Chapter IV, "Planning, Coordination, Execution, and Assessment," for more information about C2 of CO.

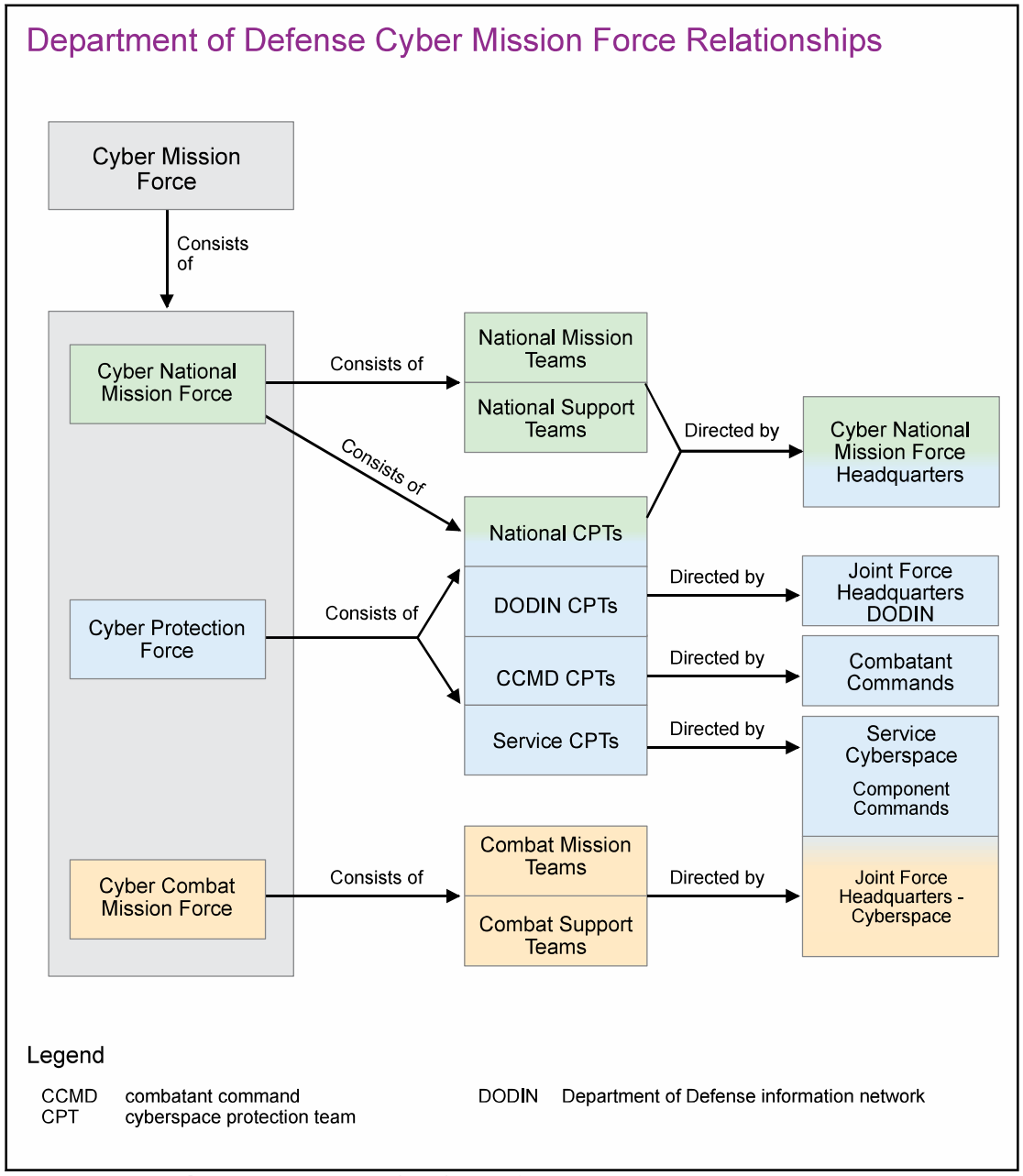


Figure I-2. Department of Defense Cyber Mission Force Relationships

d. **Other Cyberspace Forces and Staff.** Most cyberspace forces that protect the DODIN are Service-retained and some are employed in support of a specific CCDR. They may be used by the Service or SCCs to operationalize networks (i.e., design, build, configure and otherwise prepare to place into operation) and then secure, operate, and defend their Service enterprise portions of the DODIN. The Services may retain, or other CCDRs may organize, other scarce cyberspace forces that support CCMD missions as required, including CSSPs. Some of these Service-retained cyberspace forces that operate CCMD networks and systems are assigned directly to various CCDR staffs. In addition, the Defense Information Systems Agency (DISA) and various DOD agencies

and activities employ civilian staff and contractors to do these same operationalizing and DODIN operations functions.

5. Challenges to the Joint Force's Use of Cyberspace

The JFC faces a unique set of persistent challenges executing CO in a complex global security environment.

a. **Threats.** Cyberspace presents the JFC's operations with many threats, from nation-states to individual actors to accidents and natural hazards.

(1) **Nation-State Threat.** This threat is potentially the most dangerous because of nation-state access to resources, personnel, and time that may not be available to other actors. Some nations may employ cyberspace capabilities to attack or conduct espionage against the US. Nation-state threats involve traditional adversaries; enemies; and potentially, in the case of espionage, even traditional allies. Nation-states may conduct operations directly or may outsource them to third parties, including front companies, patriotic hackers, or other surrogates, to achieve their objectives.

(2) **Non-State Threats.** Non-state threats are formal and informal organizations not bound by national borders, including legitimate nongovernmental organizations (NGOs), and illegitimate organizations such as criminal organizations, violent extremist organizations, or other enemies and adversaries. Non-state threats use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, undermine confidence in governments, conduct espionage, and conduct direct terrorist actions within cyberspace. Criminal organizations may be national or transnational in nature and steal information for their own use, including selling it to raise capital and target financial institutions for fraud and theft of funds. They may also be used as surrogates by nation-states or non-state threats to conduct attacks or espionage through cyberspace.

(3) **Individuals or Small Group Threat.** Even individuals or small groups of people can attack or exploit US cyberspace, enabled by affordable and readily available techniques and malware. Their intentions are as varied as the number of groups and individuals. These threats exploit vulnerabilities to gain access to discover additional vulnerabilities or sensitive data or maneuver to achieve other objectives. Ethical hackers may share the vulnerability information with the network owners, but, more frequently, these accesses are used for malicious intent. Some threats are politically motivated and use cyberspace to spread their message. The activities of these small-scale threats can be co-opted by more sophisticated threats, such as criminal organizations or nation-states, often without their knowledge, to execute operations against targets while concealing the identity of the threat/sponsor and also creating plausible deniability.

(4) **Accidents and Natural Hazards.** The physical infrastructure of cyberspace is routinely disrupted by operator errors, industrial accidents, and natural disasters. These unpredictable events can have greater impact on joint operations than the actions of enemies. Recovery from accidents and hazardous incidents can be

complicated by the requirement for significant coordination external to DOD and/or the temporary reliance on back-up systems with which operators may not be proficient.

b. **Anonymity and Difficulties with Attribution.** To initiate an appropriate defensive response, attribution of threats in cyberspace is crucial for any actions external to the defended cyberspace beyond that authorized as authorized self-defense. The most challenging aspect of attributing actions in cyberspace is connecting a particular cyber-persona or action to a named individual, group, or nation-state, with sufficient confidence and verifiability to hold them accountable. This effort requires significant analysis and, often, collaboration with non-cyberspace agencies or organizations. The nature of cyberspace, government policies, and laws, both domestic and international, presents challenges to determining the exact origin of cyberspace threats. The ability to hide the sponsor and/or the threat behind a particular malicious effect in cyberspace makes it difficult to determine how, when, and where to respond. The design of the Internet lends itself to anonymity and, combined with applications intended to hide the identity of users, attribution will continue to be a challenge for the foreseeable future.

c. **Geography Challenges.** In cyberspace, there is no stateless maneuver space. Therefore, when US military forces maneuver in foreign cyberspace, mission and policy requirements may require they maneuver clandestinely without the knowledge of the state where the infrastructure is located. Because CO can often be executed remotely, through a virtual presence enabled by wired or wireless access, many CO do not require physical proximity to the target but use remote actions to create effects, which represents an increase in operational reach not available in the physical domains. This use of global reach applies equally to both external operations in red and gray cyberspace, as well as internal protection effects in blue cyberspace. The cumulative effects of some CO may extend beyond the initial target, a joint operations area (JOA), or outside of a single area of responsibility (AOR). Because of transregional considerations and the requirement for high-demand forces and capabilities, some CO are coordinated, integrated, and synchronized using centralized execution from a location remote from the supported commander.

d. **Technology Challenges.** Using a cyberspace capability that relies on exploitation of technical vulnerabilities in the target may reveal its functionality and compromise the capability's effectiveness for future missions. This has implications for both offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO) missions. Cyberspace capabilities without hardware components can be replicated for little or no cost. This means that once discovered, these capabilities will be widely available to adversaries, in some cases before security measures in the DODIN can be updated to account for the new threat. In addition, since similar technologies around the world share similar vulnerabilities, a single adversary may be able to exploit multiple targets at once using the same malware or exploitation tactic. Malware can be modified (or be designed to automatically modify itself), complicating efforts to detect and eradicate it.

e. **Private Industry and Public Infrastructure.** Many of DOD's critical functions and operations rely on contracted commercial assets, including Internet service providers

(ISPs) and global supply chains, over which DOD and its forces have no direct authority. This includes both data storage services and applications provided from a cloud computing architecture. Cloud computing enables DOD to consolidate infrastructure, leverage commodity IT functions, and eliminate functional redundancies while improving continuity of operations. But, the overall success of these initiatives depends upon well-executed risk mitigation and protection measures, defined and understood by both DOD components and industry. Dependency on commercial Internet providers means DOD coordination with the Department of Homeland Security (DHS), other interagency partners, and the private sector is essential to establish and maintain security of DOD's information. DOD supports DHS, which leads interagency efforts to identify and mitigate cyberspace vulnerabilities in the nation's critical infrastructure. DOD has the lead for improving security of the defense industrial base (DIB) sector, which includes major sector contractors and major contractor support to operations regardless of corporate country of domicile and continues to support the development of whole-of-government approaches for its risk management. The global technology supply chain affects mission-critical aspects of the DOD enterprise, and the resulting IT risks can only be effectively mitigated through public-private sector cooperation.

(1) **Globalization.** The combination of DOD's global operations with its reliance on cyberspace and associated technologies means DOD often procures mission-essential IT products and services from foreign vendors. A prime example is our reliance on network backbones and transmission equipment in other countries, such as undersea cables, fiber optic networks and telecommunications services, satellite and microwave antennas, and leased channels on foreign satellites. These systems may normally be reliable and trustworthy, but they can also leave US forces vulnerable to access denial by service interruption, communications interception and monitoring, or infiltration and data compromise. Another example is DOD's use of commercial, globally interconnected, globally sourced IT components in mission-critical systems and networks. Leveraging rapid technology development of the commercial marketplace remains a key DOD advantage. While globally sourced technology provides innumerable benefits to DOD, it also provides adversaries the opportunity to compromise the supply chain to access or alter data and hardware, corrupt products, and to intercept or deny communications and other mission-critical functions. Supply chain risks threaten all users and our collective security; therefore, DOD cannot ignore these risks to its missions. Globalization, including by US companies, introduces risks across the entire system lifecycle, to include design, manufacturing, production, distribution, operation and maintenance, and disposal of a system or component. Each of these lifecycle stages presents the opportunity to manipulate, deny, or collect information on such systems. It is not feasible to eliminate our reliance on foreign-owned services and products, but our reliance on them makes it essential every reasonable avenue for risk mitigation be pursued, to include user and commander education at all levels, encryption, C2 system redundancy, operations security (OPSEC), and careful inspection of vendor-provided equipment in accordance with (IAW) DOD IT procurement policy.

(2) **Mitigations.** DOD partners with the DIB to increase the security of information about DOD programs residing on or transiting DIB unclassified networks. The Department of Defense Cyber Crime Center (DC3) serves as DOD's operational

focal point for voluntary cyberspace information sharing and incident reporting program. In addition, DOD is strengthening its acquisition regulations to require consideration of applicable cybersecurity policies during procurement of all DODIN components to reduce risks to joint operations.

CHAPTER II
CYBERSPACE OPERATIONS CORE ACTIVITIES

"When I first started working cyberspace operations, these operations were often just concepts, and when conducted, performed ad-hoc by technical specialists on loan from other organizations. Today this is not the case. Now, a mature and highly capable cyber force is built and in the fight, aggressively defending our network, conducting daily operations against adversaries, and strengthening the combat power and lethality of U.S. forces around the world. This swift growth represents tremendous opportunity."

Lieutenant General Paul Nakasone
Prospective Commander, US Cyber Command
Testimony before Senate Committee on Armed Services
March 1, 2018

1. Introduction

a. CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. CO comprise the military, national intelligence, and ordinary business operations of DOD in and through cyberspace. Although commanders need awareness of the potential impact of the other types of DOD CO on their operations, the military component of CO is the only one guided by joint doctrine and is the focus of this publication. CCDRs and Services use CO to create effects in and through cyberspace in support of military objectives. Military operations in cyberspace are organized into missions executed through a combination of specific actions that contribute to achieving a commander's objective. Various DOD agencies and components conduct national intelligence, ordinary business, and other activities in cyberspace. Although discussed briefly here for context, these activities are guided by DOD policies concerning CO. While joint doctrine does apply to CSAs where it directly relates to their mission to support military forces, CSAs and other DOD agencies and activities also conduct various CO activities that are considered cyberspace-enabled activities.

b. **Cyberspace-Enabled Activities.** Most DOD cyberspace actions use cyberspace to enable other types of activities, which employ cyberspace capabilities to complete tasks but are not undertaken as part of one of the three CO missions: OCO, DCO, or DODIN operations. These uses include actions like operating a C2 or logistics system, sending an e-mail to support an information objective, using the Internet to complete an online training course, or developing a briefing. Other than being an authorized user of the network, DOD personnel need no special authorities to use cyberspace capabilities in this way. It is through these uses of cyberspace that the majority of DODIN vulnerabilities are exposed to, and exploited by, our adversaries. The challenge is to train all DODIN users to understand the significance of cyberspace threats and to recognize threat tactics so these uses of cyberspace do not create unnecessary risk to the mission. Protecting the DODIN by establishing a culture of vulnerability awareness, particularly through DOD and

interagency policies, practices, and training, is critical to the success of all types of cyberspace-enabled DOD missions.

2. Military Operations In and Through Cyberspace

a. **Cyberspace Missions.** All actions in cyberspace that are not cyberspace-enabled activities are taken as part of one of three cyberspace missions: OCO, DCO, or DODIN operations. These three mission types comprehensively cover the activities of the cyberspace forces. The successful execution of CO requires integration and synchronization of these missions. Military cyberspace missions and their included actions are normally authorized by a military order (e.g., execute order [EXORD], operation order [OPORD], tasking order, verbal order), referred to hereafter as mission order, and by authority derived from DOD policy memorandum, directive, or instruction. Cyberspace missions are categorized as OCO, DCO, or DODIN operations based only on the intent or objective of the issuing authority, not based on the cyberspace actions executed, the type of military authority used, the forces assigned to the mission, or the cyberspace capabilities used. Some orders may cover multiple types of missions. For example, a standing order to protect the DODIN may include both DODIN operations and DCO mission components, and an order for an external mission could support both offensive and defensive objectives. Paragraph 2.b., "Cyberspace Actions," discusses the specific actions used in the execution of these missions. Effective execution of all cyberspace missions requires timely intelligence and threat indicators from traditional and cyberspace sensors, vulnerability information from DOD and non-DOD sources, and accurate assessment of previous missions. IAW current USG policy, DOD deconflicts missions in foreign cyberspace with the other USG department and agency mission partners who share this responsibility. Figure II-1 graphically depicts the primary relationships between the cyberspace missions and actions. The depiction in Figure II-1 of the types of forces that normally conduct each type of CO mission is not intended to limit a JFC's ability to employ the best-qualified unit on any particular mission.

(1) **DODIN Operations.** The DODIN operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN. These include proactive cyberspace security actions which address vulnerabilities of the DODIN or specific segments of the DODIN. It also includes the set-up of tactical networks by deployed forces to extend existing networks, maintenance actions and other non-security actions necessary for the sustainment of the DODIN, and the operation of red teams and other forms of security evaluation and testing. DODIN operations are network-focused and threat-agnostic: the cyberspace forces and workforce undertaking this mission endeavor to prevent all threats from negatively impacting a particular network or system they are assigned to protect. They are threat-informed and use all available intelligence about specific threats to improve the security posture of the network. DODIN operations does not include actions taken under statutory authority of a chief information officer (CIO) to provision cyberspace for operations, including IT architecture development; establishing standards; or designing, building, or otherwise operationalizing DODIN IT for use by a commander. DODIN operations is a standing mission, and although many DODIN operations activities are regularly scheduled events, they cannot be considered routine,

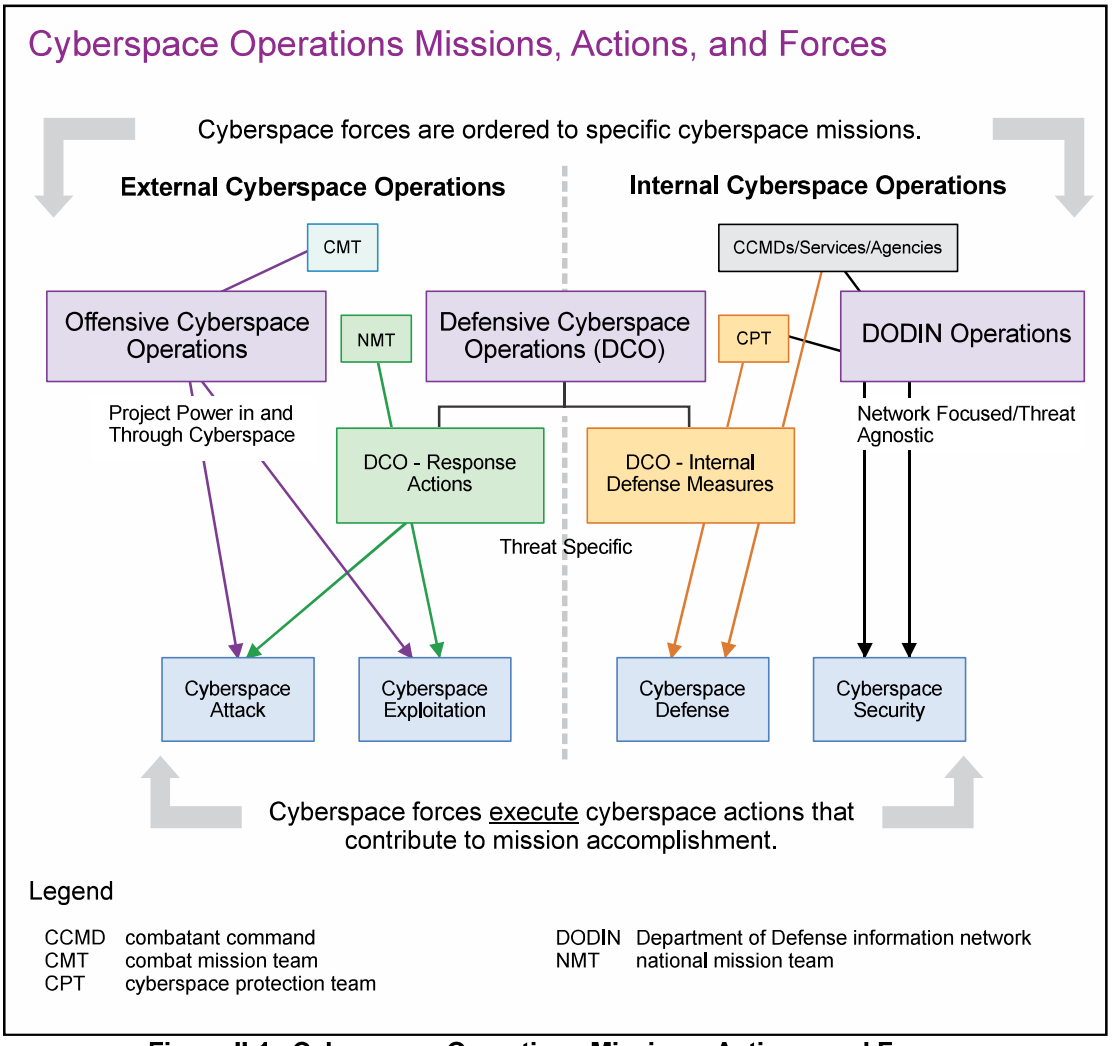


Figure II-1. Cyberspace Operations Missions, Actions, and Forces

since their aggregate effect establishes the framework on which most DOD missions ultimately depend.

See JP 6-0, Joint Communications System, *for a more detailed discussion of DODIN operations and the management of networked communication systems.*

(2) **DCO.** DCO missions are executed to defend the DODIN, or other cyberspace DOD cyberspace forces have been ordered to defend, from active threats in cyberspace. Specifically, they are missions intended to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. This distinguishes DCO missions, which defeat specific threats that have bypassed, breached, or are threatening to breach security measures, from DODIN operations, which endeavor to secure DOD cyberspace from all threats in advance of any specific threat activity. DCO are threat-specific and frequently support mission assurance objectives. DCO missions are conducted in response to specific threats of attack, exploitation, or other effects of malicious cyberspace activity and leverage information from maneuver, intelligence

collection, counterintelligence (CI), law enforcement (LE), and other sources as required. DCO include outmaneuvering or interdicting adversaries taking or about to take actions against defended cyberspace elements, or otherwise responding to imminent internal and external cyberspace threats. The goal of DCO is to defeat the threat of a specific adversary and/or to return a compromised network to a secure and functional state. The components of DCO are:

(a) **Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM).** DCO-IDM are the form of DCO mission where authorized defense actions occur within the defended network or portion of cyberspace. DCO-IDM of the DODIN is authorized by standing order and includes cyberspace defense actions to dynamically reconfirm or reestablish the security of degraded, compromised, or otherwise threatened DOD cyberspace to ensure sufficient access to enable military missions. For compromised DODIN elements, specific tactics include rerouting, reconstituting, restoring, or isolation. Most DCO missions are DCO-IDM, which include pro-active and aggressive internal threat hunting for advanced and/or persistent threats, as well as the active internal countermeasures and responses used to eliminate these threats and mitigate their effects. For example, CPT operations conducted on key terrain in cyberspace for mission-critical assets in response to indications of malicious cyberspace activity are DCO-IDM missions, even before indicators of compromise exist.

(b) **Defensive Cyberspace Operations-Response Actions (DCO-RA).** DCO-RA are the form of DCO mission where actions are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. DCO-RA actions are normally in foreign cyberspace. Some DCO-RA missions may include actions that rise to the level of use of force, with physical damage or destruction of enemy systems, depending on broader operational context, such as the existence or imminence of open hostilities, the degree of certainty in attribution of the threat, the damage the threat has caused or is expected to cause, and national policy considerations. DCO-RA missions require a properly coordinated military order and careful consideration of scope, rules of engagement (ROE), and measurable objectives.

(c) **Defense of Non-DOD Cyberspace.** While DCO generally focus on the DODIN, which includes all of DOD cyberspace, military cyberspace forces prepare to defend any US or other blue cyberspace when ordered. DOD operations rely on many non-DOD segments of cyberspace, including private sector and mission partner networks. Security of this cyberspace is the responsibility of the resource owners, which include other USG departments and agencies, private sector entities, and other partners. Since DOD-associated cyberspace are known targets for malicious cyberspace activity, protection of these non-DOD networks and systems can be a vital component of mission assurance. However, DOD cannot guarantee the robustness of the security standards applied to such networks. The commander's mission risk analysis should account for this uncertainty in the security of non-DOD cyberspace. It is essential planners and those supporting CO coordinate, through JFHQ-DODIN as required, with operators of these networks to better understand the risks they impart to joint operations. When required under a specific authorizing order, and in full coordination with DHS and other USG departments and agencies, DOD cyberspace forces undertake DCO-RA and DCO-IDM missions to defend

these and other non-DOD cyberspace segments, like national CI/KR or partner networks. Prioritization schemes for defense of CI/KR should be established in advance. If DCO-IDM missions are ordered as part of a defense support of civil authorities (DSCA) operation, Active Component forces may be supported by National Guard (NG) forces activated under Title 32,United States Code (USC), if authorized by SecDef, or Title 10, USC; US Coast Guard Forces under Title 14, USC; and/or other cyberspace forces from one of the Reserve Component (RC) units.

(3) **OCO.** OCO are CO missions intended to project power in and through foreign cyberspace through actions taken in support of CCDR or national objectives. OCO may exclusively target adversary cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, high-value targets, etc. All CO missions conducted outside of blue cyberspace with a commander's intent other than to defend blue cyberspace from an ongoing or imminent cyberspace threat are OCO missions. Like DCO-RA missions, some OCO missions may include actions that rise to the level of use of force, with physical damage or destruction of enemy systems. Specific effects created depend on the broader operational context, such as the existence or imminence of open hostilities and national policy considerations. OCO missions require a properly coordinated military order and careful consideration of scope, ROE, and measurable objectives.

b. **Cyberspace Actions.** Execution of any OCO, DCO, or DODIN operations mission requires completion of specific tactical-level actions or tasks that employ cyberspace capabilities to create effects in cyberspace. All cyberspace mission objectives are achieved by the combination of one or more of these actions, which are defined exclusively by the types of effects they create. To plan for, authorize, and assess these actions, it is important the commander and staff clearly understand which actions have been authorized under their current mission order. For example, the transition from DODIN operations to DCO-IDM missions may need to occur quickly whenever the DODIN is threatened and cyberspace operators begin to take cyberspace defense actions. To enable and synchronize this transition and subsequent cyberspace defense actions, clear orders are required that communicate to cyberspace operators the applicable constraints, restraints, and authorities. Since they will always be necessary, standing orders for DODIN operations and DCO-IDM missions cover most cyberspace security and initial cyberspace defense actions. However, OCO and DCO-RA missions are episodic. They may require clandestine maneuver and collection actions or may require overt actions, including fires. Therefore, the approval for CO actions in foreign cyberspace requires separate OCO or DCO-RA mission authorities. The cyberspace actions are:

(1) **Cyberspace Security.** Cyberspace security actions are taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other IT, including PIT, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Although they are threat-informed, cyberspace security actions occur in advance of a specific security compromise and are a primary component action of the DODIN operations mission. Cyberspace security actions protect

Note: Joint doctrine uses the term "cyberspace security" to distinguish this tactical-level cyberspace action from the policy and programmatic term "cybersecurity" used in Department of Defense (DOD) and United States Government (USG) policy. To enable effective planning, execution, and assessment, doctrine distinguishes between cyberspace security and cyberspace defense actions, a distinction not made in DOD and USG cybersecurity policy, where the term cybersecurity includes the ideas of both security and defense. Doctrine uses both "cyberspace security" and "cybersecurity," depending upon the context.

from threats within cyberspace by reducing or eliminating vulnerabilities that may be exploited by an adversary and/or implementing measures to detect malicious cyberspace activities. Examples of cyberspace security actions include increasing password strength, installing a software patch to remove vulnerabilities, encrypting stored data, training users on cyberspace security best practices, restricting access to suspicious Web sites, or blocking traffic on unused router ports.

(2) **Cyberspace Defense.** Cyberspace defense actions are taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach the cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. The CCMD, Service, or DOD agency that owns or operates the network is generally authorized to take these defensive actions except in cases when they would compromise the operations of elements of cyberspace outside the responsibility of the respective CCMD, Service, or agency. In some cases, a CPT will be assigned to assist with re-securing and mitigation actions. JFHQ-DODIN coordinates all defensive actions that impact more than one CCMD or have impacts outside the realm of the network owner. Cyberspace defense actions are the component actions of a DCO-IDM mission. Since the same personnel often perform both cyberspace security and cyberspace defense actions, these actions are collectively referred to as protection.

(3) **Cyberspace Exploitation.** Cyberspace exploitation actions include military intelligence activities, maneuver, information collection, and other enabling actions required to prepare for future military operations. Cyberspace exploitation actions are taken as part of an OCO or DCO-RA mission and include all actions in gray or red cyberspace that do not create cyberspace attack effects. Cyberspace exploitation includes activities to gain intelligence and support operational preparation of the environment for current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value; maneuvering to positions of advantage; and positioning cyberspace capabilities to facilitate follow-on actions. Cyberspace exploitation also supports current and future operations through collection of information, including mapping red and gray cyberspace to support situational awareness; discovering vulnerabilities; enabling target development; and supporting the planning, execution, and assessment of military operations. Cyberspace exploitation actions are deconflicted with other USG departments and agencies IAW national policy.

(4) **Cyberspace Attack.** Cyberspace attack actions create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains. Unlike cyberspace exploitation actions, which are often intended to remain clandestine to be effective, cyberspace attack actions will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality. Cyberspace attack actions are a form of fires, are taken as part of an OCO or DCO-RA mission, are coordinated with other USG departments and agencies, and are carefully synchronized with planned fires in the physical domains. They include actions to:

(a) **Deny.** To prevent access to, operation of, or availability of a target function by a specified level for a specified time, by:

1. **Degrade.** To deny access to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation is specified. If a specific time is required, it can be specified.

2. **Disrupt.** To completely but temporarily deny access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level is 100 percent.

3. **Destroy.** To completely and irreparably deny access to, or operation of, a target. Destruction maximizes the time and amount of denial. However, destruction is scoped according to the span of a conflict, since many targets, given enough time and resources, can be reconstituted.

(b) **Manipulate.** Manipulation, as a form of cyberspace attack, controls or changes information, information systems, and/or networks in gray or red cyberspace to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques. It uses an adversary's information resources for friendly purposes, to create denial effects not immediately apparent in cyberspace. The targeted network may appear to operate normally until secondary or tertiary effects, including physical effects, reveal evidence of the logical first-order effect.

c. **Countermeasures in Cyberspace.** Countermeasures are that form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. In cyberspace, the term applies to any CO actions that fit the description of the term, regardless of where the countermeasure is taken. As in the physical domains, countermeasure actions can be taken either internal or external to the defended terrain and can be used preemptively or reactively. Internal countermeasures are cyberspace defense actions taken as part of a DCO-IDM mission; for example, closing router ports being used by an adversary for unauthorized access or blocking malware that is beaconing out of the DODIN. External countermeasures, which would be part of a DCO-RA or OCO mission, are employed beyond the DODIN boundary against a specific malicious cyberspace activity. In support of an OCO mission, they may be cyberspace attack actions that spoof or otherwise negate

the effectiveness of adversary sensors or defenses. As part of a DCO-RA mission, they may be used to identify the source of a threat and/or use non-intrusive or minimally intrusive techniques to interdict or mitigate threats. External defensive countermeasures are normally nondestructive/nonlethal in nature, typically impact only malicious activity but not the associated threat systems and terminate when the threat stops. All external countermeasures are subject to the same synchronization, deconfliction, legal, and policy guidance as any other aspect of an OCO or DCO-RA mission.

d. **Assignment of Cyberspace Forces to CO.** Mission orders or other directives assign cyberspace forces described in Chapter I, "Overview of Cyberspace and Cyberspace Operations," to specific cyberspace missions, as depicted in Figure II-1.

(1) **Forces and Workforce Conducting DODIN Operations and DCO-IDM.** Service-retained cyberspace forces, CCMD cyberspace forces, RC forces, and DOD agency and activity staffs execute much of the DODIN operations required to secure and operate the various backbones, sub-nets, segments, enclaves, and private networks of the DODIN under the planning, direction, integration, and synchronization of the JFHQ-DODIN. These staffs include CSSPs established by the Services and DOD agencies to provide DODIN protection services under support agreements with system owners. Although they are not military forces, contracted personnel protect some segments of the DODIN. Note also that other, non-cyberspace forces conduct DODIN operations as an integral part of assigned duties. For example, operators of PIT have an implied responsibility to protect their equipment from threats in cyberspace and require specialized training to detect and defeat cyberspace threats. Protecting PIT from malicious cyberspace activity is complicated by the design of these systems, which are often developed with little consideration of cyberspace threats. Regardless of which personnel and DODIN segments are involved, when personnel with DODIN security responsibilities detect compromise of cyberspace security measures, they transition, IAW standing authorities delegated by the commander, to the cyberspace defense actions of DCO-IDM to restore security to their assigned portion of the DODIN. Their effectiveness in making this transition depends upon their level of training and resources to detect and respond to threats. If discovery and mitigation of malicious cyberspace activity requires expertise beyond that available to the network operator and/or the ISP, CPTs may respond to provide support conducting cyberspace defense actions, either remotely or by deploying to the affected location. CPTs perform other tasks to support network operators, including penetration testing, security surveys, and assessment. National-level CPT support can be extended to defend non-DOD mission partner or critical infrastructure networks when ordered by SecDef.

(2) **Forces Conducting DCO-RA and OCO.** DCO-RA missions are normally assigned to NMTs, which are tactical units of the CNMF that defend the DODIN, or other blue cyberspace when ordered. The NMTs are aligned under the CNMF-HQ against specific cyberspace threats. OCO missions are normally assigned to CMTs, tactical units of the CCMF that support CCDR plans and priorities to project power in support of national objectives. The CMTs are aligned, under the JFHQs-C, in support of CCMDs. In addition to NMTs and CMTs, there are NSTs and CSTs not depicted in Figure II-1 that provide specialized technical and analytic support for the units of the CMF. This

support includes intelligence analysis, cyberspace capability development, linguist support, and planning.

Refer to Chapter IV, "Planning, Coordination, Execution, and Assessment," for more information about C2 of these cyberspace forces.

e. **Referring to Adversary Activities in Cyberspace.** DOD CO planning terms may not accurately describe the actions of our adversaries and enemies in cyberspace because their mission objectives and commander's intent may not be known with certainty. Therefore, the term "malicious cyberspace activity" refers to all such activities. If the context of the discussion requires more specific descriptions of this activity, use generic terms (e.g., attack, exploitation, sabotage, maneuver), depending upon the specific effects of the malicious actions.

3. National Intelligence Operations In and Through Cyberspace

National-level intelligence organizations conduct intelligence activities in, through, and about cyberspace in response to national intelligence priorities. This intelligence can support a military commander's planning and preparation. Although DOD's cyberspace forces may collect tactically and operationally useful information while maneuvering to and through foreign cyberspace, like all joint forces, they also depend on intelligence support from traditional military and national intelligence sources.

See JP 2-0, Joint Intelligence, *and JP 2-01,* Joint and National Intelligence Support to Military Operations, *for a more complete discussion of national intelligence activities, including intelligence federation.*

4. Department of Defense Ordinary Business Operations In and Through Cyberspace

Ordinary business operations in and through cyberspace are "cyberspace-enabled activities" that comprise those non-intelligence and non-warfighting capabilities, functions, and actions used to support and sustain DOD forces and components. This includes the cyberspace-enabled functions of the civilian-run DOD agencies and activities, such as the Defense Finance and Accounting Service and the Defense Contract Audit Agency. Since the conduct of DOD ordinary business operations in cyberspace is guided by DOD policy and not generally by joint doctrine, it is not discussed here in detail. However, vulnerabilities that may exist in the applications and devices used for DOD ordinary business operations might be exploited in a manner that directly impacts a military commander's mission. Since DOD agencies and activities use many of the same networks as military commanders, a compromise in any area of the DODIN used for business operations might result in a loss of mission assurance in cyberspace for military operations.

5. The Joint Functions and Cyberspace Operations

a. JP 3-0, *Joint Operations,* delineates joint functions common to joint operations at all levels of warfare. These joint functions comprise related capabilities and activities

grouped together to help commanders integrate, synchronize, and direct joint operations. This section presents an overview of how military operations leverage cyberspace capabilities to enable these functions in support of all DOD missions and how the functions themselves are accomplished in cyberspace during CO.

b. **C2.** Discussion of C2 and cyberspace requires a distinction between using cyberspace systems that implement the C2 of military operations and the C2 of forces that execute CO. The former, addressed here, is a cyberspace-enabled activity, and the latter is addressed in Chapter IV, "Planning, Coordination, Execution, and Assessment," paragraph 5, "Command and Control of Cyberspace Forces." C2 encompasses the exercise of authority and direction by commanders over assigned and attached forces in the accomplishment of their mission. Use of cyberspace as a means of exchanging communications is overwhelmingly the most common method at the strategic and operational levels of warfare and is increasingly important in tactical warfare. Digital communications methods have largely supplanted analog communications, except at the tactical level, where analog signaling methods remain. Analog communications will likely persist indefinitely in tactical operations for reasons of simplicity, reliability, and security. However, military C2 systems that function by the transmission of digital data are part of the DODIN. Cyberspace provides communications pathways, planning and decision-support aids, and cyberspace-related intelligence to enable timely decision making and execution of those decisions. This provides the commander the advantage of controlling the timing and tempo of operations. Cyberspace offers an exceptionally diverse array of circuits for issuance of commands and signals to forces and for those forces to relay operational information back up the chain of command. Military orders converted to digital form, including digital voice and video, can travel on circuits that transit all of the physical domains, significantly increasing the likelihood of timely delivery. However, a commander's confidence in the C2 system can be easily compromised when the security of the DODIN becomes suspect; therefore, the more the commander relies on cyberspace for C2, the more important protection of supporting cyberspace assets is to this joint function.

See JP 3-30, Command and Control of Joint Air Operations; *JP 3-31,* Command and Control for Joint Land Operations; *and JP 3-32,* Command and Control of Joint Maritime Operations, *for more information on how cyberspace is used to enable operations in the physical domains.*

c. **Intelligence.** Understanding the OE is fundamental to all joint operations, including CO. Intelligence may be derived from information gained during military operations in cyberspace or from other sources. Intelligence operations in cyberspace not conducted by a military commander are covered in paragraph 3, "National Intelligence Operations In and Through Cyberspace." All-source intelligence support to CO utilizes the same intelligence process used by all other military operations, with unique attributes necessary for support of CO planning detailed in Chapter IV, "Planning, Coordination, Execution, and Assessment," paragraph 3, "Intelligence and Operational Analytic Support to Cyberspace Operations Planning." The process includes:

(1) Planning and direction, to include identification of target vulnerabilities to enable continuous planning and direction of CI activities to protect against espionage, sabotage, and attacks against US citizens/facilities and continuously examining mission success criteria and associated metrics to assess the impact of CO and inform the commander's decisions.

(2) Collection sensors with access to information about cyberspace.

(3) Processing and exploitation of collected data, including identification of useful information from collected data, either real-time or after-the-fact.

(4) Analysis of information and production of intelligence products.

(5) Dissemination and integration of intelligence related to cyberspace with operations.

(6) Evaluation and feedback regarding intelligence effectiveness and quality.

See JP 2-0, Joint Intelligence, *for more information on the joint intelligence process.*

d. **Fires.** Cyberspace attack capabilities create fires in and through cyberspace and are often employed with little or no associated physical destruction. However, modification or destruction of computers that control physical processes can lead to cascading effects (including collateral effects) in the physical domains. Depending upon the commander's objective, fires in cyberspace can be offensive or defensive, supporting or supported. Like all forms of fires, fires in and through cyberspace should be included in the joint planning and execution processes to facilitate synchronization and unity of effort and must comply with the law of war and ROE. Fires in and through cyberspace encompass a number of tasks, actions, and processes, including targeting, coordination, and deconfliction. If multiple USG or allied entities have requirements to create effects or collect intelligence on the same target in cyberspace, synchronization and deconfliction across all USG entities will be required, otherwise their uncoordinated actions could expose or interfere with each other. Even if effects can be created independently and are sufficiently justified, a technical analysis is still required to determine if the capabilities can operate as planned in the same environment without interference or increasing the chances of unwanted detection.

See JP 3-60, Joint Targeting, *for more information on joint targeting, and Chapter IV, "Planning, Coordination, Execution, and Assessment," for more information on targeting during CO.*

e. **Movement and Maneuver**

(1) Movement and maneuver involves deploying forces and capabilities into an OA and positioning within that area to gain operational advantage in support of mission objectives, including accessing and, as necessary, controlling key terrain. Cyberspace operations enable force projection without the need to establish a physical presence in foreign territory. Maneuver in the DODIN or other blue cyberspace includes positioning

of forces, sensors, and defenses to best secure areas of cyberspace or engage in defensive actions as required. Maneuver in gray and red cyberspace is a cyberspace exploitation action and includes such activities as gaining access to adversary, enemy, or intermediary links and nodes and shaping this cyberspace to support future actions. The ability to access or even control such terrain can change the outcome of an engagement. A significant factor in maneuverability in cyberspace is gaining and maintaining logical access to the environment. This capability to maneuver and provide operational reach may be lost at any time if the configuration of the relevant cyberspace nodes are modified. The ubiquitous nature of cyberspace creates another major consideration, because it enables an adversary or enemy to establish key points of presence outside the physical OA, in third-party countries, protected areas, or even inside the US. Additionally, adversaries or enemies may conduct CO from physical network connections within the US, PNs, or third-party nations, thereby limiting the JFC's maneuver space based on law and policy restriction and creating dependencies on our ability to coordinate with interagency and other mission partners.

(2) Another component of maneuver in cyberspace is the ability to move data to a place or process where it has maximum military utility, including movement of data out of harm's way and into a secure location or process. Because of network latencies and performance differences between system messaging models, remote data stores are generally slower than local data stores. This could make the difference between success and failure in CO. In this context, having access to secure wired or wireless bandwidth is analogous to maintaining LOCs in the physical domains. The ability to divert the flow of data from one physical link to another in the face of threats, for example from terrestrial cables to satellite communications (SATCOM) links, is an example of freedom of maneuver in cyberspace. Therefore, managing the EMS within the battlespace is a key planning consideration for CO.

f. **Sustainment**

(1) Sustainment is the provision of logistics and personnel services to maintain operations through mission accomplishment and redeployment of the force. From the perspective of cyberspace-enabled activities in support of global logistics, DOD relies on protected DODIN and commercial network segments to coordinate sustainment of forces.

(2) Rapid advancements in IT require the development, fielding, and sustainment of cyberspace capabilities adaptable to the changing OE. For example, secure, wireless mobile devices provide anonymity for adversary Internet users; an adversary might update or change operating systems; or they may transition to using more secure virtual machines in their network architecture. Joint forces need the capability to adapt by rapidly incorporating new cyberspace capabilities into their arsenal. Additionally, the joint force may need the capability to quickly upgrade their own cyberspace to leverage these same new technologies. However, pressure to deploy new technology should be balanced against the potential for increased risk and the requirements of cybersecurity policy, and implementation should be carefully orchestrated to prevent divergence among Service-provisioned cyberspace that could create vulnerabilities in DODIN architecture.

(3) Sustainment planning should identify and address legacy systems. Many legacy mission-critical systems were not designed and configured to be easily updated. As a result, many of the vulnerabilities incurred on the DODIN are introduced via unpatched (and effectively un-patchable) systems. These vulnerabilities can be mitigated through additional layers of protection, which must then be sustained. Additionally, hardware capabilities, including sensors and other forward-deployed cyberspace capabilities, can deteriorate over time due to wear and tear or adversary discovery, requiring component repair or replacement to remain operable. This can be particularly problematic when physically inaccessible systems (such as those deployed to remote sites) require replacement or upgrade. It is vital that commanders understand the mission risk created by leaving such cyberspace capabilities in place over long periods, not just to current operations but to the success of future DOD missions that rely on such capabilities. Finally, contingency software capabilities that are infrequently accessed may also require periodic refreshing and retesting to verify they are still secure and capable of creating the required effects, despite changes in the OE.

g. **Protection**

(1) Protection of the DODIN and other critical US cyberspace includes the continuous and synchronized integration of cyberspace security and, when required, cyberspace defense actions. Protection of cyberspace assets is complicated by their logical connectivity that can enable enemies to create multiple, cascading effects that may not be restricted by physical geography and civil/military boundaries. Cyberspace capabilities requiring protection include not only the infrastructure (computers, cables, antennas, and switching and routing equipment) but also parts of the EMS (datalink frequencies to include satellite downlink, cellular, and wireless) and the content (both data and applications) on which military operations rely. Key to cyberspace protection is the positive control of all direct connections between the DODIN and the Internet and other public portions of cyberspace, as well as the ability to monitor, detect, and prevent the entrance of malicious network traffic and unauthorized exfiltration of information through these connections.

(2) Protection of blue cyberspace uses a combination of security and defensive cyberspace capabilities. Due to the speed of effects and the number of elements in cyberspace, automated procedures to defend cyberspace, verify configurations, and discover network vulnerabilities often provide a better chance of initial success against an aggressor than the manual equivalents. Several factors work against achieving perfect security of a collection of networks and systems as complex as the DODIN. Therefore, mission-critical parts of the DODIN which provide an advantage to either combatant are considered key terrain and given priority for protection. Even the strongest encryption and most secure protocols cannot protect the DODIN from poorly trained and/or unmotivated users who do not employ proper security practices. Therefore, the training of all DODIN users on appropriate behaviors and commander's strict enforcement of cyberspace security best practices is part of an overall risk management program. Commanders are accountable for the actions of their personnel in cyberspace and should ensure clear understanding at all levels of the command of cyberspace security standards, expectations, and best practices to protect cyberspace.

(3) Protection of cyberspace capabilities requires strict adherence to unique OPSEC countermeasures, since these operations might be thwarted if discovered in advance of their effects. Concealment of movement within cyberspace uses different techniques than concealment in the physical domains. Skills such as avoiding detection are fundamental to most external missions and, therefore, essential to many joint military CO.

For more information on OPSEC, refer to JP 3-13.3, Operations Security.

h. **Information**

(1) The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant actor perceptions, behavior, and/or action or inaction and support human and automated decision making. The information function helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. This function provides JFCs the ability to integrate the generation and preservation of friendly information while leveraging the inherent informational aspects of all military activities to achieve the commander's objectives and attain the end state. This joint force function supports actions that achieve objectives within the operational and information environments. Given the aim of CO is to achieve objectives within cyberspace and cyberspace is wholly contained within the information environment, it is important to understand its relationship with the information joint function.

(2) The joint force conducts CO in concert with other capabilities, to gain and maintain an advantage. Cyberspace is a medium through which specific information capabilities, such as MISO or MILDEC may be employed. Note that while some operations in the information environment may be done using only CO, they are still synchronized, integrated, and deconflicted with other activities and operations that impact the commander's objectives.

(3) It is important to understand, that although CO will enable certain primary activities within the information function, there are information activities that do not involve CO. Therefore, failure to synchronize CO with other military operations planning and execution can result in friendly forces conducting redundant or conflicting information activities, resulting in wasted time and resources and loss of operational advantage.

Refer to JP 1, Volume 1, Joint Warfighting, *for more information about the joint functions and their role in the military operations.*

Refer to JP 3-0, Joint Operations, *for information on the primary activities that support the information joint function.*

CHAPTER III
AUTHORITIES, ROLES, AND RESPONSIBILITIES

"The Defense Department (DOD) requires the commitment and coordination of multiple leaders and communities across DOD and the broader US [G]overnment to carry out its missions and execute this strategy. Defense Department law enforcement, intelligence, counterintelligence, and policy organizations all have an active role, as do the men and women that build and operate DOD's networks and information technology systems. Every organization needs to play its part."

Ashton B. Carter
Secretary of Defense
The Department of Defense Cyber Strategy, April 17, 2015

1. Introduction

a. Under the authorities of SecDef, DOD uses cyberspace capabilities to shape cyberspace and provide integrated offensive and defensive options for the defense of the nation. USCYBERCOM coordinates with CCMDs, the JS, and the Office of the Secretary of Defense (OSD); liaises with other USG departments and agencies; and, in conjunction with DHS, DOD's DC3, and the Defense Security Service, liaises with members of the DIB. Similarly, as directed, DOD deploys necessary resources to support efforts of other USG departments and agencies, and allies.

b. *The National Military Strategy* and *The Department of Defense Cyber Strategy* provide high-level requirements for national defense in cyberspace and DOD's role in defending DOD and larger US national security interests through CO.

c. **DOD's Roles and Initiatives in Cyberspace.** DOD's roles in cyberspace are, for the most part, the same as they are for the physical domains. As a part of its role to defend the nation from threats in cyberspace, DOD prepares to support DHS and the Department of Justice (DOJ), the USG leads for incident response activities during a national cybersecurity incident of significant consequences. To fulfill this mission, DOD conducts military operations to defend DOD elements of CI/KR and, when ordered, defend CI/KR related to vital US interests. DOD's national defense missions, when authorized by Presidential orders or standing authorities, take primacy over the standing missions of other departments or agencies. *The Department of Defense Cyber Strategy* establishes strategic initiatives that offer a roadmap for DOD to operate effectively in cyberspace, defend national interests, and achieve national security objectives.

d. **National Incident Response.** When directed, DOD provides cyberspace defense support during major cyberspace threat events to the US. DOD coordinates with the requesting agency or department through the lead response department or agency, as described in the Presidential Policy Directive (PPD)-41, *United States Cyber Incident Coordination*. When DHS requests such support, the fundamental principles of DSCA used to respond to domestic emergencies in the physical domains also apply to CO support.

e. **CI/KR Protection.** CI/KR consist of the infrastructure and assets vital to the nation's security, governance, public health and safety, economy, and public confidence. IAW the *National Infrastructure Protection Plan*, DOD is designated as the sector-specific agency for the DIB. DOD provides cyberspace analysis and forensics support via the DIB Cybersecurity and Information Assurance Program and the DC3. Concurrent with its national defense and incident response missions, DOD may be directed to support DHS and other USG departments and agencies to help ensure all sectors of cyberspace CI/KR are available to support national objectives. CI/KR protection relies on analysis, warning, information sharing, risk management, vulnerability identification and mitigation, and aid to national recovery efforts. Defense critical infrastructure (DCI) is a subset of CI/KR that includes DOD and non-DOD assets essential to project, support, and sustain military forces and operations worldwide. Geographic combatant commanders (GCCs) have the responsibility to prevent the loss or degradation of DCI within their AORs and coordinate with the DOD asset owner, heads of DOD components, and defense infrastructure sector lead agents to fulfill this responsibility. CCDRs may act to prevent or mitigate the loss or degradation of non-DOD-owned DCI only in coordination with the CJCS and the Under Secretary of Defense for Policy (USD[P]) and at the direction of SecDef IAW Department of Defense Directive (DODD) 3020.40, *Mission Assurance (MA)*. As the lead agent of the DODIN sector of the DCI, the Commander, JFHQ-DODIN, is responsible for matters pertaining to the identification, prioritization, and remediation of critical DODIN infrastructure issues. Likewise, DOD coordinates and integrates when necessary with DHS for support of efforts to protect the DIB.

2. Authorities

a. Authority for CO actions undertaken by the US Armed Forces is derived from the US Constitution and federal law. Key laws that apply to DOD include Title 10, USC, *Armed Forces;* Title 50, USC, *War and National Defense;* and Title 32, USC, *National Guard.* See Figure III-1 for a summary of applicable titles of USC as they apply to CO.

b. Authorities for specific types of military CO are established within SecDef policies, including DOD instructions, directives, and memoranda, as well as in EXORDs and OPORDs authorized by the President or SecDef and subordinate orders issued by commanders approved to execute the subject missions. These include the directive authority for cyberspace operations (DACO), established by CJCS EXORD, that enables DOD-wide synchronized protection of the DODIN. The military missions and related actions of the cyberspace forces remain as described in Chapter II, "Cyberspace Operations Core Activities," regardless of the type of authority under which they are executed.

Refer to Appendix A, "Classified Planning Considerations for Cyberspace Operations," for additional information on authorities for CO.

3. Roles and Responsibilities

a. **SecDef**

(1) Directs the military, intelligence, and ordinary business operations of DOD in cyberspace.

United States Code

United States Code (USC)	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland security	Department of Homeland Security	Security of US cyberspace
Title 10	*Armed Forces*	National defense	Department of Defense	Man, train, and equip US forces for military operations in cyberspace
Title 18 Title 28	*Crimes and Criminal Procedure* *Judiciary and Judicial Procedure*	Law enforcement	Department of Justice	Crime prevention, apprehension, and prosecution of criminals operating in cyberspace
Title 32	*National Guard*	National defense and civil support training and operations, in the US	State Army National Guard, State Air National Guard	Domestic consequence management (if activated for federal service, the National Guard is integrated into the Title 10, USC), *Armed Forces*
Title 40	*Public Buildings, Property, and Works*	Chief Information Officer roles and responsibilities	All Federal departments and agencies	Establish and enforce standards for acquisition and security of information technologies
Title 44	*Public Printing and Documents*	Defines basic agency responsibilities and authorities for information security policy	All Federal departments and agencies	The foundation for what we now call cybersecurity activities, as outlined in Department of Defense Instruction, 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations*.
Title 50	*War and National Defense*	A broad spectrum of military, foreign intelligence, and counterintelligence activities	Commands, Services, and agencies under the Department of Defense and intelligence community agencies aligned under the Office of the Director of National Intelligence	Secure US interests by conducting military and foreign intelligence operations in cyberspace

Figure III-1. United States Code

(2) Provides policy and guidance for employment of forces conducting cyberspace missions through the USD(P), the SecDef's Principal Cyber Advisor, and the Deputy Assistant Secretary of Defense for Cyber Policy.

(3) Develops and issues the DOD Information Resources Management Strategic Plan through the DOD CIO. The DOD CIO is the DODIN architect and, as such, develops, maintains, and enforces compliance with DODIN architecture standards and cybersecurity policy. Inherent in the DOD CIO's architecture responsibility are the responsibilities for interoperability, data sharing, effective use of enterprise services, spectrum management, and DODIN program synchronization.

(4) Develops and oversees implementation of DOD policy, strategy, programs, and guidance regarding: intelligence; CI; security; sensitive activities; and other intelligence-related matters in cyberspace, to include all intelligence, surveillance, and reconnaissance (ISR) cyberspace activities and associated tasking, processing, exploitation, and dissemination through the Under Secretary of Defense for Intelligence IAW DODD 5143.01, *Under Secretary of Defense for Intelligence (USD[I]).*

(5) Coordinates with secretaries of other USG departments to establish appropriate representation and participation of personnel on joint interagency coordination groups (JIACGs), working groups, task forces, and collaboration and deconfliction bodies.

b. **CJCS**

(1) As the global integrator, advises the President and SecDef on operational policies, responsibilities, and programs.

(2) Assists SecDef in implementing operational responses to threats in cyberspace.

(3) Translates SecDef guidance into orders.

(4) Ensures cyberspace plans and operations are compatible with other military plans and operations.

(5) Assists CCDRs in meeting SecDef-approved operational requirements.

c. **Service Chiefs**

(1) Provide appropriate administration of and support to cyberspace forces, including Service-retained forces and forces assigned or attached to CCMDs.

(2) Train and equip cyberspace forces and develop cyberspace capabilities for deployment/support to CCMDs, as directed by SecDef.

(3) Comply with CDRUSCYBERCOM's direction for security, operation, and defense of their respective Service segments of the DODIN, including applicable direction issued under CDRUSCYBERCOM's DACO, either from USCYBERCOM directly or from JFHQ-DODIN or the SCCs, as delegated.

(4) Coordinate with CDRUSCYBERCOM to prioritize cyberspace mission requirements and force capabilities.

(5) Provide users of the EMS with regulatory and operational guidance in the use of frequencies through the authority of Army (Army Spectrum Management Office), Navy (Navy and Marine Corps Spectrum Center), and Air Force (Air Force Spectrum Management Office).

d. **Chief, National Guard Bureau (NGB)**

(1) Advises CDRUSCYBERCOM on NGB matters pertaining to CCMD CO missions, and supports planning and coordination for such activities as requested by the CJCS or the CCDRs.

(2) Serves as the channel of communications on all CO matters pertaining to the NG between USCYBERCOM and the 50 states, the Commonwealth of Puerto Rico, the District of Columbia, Guam, and the US Virgin Islands.

(3) Responds to direction from USCYBERCOM and JFHQ-DODIN, issued under DACO, to secure, operate, and defend the NGB segments of the DODIN.

e. **CDRUSCYBERCOM**

(1) As the coordinating authority for CO, plans, coordinates, integrates, synchronizes, and conducts activities to:

(a) Direct the security, operations, and defense of the DODIN.

(b) Prepare to, and when directed, conduct military CO external to the DODIN, including in gray and red cyberspace, in support of national objectives.

(2) Deconflicts cyberspace exploitation and cyberspace attack actions IAW national and DOD policy.

(3) For CO events requiring actions and effects across multiple geographic AORs, CDRUSCYBERCOM is the supported commander. For theater-specific events, CDRUSCYBERCOM may be designated a supporting or supported commander, depending upon the order issued.

(4) Leverages intelligence community (IC) sensors and directs DODIN sensors, as appropriate, to establish and share comprehensive situational awareness of red and gray cyberspace in support of assigned mission.

(5) Coordinates with the IC, CCMDs, Services, DOD agencies and activities, and multinational partners to facilitate development of improved cyberspace accesses to support planning and operations.

(6) As directed, provides military representation to USG departments and agencies, US commercial entities, and international organizations for cyberspace matters.

(7) Notifies the CCMDs of ongoing or developing cyberspace threats and anomalies to reduce potential risks and effectively integrate systems, networks, services, and EMS usage and to ensure compliance with DOD-mandated DODIN configuration standards.

(8) Performs analysis of threats to the DODIN, including threat analysis of foreign malicious cyberspace activity. In coordination with CCMDs, changes the global protection posture of the DODIN, as warranted by threat assessments.

(9) Plans for and, as directed, coordinates or executes DCO of US CI/KR.

(10) **Commander, JFHQ-DODIN.** In coordination with all CCDRs and other DOD components, conducts the operational-level planning, direction, coordination, execution, and oversight of global DODIN operations and DCO-IDM missions. Maintains support relationships, as established by CDRUSCYBERCOM, with all CCDRs for theater/functional DODIN operations and DCO-IDM. Commander, JFHQ-DODIN, is supported for global DODIN operations and DCO-IDM, and CCDRs are supported for DODIN operations and DCO-IDM with effects contained within their AOR or functional mission area. Exercises DACO over all DOD components as delegated by CDRUSCYBERCOM.

(11) **Commander, CNMF-HQ.** When directed, conducts the defense of the nation's cyberspace through operational-level planning, coordination, execution, and oversight of DCO-RA missions and, when directed, employment of national CPTs on DCO-IDM missions focused on internal threats to critical blue cyberspace outside the DODIN.

(12) **Commanders, SCCs.** In coordination with Commander, JFHQ-DODIN, conduct the operational-level planning, direction, coordination, execution, and oversight of DODIN operations and DCO-IDM within their Service portion of the DODIN. To achieve unity of action for protection of the DODIN, as directed, exercise DACO over organizations within their Service that take cyberspace security and cyberspace defense actions. Exercise administrative control of Service cyberspace forces, to include those that are Global Force Management Implementation Guidance (GFMIG)-assigned to USCYBERCOM.

(13) **Commanders, JFHQ-C.** Analyze, plan, and execute CO missions in support of the CCDRs. Focus on refining intelligence requirements (IRs), providing tactical expertise regarding feasibility of courses of action, and integrating CO into CCDR plans and orders.

(14) **USCYBERCOM Cyberspace Operations-Integrated Planning Element (CO-IPE).** Integrates within a CCDR's CO support staff to provide CO expertise and reachback capability to USCYBERCOM. CO-IPEs are organized from USCYBERCOM, JFHQ-DODIN, and JFHQ-C personnel and are co-located with each CCMD for full integration into their staffs. CO-IPEs provide a CCDR with CO planners and other subject

matter experts required to support development of CCMD requirements for CO and to assist CCMD planners with coordinating, integrating, and deconflicting CO.

f. **Other CCDRs**

(1) Secure, operate, and defend tactical and constructed DODIN segments within their commands and AORs.

(2) Integrate CO into plans (e.g., theater and functional campaign plans, concept plans [CONPLANs], and operation plans [OPLANs]); integrate cyberspace capabilities into military operations as required; and work closely with the joint force, USCYBERCOM, SCCs, and DOD agencies to create fully integrated capabilities.

(3) In coordination with USCYBERCOM, CCDRs orchestrate planning efforts for CO, designate the desired effects of CO, and determine the timing and tempo for CO conducted in support of their missions. Functional CCDRs direct DODIN operations and DCO-IDM over DODIN segments under their control, consistent with their functional responsibilities.

(4) GCCs lead, prioritize, and direct theater-specific DCO-IDM in response to compromises of DODIN security through the unified command theater network control center or equivalent organization. For cybersecurity events that have been categorized as a global event by USCYBERCOM, CDRUSCYBERCOM is the supported commander for the DCO-IDM, and other CCDRs support response efforts and tasking from JFHQ-DODIN.

(5) Serve as a focal point for in-theater DODIN operations that integrate multinational partners.

(6) Plan for communications system support of operations that may be directed by SecDef and ensure the interoperability of DOD forces with non-DOD mission partners in terms of equipment, procedures, and standards.

(7) Retain authority to approve or deny DOD component-initiated modifications to the DODIN that will impact in-theater operations only.

(8) In coordination with the DOD asset owner, heads of DOD components, and DOD infrastructure sector lead agents, GCCs act to prevent the loss, degradation, or other denial of DOD-owned DCI within their AORs. Act only in coordination with the CJCS and USD(P) to prevent or mitigate the loss or degradation for non-DOD-owned DCI.

(9) In coordination with CDRUSCYBERCOM, advocate for cyberspace capabilities and resources needed to support the CCDR's missions.

(10) Provide users of the EMS with regulatory and operational guidance in the use of required frequencies for CO IAW coordinated agreements between US forces and PNs.

g. **Commanders, US Pacific Command and US Northern Command.** In addition to responsibilities in paragraph 3.f., "Other CCDRs," these CCDRs fulfill specific CO responsibilities related to DSCA and homeland defense with CDRUSCYBERCOM and others, as required.

h. **Commander, United States Strategic Command (CDRUSSTRATCOM).** In addition to responsibilities in paragraph 3.f., "Other CCDRs," CDRUSSTRATCOM fulfills specific CO-related SATCOM responsibilities.

(1) Represents the DOD SATCOM community by coordinating and orchestrating consolidated user positions with CCMDs, Services, DOD agencies, and international partners. CDRUSSTRATCOM has operational and configuration management authority for the SATCOM component of the DODIN, including on-orbit assets, control systems, and DOD ground terminal and gateway infrastructure. Directs day-to-day operations of DOD-owned and leased SATCOM resources, as well as international partner and non-DOD SATCOM resources used by DOD to support mission requirements.

(2) Develops, coordinates, and executes SATCOM operations policies and procedures; constellation deployment plans; and satellite positioning, repositioning, and disposal plans. Assesses, in collaboration with DISA and JFHQ-DODIN, how these various plans impact communications support to current and future operations, OPLANs, and CONPLANs. Except in the case of emergencies, CDRUSSTRATCOM coordinates SATCOM actions with users prior to execution.

i. **Director, DISA**

(1) Complies with CDRUSCYBERCOM direction, through the commander of JFHQ-DODIN, to execute DODIN operations and DCO-IDM missions at the global and enterprise level, within DISA-operated portions of the DODIN.

(2) Provides engineering, architecture, and provisioning support for integrated DODIN operations, including enterprise management, content management, and mission assurance.

(3) Provides shared situational awareness of DISA-operated portions of the DODIN.

(4) Supports compliance inspections IAW Department of Defense Instruction (DODI) 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations.*

(5) Acquires all commercial SATCOM resources (unless the DOD CIO has granted a waiver to the requesting organization). Supports CDRUSSTRATCOM as the Consolidated SATCOM System Expert for commercial SATCOM and DOD gateways.

(6) Plans, mitigates, and executes service restoration at the global and enterprise level, as directed by commander of JFHQ-DODIN.

(7) Provides and maintains a critical nodes defense plan for long-haul communications.

j. **Director, National Security Agency/Chief, Central Security Service**

(1) Provides signals intelligence (SIGINT) support and cybersecurity guidance and assistance to DOD components and national customers, pursuant to DOD policy (DODI 8500.01, *Cybersecurity;* DODI, 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations;* and DODI 8560.01, *Communications Security [COMSEC] Monitoring and Information Assurance [IA] Readiness Testing);* Executive Order 12333, *US Intelligence Activities;* and National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*.

(2) Provides DOD with capacity/capability in both cyberspace security and cyberspace defense products and expertise and intelligence support required to execute CO, including operation of cyberspace perimeter defenses under direction of USCYBERCOM; target development assistance; situational awareness and attack sensing and warning; threat analysis; internal threat hunting; red-teaming and security assist visits; communications monitoring; forensics; linguist support; and other specialized support, as authorized.

k. **Director, Defense Intelligence Agency (DIA)**

(1) Provides timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policy makers.

(2) Conducts all-source analysis in support of CO, to include contributing to the development of CO-related joint intelligence preparation of the OE products.

(3) Serves as the DOD focal point for all CI cyberspace investigations and operations. In conjunction with the Military Departments and DOD agencies, DIA strives to identify and neutralize all CI-related cyberspace threats to DOD. DIA supports CI operations in cyberspace to promote cyberspace superiority and provides worldwide cyberspace CI situational awareness and coordination.

(4) In coordination with JS, Services, other DOD agencies and activities, and OSD, engineers, develops, implements, and manages the sensitive compartmented information portion of the DODIN, including the configuration of information, data, and communications standards for intelligence systems. Included within this is the overall responsibility for the operation of Joint Worldwide Intelligence Communications System, a strategic, secure, high-capacity telecommunications network serving the IC with voice, data, and video services. DIA establishes defense-wide intelligence priorities for achieving interoperability between tactical, theater, and national intelligence-related systems and between intelligence-related systems and the tactical, theater, and national elements of the DODIN.

(5) Sets policies, standards, and requirements for targets, including the virtual elements of facility, individual, organization, and equipment targets. All target development, to include targets in support of CO, adheres to the standards put forth in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3370.01, *Target Development Standards*.

l. **Director, DC3.** Administratively assigned to the Department of the Air Force but supporting the entire DOD, the DC3:

(1) Provides digital and multimedia forensics; cyberspace investigative training; research, development, test and evaluation; and cyberspace vulnerability analysis for DODIN protection, LE, IC, CI, and counterterrorism organizations.

(2) Serves as the DOD center of excellence and establishes DOD standards for digital and multimedia forensics.

(3) Serves as the operational focal point for the DIB cyberspace security information sharing activities performed to protect unclassified DOD information that transits or resides on unclassified DIB information systems and networks.

m. **Other DOD Agencies and Activities.** All DOD agencies and activities are responsible for developing and maintaining their IT in a manner consistent with and reflective of applicable DODIN architecture and cybersecurity standards, and they plan, resource, acquire, implement, and maintain agency-specific IT IAW the DOD policy and resource priorities. Those DOD agencies, which are also part of the IC, are additionally subject to the policies and guidance of the IC CIO. All DOD agencies and activities respond to direction from USCYBERCOM and JFHQ-DODIN, issued under DACO, to secure, operate, and defend their segments of the DODIN.

n. **DHS**

(1) DHS has the responsibility to secure US cyberspace, at the national level, by protecting non-DOD USG networks against cyberspace intrusions and attacks, including actions to reduce and consolidate external access points, deploy passive network defenses and sensors, and define public and private partnerships in support of national cybersecurity policy.

(2) DHS protects USG network systems from cyberspace threats and partners with government, industry, and academia, as well as the international community, to make cybersecurity a national priority and a shared responsibility.

(3) Pursuant to the Homeland Security Act of 2002 and Homeland Security Presidential Directive-5, *Management of Domestic Incidents,* the Secretary of Homeland Security is the principal federal official for domestic incident management. Pursuant to PPD-41, *United States Cyber Incident Coordination,* DHS is the lead federal agency for cyberspace incident asset response. For significant cybersecurity incidents external to the DODIN and IC networks, DHS's National Cybersecurity and Communications

Integration Center is the lead federal agency for technical assistance and vulnerability mitigation.

o. **DOJ**

(1) DOJ, including the Federal Bureau of Investigation (FBI), leads counterterrorism and CI investigations and related LE activities associated with government and commercial CI/KR. DOJ investigates, defeats, prosecutes, and otherwise reduces foreign intelligence, terrorist, and other cyberspace threats to the nation's CI/KR. The FBI is the lead agency for significant cybersecurity incident threat response activities, except those that affect the DODIN or the IC. Given the ability of malicious cyberspace activity to spread, investigation of threats to the DODIN will need to be coordinated with the FBI.

(2) The FBI also conducts domestic collection, analysis, and dissemination of cybersecurity threat information and operates the National Cyber Investigative Joint Task Force, a multi-agency focal point for coordinating, integrating, and sharing pertinent information related to cybersecurity threat investigations, with representation from DHS, the IC, DOD, and other agencies as appropriate.

4. Legal Considerations

a. DOD conducts CO consistent with US domestic law, applicable international law, and relevant USG and DOD policies. The laws that restrict military actions in US territory also apply to cyberspace. Therefore, DOD cyberspace forces that operate outside the DODIN, when properly authorized, are generally limited to operating in gray and red cyberspace only, unless they are issued different ROE or conducting DSCA under appropriate authority. Since each CO mission has unique legal considerations, the applicable legal framework depends on the nature of the activities to be conducted, such as OCO or DCO, DSCA, ISP actions, LE and CI activities, intelligence activities, and defense of the homeland. Before conducting CO, commanders, planners, and operators require clear understanding of the relevant legal framework to comply with laws and policies, the application of which may be challenging given the global nature of cyberspace and the geographic orientation of domestic and international law. It is essential commanders, planners, and operators consult with legal counsel during planning and execution of CO.

b. **Application of the Law of War.** Members of DOD comply with the law of war during all armed conflicts and in all other military operations. The law of war encompasses all international law for the conduct of armed hostilities binding on the US or its individual citizens, including treaties and international agreements to which the US is a party and applicable customary international law. The law of war rests on fundamental principles of military necessity, proportionality, distinction (discrimination), and avoidance of unnecessary suffering, all of which may apply to certain CO.

See JP 1-04, Legal Support to Military Operations; *DODD 2311.01E,* DOD Law of War Program; *CJCSI 5810.01,* Implementation of the DOD Law of War Program; *and the* Department of Defense Law of War Manual *for more information on the law of war.*

CHAPTER IV
PLANNING, COORDINATION, EXECUTION, AND ASSESSMENT

"We're trying to both physically and virtually isolate ISIL [Islamic State of Iraq and the Levant], limit their ability to conduct command and control, limit their ability to communicate with each other, limit their ability to conduct operations locally and tactically. I'll be one of the first ones arguing that that's about all we should talk about.... We want them to be surprised when we conduct cyber[space] operations. And, frankly, they're going to experience some friction that's associated with us and some friction that's just associated with the normal course of events in dealing in the information age."

General Joseph Dunford
Chairman of the Joint Chiefs of Staff
February 2016 News Conference

1. Joint Planning Process and Cyberspace Operations

a. Commanders integrate CO into their operations at all levels. Their plans should address how to effectively integrate cyberspace capabilities, counter adversaries' use of cyberspace, identify and secure mission-critical cyberspace, access key terrain in cyberspace, operate in a degraded environment, efficiently use limited cyberspace assets, and pair operational requirements with cyberspace capabilities. The commander provides initial planning guidance, which may specify time constraints, outline initial coordination requirements, authorize the movement of forces within the commander's authority, and direct other actions as necessary. Supporting CO plans and concepts describe the role and scope of CO in the commander's effort and address how CO support the execution of the supported plan. If requested by a commander, CDRUSCYBERCOM provides assistance in integrating cyberspace forces and capabilities into the commander's plans and orders.

b. JP 5-0, *Joint Planning,* describes the joint planning process (JPP) as a proven process to organize the work of the commander, staff, subordinate commanders, and other partners to develop plans that appropriately address the problem to be solved. It focuses on framing the situation and end states, defining the military mission, analysis of critical factors, and designing an operational approach to accomplish mission objectives. CO capabilities and functions are integrated along with all other joint capabilities and functions into the JPP and into the Adaptive Planning and Execution enterprise.

See JP 5-0, Joint Planning, *for more information on the JPP.*

2. Cyberspace Operations Planning Considerations

a. **Overview.** Although CO planners are presented the same operational design considerations and challenges as planners for operations in the physical domains, there are some unique considerations for planning CO. For instance, because of unforeseen linkages in cyberspace, higher-order effects of some CO may be more difficult to predict. This may require more branch and sequel planning. Further, while many elements of cyberspace can be mapped geographically, a full understanding of an adversary's disposition and

capabilities in cyberspace involves understanding the target, not only at the underlying physical network layer but also at the logical network layer and cyber-persona layer, including profiles of system users and administrators and their relationship to adversary critical factors. For planning internal operations within DOD cyberspace, DODIN operations and DCO-IDM planners require a clear understanding of which friendly forces or capabilities might be targeted by an adversary; what DODIN vulnerabilities are most likely to be targeted and the potential effects of the adversary's action; the mission assurance risks involved; and an understanding of applicable domestic, foreign, and international laws and USG policy. Threats in cyberspace may be nation-states, non-state groups, or individuals, and the parts of cyberspace they control are not necessarily within the geographic borders associated with the threat's nationality or proportional to their geopolitical influence. A criminal element, a politically motivated group, or even a well-resourced individual may have a greater presence and capability in cyberspace than do many nations. Moreover, many adversaries operate cyberspace capabilities from portions of cyberspace geographically associated with the US or owned by a US entity. Each of these factors complicates the planning of CO.

b. **Planning Timelines.** For external missions, it is essential OCO and DCO-RA planners understand the authorities required to execute the specific CO actions proposed. The applicable authorities may vary depending upon the phase of the operation. This includes accounting for the lead time required to obtain the necessary intelligence to define the correct target; develop target access; confirm the appropriate authorities; complete necessary coordination, including interagency coordination and/or synchronization; and to verify the cyberspace capability matches the intended target using the results of technical assurance evaluations. For internal missions, the timelines for DCO-IDM and DODIN operations planners are impacted by other factors, including levels of automation available to manage network posture, availability of security solutions from commercial providers and their licensing requirements, and operational considerations that may impact a defender's abilities to maneuver or take systems off-line to better manage their protection. However, the planning fundamentals remain the same, and despite the additional considerations and challenges of integrating CO, planners use most elements of the traditional processes to implement the commander's intent and guidance.

c. **Planning Considerations for Operating in Red and Gray Cyberspace**

(1) **Characteristics of Cyberspace Capabilities.** While cyberspace is complex and ever changing, cyberspace capabilities, whether devices or computer programs, must reliably create the intended effects. However, cyberspace capabilities are developed based on environmental assumptions and expectations about the operating conditions that will be found in the OE. These conditions may be as simple as the type of computer operating system being used by an adversary or as complex as the exact serial number of the hardware or version of the software installed, what system resources are available, and what other applications are expected to be running (or not running) when the cyberspace capability activates on target. These expected conditions should be well documented by the capability developer and are important for planners and targeting personnel to understand as capability limitations. The extent to which the expected environmental conditions of a target cannot be confirmed through ISR sources represents an increased level of risk

associated with using the capability. All other factors being equal, cyberspace capabilities that have the fewest environmental dependencies and/or allow the operator to reconfigure the capability are preferred. DODI O-3600.03, *Technical Assurance Standard (TAS) for Computer Network Attack (CNA) Capabilities,* provides detailed requirements for technical assurance evaluations that document these characteristics.

(2) **Cascading, Compounding, and Collateral Effects.** Overlaps among military, other government, corporate, and private activities on shared networks in cyberspace make the evaluation of probable cascading, compounding, and collateral effects particularly important when targeting for CO. The effects can ripple through a targeted system, sometimes cascading through links with related systems that were not evident to the planner. Cascading effects sometimes travel through systems subordinate to the one targeted but can also move laterally to peer systems or up to higher-level systems. Compounding effects are an aggregation of various levels of effects that have interacted in ways that may be intended or may have been unforeseen. Collateral effects, including collateral damage, are the incidental effects of military operations on non-combatants and civilian property that were not the intended targets of the strike. Depending upon the strategic and operational situation, an order or applicable ROE may limit CO to only those actions likely to result in no or low levels of collateral effects. A collateral effects estimate to meet policy restrictions is separate from the proportionality analysis required by the law of war. This estimate is a tool for the commander to understand risk when considering approval of operations. Therefore, even if a proposed CO is permissible after a collateral effects analysis, the likely effects of the proposed CO must also be permissible under a law of war proportionality analysis, as applicable.

(3) **Reversibility of Effects.** An important consideration for planning cyberspace attack and cyberspace exploitation effects is the level of control over the duration of the effect that can be exercised by friendly forces. There are two basic ways to categorize effects by this standard:

(a) **Operator Reversible Effects.** Effects that can be recalled, recovered, or terminated by friendly forces. These effects may represent a lower risk of undesired consequences, including discovery or retaliation.

(b) **Non-Operator Reversible Effects.** Effects that cannot be recalled, recovered, or terminated by friendly forces after execution. These effects may represent a higher risk of response from the threat or other undesired consequences and may require more coordination.

See Appendix A, "Classified Planning Considerations for Cyberspace Operations," for additional planning considerations for external missions. See JP 3-60, Joint Targeting, *for additional information on creation of effects. Refer to CJCSI 3160.01,* No-Strike and the Collateral Damage Estimation Methodology, *for additional information on collateral damage.*

d. **Planning Considerations for Protecting the DODIN**

(1) **For Specific Plans and Operations.** DODIN operations underpin nearly every aspect of military operations, and this reliance on cyberspace is well understood by our adversaries. However, a commander's reliance on specific segments of the DODIN is often not considered during plans development, but planning for DODIN resiliency is essential. JFC planning staffs should incorporate DCO-IDM branches and sequels for any operations that pose an increased threat to the DODIN. The CCDR's CO staff coordinates and deconflicts DCO-IDM mission activities with the USCYBERCOM CO-IPEs. If the planned defensive actions will create effects in cyberspace outside of the GCC's AOR, JFHQ-DODIN will ensure the cyberspace defense actions are coordinated and synchronized globally.

(2) **Prioritizing DODIN Protection.** Cybersecurity policies generally apply to all of the DODIN, unless specific exceptions or waivers are granted. Each segment of the DODIN has an organization responsible for its security and first-line defensive actions, including administrative and non-mission-critical networks, which are protected primarily by their operators and their CSSP. Some of these protection services may be contracted, particularly when the creation and operation of the network itself has been contracted. The determination of whether or not a specific piece of contractor hardware or a specific contractor network segment is considered part of the DODIN is determined by the exact language of the contract. Given the limited number of CPTs and other cyberspace forces, the significant scope of the DODIN means not every segment can be defended in the same depth. Primarily, these specialized cyberspace forces focus on protecting the highest priority segments of the DODIN, including mission-critical, classified, and those directly supporting operations. As resources allow, CPTs may assist service providers and network segment operators with defense of lower priority networks.

(3) **Coordinating DODIN Defense.** Effective response to intrusions or other malicious activity on the DODIN requires coordinated action. Although the ultimate goal of DCO is to defeat the threat and reestablish secure cyberspace, the nature of the threat determines the specific response to each incident. All cybersecurity incidents are reported IAW DOD policy, but some threat adversary activity may be effectively remediated by well-trained, local cyberspace forces without external support. Sophisticated nation-state threats that penetrate our security measures require a different type of response. Each encounter with a peer or near-peer adversary in cyberspace warrants careful consideration of the response. Choosing when, where, and how to engage the threat is as important in DCO as it is to defense in the physical domains. If circumstances allow, including a consideration of threat to the supported mission, intelligence gain/loss (IGL) considerations may suggest careful observation of the threat while limiting its maneuver. When a command is engaged with a threat in cyberspace, the global enterprise adapts to support that command IAW defensive priorities. Reachback support for analytics, intelligence, and even fires is provided to maintain continuity of operations at the supported command. Local and Service commanders consult with USCYBERCOM and its subordinate HQ staffs to create tailored responses to specific threats. Some incidents require remote or on-site response by CPTs to assist network operators and the assigned CSSP with remediation and restoration of the affected network segment.

(4) **Situational Awareness.** Cyberspace situational awareness is the requisite current and predictive knowledge of cyberspace and the OE upon which CO depend, including all factors affecting friendly and adversary cyberspace forces. A commander continually assesses the OE through a combination of staff element and other reporting; personal observation; intelligence, to include threat warning; and representations of various activities occurring in the OE using a common operational picture (COP). The DODIN is a primary source of information used to support the commander's situational awareness of the OE, including the status of the DODIN itself. Sustainment of DODIN sensors, communication channels, data feeds, and user interfaces is a key outcome of DODIN operations. Accurate and comprehensive situational awareness is critical for rapid decision making in a constantly changing OE and while engaging an elusive, adaptive adversary. Situational awareness of adversary activity in gray and red cyberspace relies heavily on cyberspace exploitation and SIGINT, but contributions can come from all sources of intelligence. Situational awareness within the DODIN is provided by the Services and agencies operating their portions of the DODIN, by DISA and JFHQ-DODIN through the network operations and security centers, by USCYBERCOM's Joint Operations Center, and by the Joint Functional Component Command for Space's Joint Space Operations Center for SATCOM. They coordinate with each other as required for operational effectiveness and shared situational awareness. The ever-increasing complexity and scope of cyberspace means a commander never has perfect or even optimal situational awareness of cyberspace factors that could impact operations and should consider the risks represented by this lack of information when making decisions.

e. **Preparing for Assessment.** Assessment is used to measure progress of the joint force toward mission accomplishment. Commanders continuously assess the OE and the progress of operations and compare them to their initial vision and intent. The assessment process begins during the planning process and helps the commander and staff decide what to measure and how to measure it, in order to determine progress toward accomplishing a task, creating an effect, or achieving an objective. The data collected to support these measures can range from simply noting an inability to reach the target network after a cyberspace attack to complex network monitoring and statistical analysis. Data gathered about the target's state prior to the operation, through access, execution, and possibly its long-term post-attack state, may facilitate later assessment of higher-order effects. Assessment of internal missions to protect the DODIN requires similar preparation. It is difficult to determine the degree that protection measures reduce risk to mission without accurate knowledge of the initial conditions of the network. Assessment of CO is not limited to analysis of data from within cyberspace. For example, if the desired effect of an OCO mission was to cause a power outage, the assessment might be made using visual sensors to observe indications of an outage. Planners submit assessment requests, with sufficient justification, as early as is necessary for the appropriate allocation of resources. For further information, see paragraph 7, "Assessment of Cyberspace Operations."

Refer to Appendix A, "Classified Planning Considerations for Cyberspace Operations," for additional information on planning CO.

3. Intelligence and Operational Analytic Support to Cyberspace Operations Planning

a. **IRs.** During mission analysis, the joint force staff identifies significant information gaps about the adversary and other relevant aspects of the OE. After gap analysis, the staff formulates IRs, which are general or specific subjects upon which there is a need for the collection of information or the production of intelligence. Based upon identified IRs, the staff develops more specific questions known as information requirements (those items of information that must be collected and processed to develop the intelligence required by the commander). Information requirements related to cyberspace can include such things as network infrastructures and status, readiness of adversary's equipment and personnel, and unique cyberspace signature identifiers such as hardware/software/firmware versions and configuration files. These IRs are met through a combination of military intelligence and national intelligence sources.

See JP 2-0, Joint Intelligence, *for additional information on IRs.*

(1) **Requests for Information (RFIs).** CO planners can submit an RFI to generate intelligence collection efforts in any part of the OE or discipline in support of the JPP. RFIs are specific, time-sensitive, ad hoc requirements for intelligence information to support an ongoing crisis or operation and not necessarily related to standing requirements or scheduled intelligence production. RFIs fulfill customer requirements and range from disseminating existing products through integrating or tailoring on-hand information to scheduling new collection and production. The RFI manager translating the customer's requirement and the primary intelligence producer determine how best to meet the customer's needs. In addition to information collected during military operations, information required to support CO planning can come from SIGINT, human intelligence, CI, measurement and signature intelligence, geospatial intelligence, or open-source intelligence (OSINT). Regardless of source, the information should be timely, accurate, and in a usable format.

See JP 2-01, Joint and National Intelligence Support to Military Operations, *for additional information on RFIs.*

(2) **Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) Architecture.** The DOD's global connectivity enables commanders to task assigned or attached ISR sensors or assets and submit collection and production requirements directly to other ISR or IC activities.

For more information on TCPED, see JP 2-01, Joint and National Intelligence Support to Military Operations.

b. **Threat Detection and Characterization.** Some threats in cyberspace are detected by intelligence sources and others during the course of military maneuver.

(1) **Detection.** The activities in cyberspace of a sophisticated threat may be difficult to detect. Unlike actions in the physical domains, which are often detected by the presence of military equipment or other types of observables, threat actions in cyberspace

may not be easily distinguishable from legitimate network activity. Detecting of activities in cyberspace is critical for enabling effective CO.

(2) **Characterization.** Because the DOD cyberspace missions are categorized based on the commander's intent and because friendly forces are often uncertain of a threat's actual intent, threat activities in cyberspace are referred to more generically. Threat actions in cyberspace are generally referred to as malicious cyberspace activity. If known details of adversary activity support more precise categorization, specific threat actions may qualify as cyberspace attack if they have created noticeable denial effects or cyberspace exploitation if the adversary has only maneuvered for collection or enabling purposes.

(3) **Analysis and Attribution.** Due to the characteristics of the physical network, logical network, and cyber-persona layers of cyberspace, attribution of malicious cyberspace activity to a specific person, criminal organization, non-state threat, or even a responsible nation-state can be exceptionally difficult. Although attribution is not necessarily required for self-defense, the difficulty of attribution, along with the possibility that an apparent threat may actually be an attempt at misdirection, is one of the principal reasons DCO-RA mission planning may be more difficult than planning for response to conventional attack. The risks of a defensive response against the wrong threat, particularly a nation-state or a target within an unwitting nation-state where the attack originated, are weighed against strategic objectives and the consequences of making an attribution mistake. Working effectively within these constraints requires unique skills on the part of all-source intelligence analysts to understand the context of the threat activity. They use skills like analyzing deception techniques, anonymity techniques, virtual representations and avatars, and other artifacts of the logical network and cyber-persona layers to characterize activities with the requisite degree of confidence required to enable an effective response.

c. **IGL.** Another planning concern is that maneuver and fires in red and gray cyberspace could potentially compromise intelligence collection activities sources and methods. To the maximum extent practicable, an IGL assessment is required prior to executing such actions. The IGL assessment can be complicated by the array of non-DOD USG and multinational partners operating in cyberspace. JFCs use IGL analysis to weigh the risks of conducting the CO versus achieving the desired objective via other methods.

d. **Warning Intelligence.** Cyberspace threat intelligence includes all-source analysis to factor in political, military, and technical warning intelligence. Adversary cyberspace actions may occur separate from, and well in advance of, related activities in the physical domains. Additionally, cyberspace threat sensors may recognize malicious activity with only a very short time available to respond. These factors make the inclusion of all-source intelligence analysis very important for effectively assessing adversaries' intentions in cyberspace.

e. **OSINT.** All-source intelligence analysis of cyberspace sources should take advantage of the information available from OSINT, including Internet social media and other nontraditional sources of information. The constantly evolving sphere of open-

source activity offers the opportunity to add useful data to all-source analysis. But this constantly changing landscape of media and the low "signal to noise" ratio of data available in cyberspace also complicate the intelligence collection problem, requiring active collection management to stay abreast of these sources.

f. **ISR in Cyberspace.** ISR in cyberspace is an activity that synchronizes and integrates the planning and operation of sensors; assets; and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. ISR in cyberspace focuses on gathering tactical and operational information and on mapping enemy and adversary networks to support military planning. To facilitate the optimum utilization of all available ISR assets, an ISR concept of the operations (CONOPS) should be developed in conjunction with the command's planning effort. The ISR CONOPS should be based on the collection strategy and ISR execution planning and should be developed jointly by the joint force intelligence directorate of a joint staff and the operations directorate of a joint staff. The ISR CONOPS documents the synchronization, integration, and operation of ISR resources in direct support of current and future operations. It outlines the capability to task, collect, process, exploit, and disseminate accurate and timely information that provides the awareness necessary to successfully plan and conduct operations. It addresses how all available ISR collection assets and associated processing, exploitation, and dissemination infrastructure, including multinational and commercial assets, will be used to satisfy the joint force's anticipated collection tasks. It also requires appropriate deconfliction and personnel that are trained and certified to a common standard with the IC.

4. Targeting

The purpose of targeting is to integrate and synchronize fires (the use of weapon systems or other actions to create a specific lethal or nonlethal effect on a target) into joint operations. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. Integrating and synchronizing planning, execution, and assessment are pivotal to the success of joint targeting. The overall joint targeting cycle and target development process described in JP 3-60, *Joint Targeting,* apply generally to targeting in support of CO. In addition, the coordination required by Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3139.01, *(U) Review and Approval Process for Cyberspace Operations,* for certain OCO and DCO-RA missions is unique to CO and applies to many aspects of the joint targeting cycle. Therefore, CO planners and decision makers often use a targeting process specifically adapted to the circumstance. Three fundamental aspects of CO require consideration in the targeting processes: recognizing cyberspace capabilities are a viable option for engaging some designated targets; understanding a CO option may be preferable in some cases, because it may offer low probability of detection and/or no associated physical damage; and higher-order effects on targets in cyberspace may impact elements of the DODIN, including retaliation for attacks attributed to the joint force. Additionally, some characteristics unique to the cyberspace components of targets and to cyberspace capabilities are described below.

a. **Targeting In and Through Cyberspace.** Planning and targeting staffs develop and select targets in and through cyberspace based on the commander's objectives rather than on the capabilities available to achieve them. The focus is on creating effects that accomplish targeting-related tasks and objectives, not on using a particular cyberspace capability simply because it is available. Targets that can be accessed in cyberspace are developed, vetted, and validated within the established targeting process. Although targets paired with cyberspace capabilities can often be engaged with no permanent damage, due to the interconnectedness of cyberspace, the effects of CO may cross geographical boundaries and, if not carefully planned, may have unanticipated effects. As a result, engaging targets in and through cyberspace requires close coordination within DOD and with interagency and multinational partners. Every target has distinct intrinsic or acquired characteristics (i.e., physical, functional, cognitive, environmental, and temporal) that form the basis for detection, location, and identification; for determining target value within the target system; and for classification for future surveillance, analysis, strike, and assessment. The challenge in targeting for CO is to identify, correlate, coordinate, and deconflict multiple activities occurring across the physical network, logical network, and cyber-persona layers. This requires a C2 capability that can operate at the tempo of CO and can rapidly integrate impacted stakeholders.

(1) **Physical Network Layer Target Features.** The physical network layer is the medium where the data travels. It includes wired (e.g., land and undersea cable) and wireless (e.g., radio, radio-relay, cellular, satellite) transmission means. It is a point of reference for determining geographic location and the applicable legal framework.

(2) **Logical Network Layer Target Features.** The logical network layer provides an alternate view of the target, abstracted from its physical location, and referenced from its logical position in cyberspace. This position is often represented through a network address (e.g., IP address). It depicts how nodes in the physical domains address and refer to one another to form entities in cyberspace. The logical network layer is the first point where the connection to the physical domains may be lost. Targeting in the logical layer requires the logical identity and logical access to the target to have a direct effect.

(3) **Cyber-Persona Layer Target Features.** The cyber-persona layer, the aggregate of an individual's or group's online identity(ies), and an abstraction of logical network layer data, holds important implications for joint forces in terms of positive target identification and affiliation and activity attribution. Cyber-personas are created to group information together about targeted actors in order to organize analysis, engagement, and intelligence reporting. Because cyber-personas can be complex, with elements in many virtual locations but often not linked to a single physical location or form, sufficient intelligence collection and analysis capabilities are required for the joint forces to gain insight and situational awareness required to enable effective targeting of a cyber-persona. Ultimately, cyber-personas will be linked to features that will be engaged in either the logical or physical network layers.

b. **Target Access.** Cyberspace forces develop access to targets or target elements in cyberspace by using cyberspace exploitation actions. This access can then be used for

various purposes, ranging from information collection to maneuver and to targeting nomination. Not all accesses are equally useful for military operations. For instance, the level of access required to collect information from an entity may not be sufficient to create a desired effect. Developing access to targets in or through cyberspace follows a process which can often take significant time. In some cases, remote access is not possible, and close proximity may be required. All target access efforts in cyberspace require coordination with the IC for deconfliction IAW national policy and to illuminate potential IGL concerns. If direct access to the target is unavailable or undesired, sometimes a similar or partial effect can be created by indirect access using a related target that has higher-order effects on the desired target. Some denial of service cyberspace attacks leverage this type of indirect access.

c. **Target Nomination and Synchronization.** CO use standard target nomination processes, but target folders should include unique cyberspace aspects (e.g., hardware and software configurations, IP address, cyber-persona applications) of the target. Development of this data is imperative to understand and characterize how elements targetable through cyberspace are relevant to the commander's objective. This data also allows the planner to match an appropriate cyberspace capability against a particular target. Component commanders, national agencies, supporting commands, and/or the JFC planning staff nominate targets to the targeting staff for development and inclusion on the joint target list (JTL). Once placed on the JTL, JFCs in receipt of an EXORD with relevant objectives and ROE can engage the target with organic assets (if within a component commander's assigned area of operations) or nominate the target to CDRUSCYBERCOM for action by other joint force components and other organizations.

See JP 3-60, Joint Targeting, *and CJCSI 3370.01,* Target Development Standards, *for additional details on vetting, validation, and joint targeting working groups.*

d. **Time-Sensitive Targets (TSTs)**

(1) A TST is a validated target of such high priority to friendly forces that the commander designates it for immediate engagement because it poses (or will soon pose) a threat to friendly forces or is a highly lucrative, fleeting target. TSTs are normally engaged dynamically. However, to be successfully engaged, they require considerable planning and preparation within the joint targeting cycle. Engaging TSTs in cyberspace is difficult in most situations, because they are likely to cross-AORs and require detailed joint, interagency, and/or multinational planning efforts.

(2) Being prepared to engage a TST in cyberspace requires coordination between cyberspace planners, operators, and the supported commander early in the planning phase, to increase the likelihood that adequate flexibility and access is available should a fleeting opportunity arise. In addition, JFCs should establish procedures to quickly promulgate strike orders for TSTs in cyberspace. Successful prosecution of TSTs in cyberspace requires a well-organized and well-rehearsed process for sharing sensor data and target information, identifying suitable strike assets, obtaining mission approval, and rapidly deconflicting cyberspace capability employment. Performing as much advanced

coordination and decision making as possible, based on the types of TSTs expected and the nature of the mission, is the key to success.

See JP 3-60, Joint Targeting, *for additional information on joint targeting, and JP 2-01,* Joint and National Intelligence Support to Military Operations, *for additional information on intelligence operations.*

Refer to Appendix A, "Classified Planning Considerations for Cyberspace Operations," for additional information on intelligence support to planning CO.

5. Command and Control of Cyberspace Forces

a. Clearly established command relationships are crucial for ensuring timely and effective employment of forces, and CO require unity of command and unity of effort. However, the complex nature of CO, where cyberspace forces can be simultaneously providing actions at the global level and at the theater or JOA level, requires adaptations to traditional C2 structures. Joint forces principally employ centralized planning with decentralized execution of operations. CO require constant and detailed coordination between theater and global operations, creating a dynamic C2 framework that can adapt to the constant changes, emerging threats, and unknowns. Certain CO functions, including protection of the DODIN's global networks and pursuit of global cyberspace threats, lend themselves to centralized planning and execution to meet multiple, near-instantaneous requirements for response. Centrally controlled CO should be integrated and synchronized with the CCDR's regional or local CO, conducted by forces assigned or attached to the CCDR, or in support of the CCDR. For these reasons, there may be times when C2 of forces executing simultaneous global CO and theater CO is conducted using supported/supporting command relationships under separate, but synchronized, chains of command. CO are integrated and synchronized by the supported commander into their CONOPS, detailed plans and orders, and specific joint operations.

b. **C2 for Global CO.** CDRUSCYBERCOM is the supported commander for transregional and global CO and manages day-to-day global CO even while he or she is the supporting commander for one or more geographic or functional CCDR's operations. For a specific CO mission, the supported/supporting command relationships are established in an EXORD, OPORD, or establishing directive. A supported relationship for CO does not exempt either command from coordinating response options with affected commanders prior to conducting an operation. Regardless of the approach employed for any particular operation, unless otherwise specified by the President or SecDef, C2 for CO are implemented IAW existing CJCS C2 EXORD and other relevant orders to help ensure effective coordination and synchronization of joint forces and to provide a common construct for JFCs to execute their mission within a global context. JFHQ-DODIN centrally coordinates and directs global DODIN operations and DCO-IDM when these operations have the potential to impact the integrity and operational readiness of multiple DOD components. Although execution of many actions may be decentralized, CDRUSCYBERCOM is the supported commander for CO to secure, operate, and defend the DODIN and, when ordered, to defend other US critical cyberspace assets, systems, and functions. As the DODIN continues to migrate towards a common architecture standard,

routine cyberspace security actions for global networks will continue shifting to centralized locations, such as a global enterprise operations center.

c. **C2 for CO Supporting CCMDs.** CCDRs are supported for CO in their AOR or for their transregional responsibilities, with CDRUSCYBERCOM supporting as necessary. These CO comprise actions intended to have effects localized within a GCC's AOR or a functional CCMD's transregional responsibilities. These could be cyberspace security and defense actions internal to a theater DODIN segment or external actions, such as cyberspace exploitation or cyberspace attack against a specific enemy capability. In addition to the theater segments of global networks, CCMD-level DODIN operations and DCO-IDM include the protection of stand-alone and tactical networks and computers used exclusively by the CCMD. For example, CCMD-level maneuvers in cyberspace include activities to reposition capabilities to enhance threat detection in specified areas, focus cyberspace forces activity in areas linked to specific operational branches and sequels to keep the adversary at risk, or activate stand-by tactical cyberspace capabilities to transition friendly C2 to more secure locations. Such CO maneuvers are vital when a CCDR's systems are under attack to the degree that subsets of the DODIN are degraded, compromised, or lost. In such operations, the supported CCDR coordinates, through their USCYBERCOM CO-IPE, with their associated enterprise operation center, supported by JFHQ-DODIN and DISA, to restore the affected cyberspace. The supported CCDR also integrates, synchronizes, and normally directs CO actions in red and gray cyberspace, including fires, with other lethal and nonlethal effects, for which they may use assigned, attached, or supporting cyberspace forces. CCDRs develop and coordinate their requirements for such effects with the USCYBERCOM CO-IPE, for deconfliction and prioritized execution. When a CCDR establishes a subordinate force (e.g., a joint task force), the cyberspace unit(s) assigned to support that force are determined by the CCDR's mission requirements in coordination with CDRUSCYBERCOM.

d. **C2 Distinctives for Routine and Crisis/Contingency CO.** The CJCS has established two models for C2 of CO, depending upon the prevailing circumstances. The relationships are described below and depicted graphically in Figure IV-1 and Figure IV-2.

(1) The following relationships guide the C2 of cyberspace forces during normal operating conditions, when no crisis or contingency is in effect:

(a) USCYBERCOM C2 relationships:

1. CDRUSCYBERCOM has COCOM of all GFMIG-assigned cyberspace forces.

2. CDRUSCYBERCOM has support relationships with all other CCDRs.

3. CNMF commander has OPCON of NMTs/NSTs and national CPTs.

4. JFHQ-C commanders have OPCON of CMTs/CSTs.

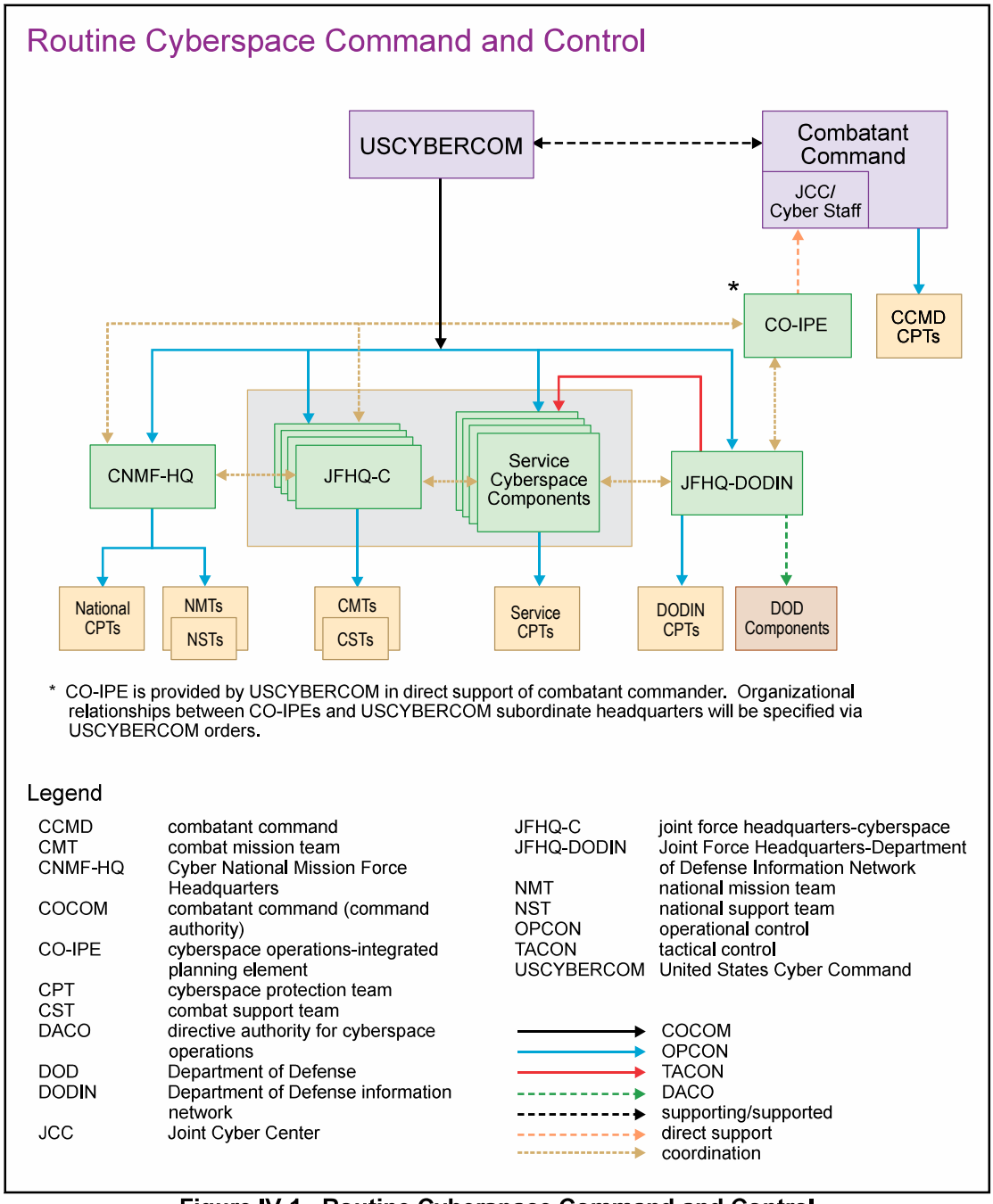


Figure IV-1. Routine Cyberspace Command and Control

5. SCC commanders have OPCON of Service CPTs and other forces attached by CDRUSCYBERCOM (e.g., CSSPs).

6. JFHQ-DODIN commander has OPCON of DODIN CPTs.

7. JFHQ-DODIN commander has tactical control (TACON) of SCC commands for DODIN operations and DCO-IDM only.

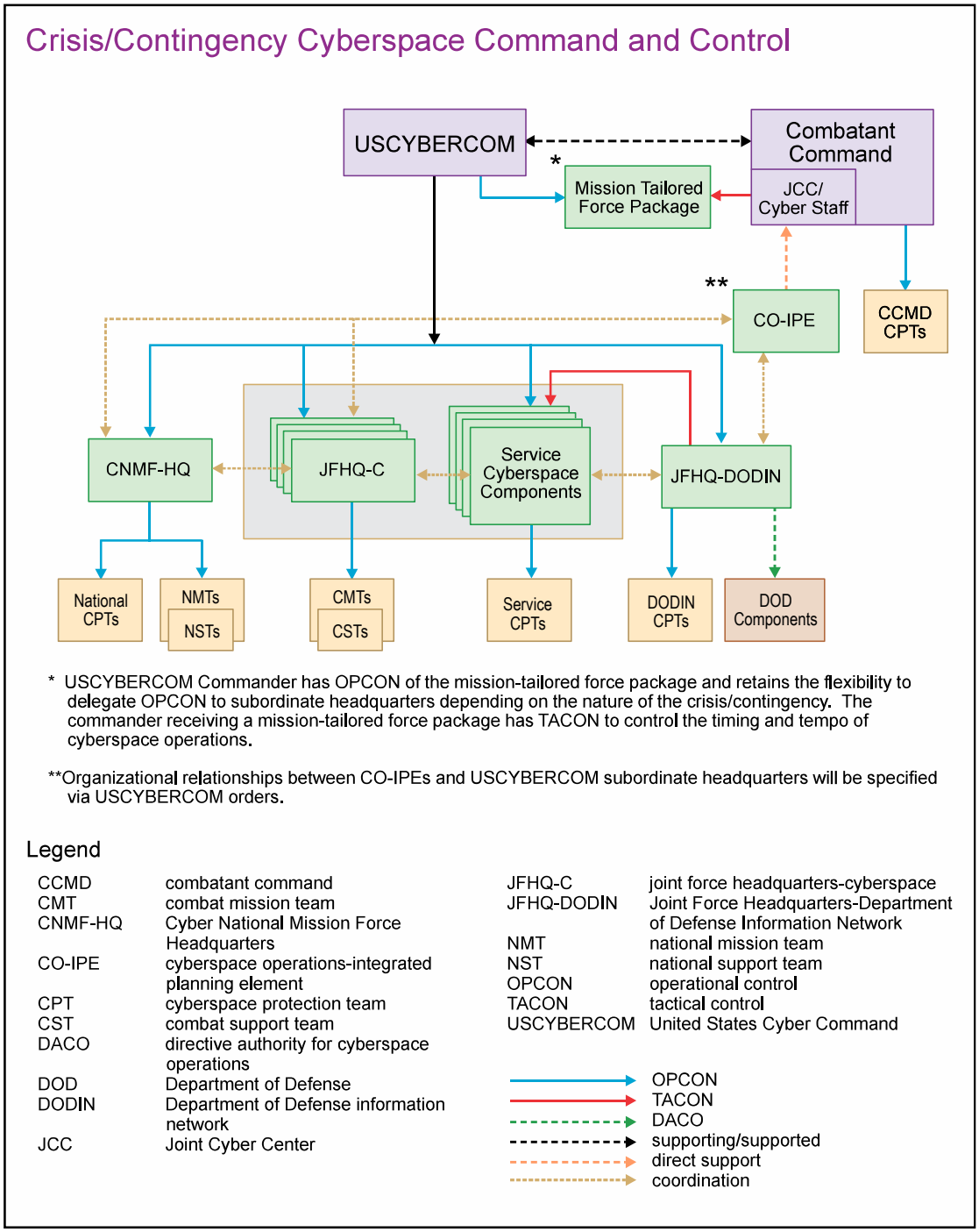


Figure IV-2. Crisis/Contingency Cyberspace Command and Control

8. JFHQ-DODIN commander has DACO, delegated from CDRUSCYBERCOM, over all DOD components for global DODIN operations and DCO-IDM.

9. SCC commanders have DACO, delegated from CDRUSCYBERCOM, over all related Service components for DODIN operations and DCO-IDM.

(b) CCMD C2 relationships:

1. CCDRs have COCOM of assigned cyberspace forces.

2. CCDRs have OPCON of CCMD CPTs.

3. SecDef establishes support relationships between CCDRs for CO.

4. JFHQ-C commanders support more than one CCDR using the general support model.

5. USCYBERCOM CO-IPEs provide direct support to CCDRs.

(2) When a cyberspace-related crisis or contingency is in effect, the routine relationships carry over, with these additional caveats:

(a) USCYBERCOM commander retains OPCON of any cyberspace forces USCYBERCOM provides to support a CCDR for crisis/contingency operations.

(b) When directed, CCDRs receiving forces from USCYBERCOM for crisis/contingency operations (e.g., a mission-tailored force package [MTFP]) have TACON of those forces.

(3) **MTFP.** A MTFP is a USCYBERCOM-tailored support capability comprised of assigned CO forces, additional CO support personnel, and cyberspace capabilities, as required. When directed, USCYBERCOM establishes a tailored force to support specific CCMD crisis or contingency mission requirements beyond the capacity of forces available for routine support. Each MTFP is task-organized and provided to the supported CCDR for the duration of the crisis/contingency operation or until redeployed by CDRUSCYBERCOM in coordination with the supported CCDR.

e. **C2 Distinctives for Internal and External Cyberspace Missions.** The nature of C2 relationships for CO vary, depending upon whether they are internal to DODIN or other defended cyberspace, or they are external missions in foreign cyberspace.

(1) **Internal Missions.** C2 of forces conducting DODIN operations and DCO-IDM may require preplanned and preauthorized actions based on particular conditions and triggers, executed either manually or automatically, depending upon the nature of the threat and urgency of the required response. The commander's operations and planning staff should understand the interrelationships of the cyberspace they are protecting, how the appropriate capabilities can be effectively employed to defeat threats, and, when necessary, how to deconflict cyberspace defense actions with the mission critical operations that cannot be interrupted. Cyberspace forces defending CCMD segments of the DODIN may be geographically separated from the supported theater of operations. For example, forces conducting remote actions in support of DCO-IDM often simultaneously support defense of cyberspace in multiple geographic locations. This requires extensive coordination, planning, and early integration of requirements and capabilities. Such cases require all involved commanders to take extra measures so the supported commander is continuously

aware of the remote supporting forces' operational status. In other cases, CPTs may be deployed to specific locations where they are placed in direct support to local commanders to resecure compromised cyberspace. In other cases where there is no local military commander, for instance, when a CPT is deployed to assist a DOD agency, all C2 authorities remain with the CPT's commander. Supported and supporting commanders coordinate the deployment and employment of cyberspace forces required to accomplish the assigned mission.

(2) **External Missions.** C2 relationships established to execute OCO and DCO-RA missions, which involve actions in foreign cyberspace, require careful consideration of projected effects and geopolitical boundaries. The reliance of the global population on the interconnectivity of cyberspace requires carefully controlling the effects created during OCO and DCO-RA missions, with detailed planning, in-depth intelligence support, and national-level deconfliction to assure appropriate consideration of nonmilitary factors such as foreign policy implications. Some of these external missions require centralized execution by CMTs or NMTs to create a global effect. For example, a DCO-RA mission employing external countermeasures in multiple AORs to counter a large botnet (a network of computers linked together by malware) or actions, up to and including pre-emption, to block cyberspace attack command signals directed from one AOR at another. Other external missions may be more regionally and tactically focused and use regionally deployed cyberspace forces. When directed, GCCs control operations in and through cyberspace when there is confidence that effects are limited to their geographic AOR. Such authorities require GCCs to remain cognizant of national cyberspace policy and its application to their plans and operations.

(3) Based on the nature of CO, the cyberspace C2 framework is adjusted for flexible and agile C2 of cyberspace forces to ensure US freedom of action in cyberspace while denying adversaries the same. For additional details beyond those discussed here, refer to the applicable CJCS EXORD and other relevant orders.

f. **Enabling C2 of Cyberspace Forces.** To provide effective C2 of forces conducting CO, several enabling factors are essential.

(1) **COP.** Despite the difficulties of achieving accurate and comprehensive situational awareness of all the aspects of cyberspace relative to a commander, the best available, real-time COP for cyberspace is important for effective C2 of forces executing CO. A COP of activities in cyberspace requires rapid fusion, correlation, and display of data from global network sensors to deliver a reliable picture of friendly, neutral, adversary, and enemy activity in all layers of cyberspace. In addition, an accurate cyberspace COP integrates real-time threat and event data from myriad sources (e.g., DOD enterprise operations centers and other service providers, IC, interagency partners, private industry, and international partners) and improves commanders' ability to identify, monitor, characterize, track, locate, and take action in response to malicious cyberspace activity. CDRUSCYBERCOM maintains global cyberspace situational awareness, and CCMDs maintain regional/functional cyberspace situational awareness along with an awareness of global factors in cyberspace that may impact operations in their theater/functional area.

(2) **Reach-Forward.** The complexity presented by cyberspace requires flexibility of forces and C2 to counter the broad variety of threats. Units of cyberspace forces operating under JFHQ-DODIN and the CNMF-HQ, which provide global CO support, may need to reach-forward to support multiple CCMDs simultaneously. Allowing them to support CCMDs in this way permits faster adaptation to rapidly changing needs and allows threats that initially manifest only in one AOR to be mitigated globally in near real-time. Likewise, while synchronizing CO missions related to accomplishing CCDR objectives, some cyberspace capabilities that support this activity may need to be forward deployed, or for speed in time-critical situations, made available via reachback. This might involve augmentation or deployment of cyberspace capabilities to forces already forward or require deployment of a fully equipped team of personnel and capabilities.

(3) **Reachback.** At the same time, CCMDs require the freedom and capability to effectively plan, coordinate, and conduct theater and functional CO. To enable these efforts, staff supporting GCCs and other CCDRs should arrange for timely and effective reachback support from USCYBERCOM and its subordinate units to augment the expertise and capacity of the supported commander.

(a) CCDRs size and structure their CO support staff to best support their mission and requirements. This staff, supported by a USCYBERCOM CO-IPE, coordinates CO requirements and capabilities throughout their planning, intelligence, operations, assessment, and readiness processes to integrate and synchronize CO with other military operations. Additionally, as necessary and in partnership with USCYBERCOM, the CCMD coordinates regionally with interagency and multinational partners. The CCMD:

1. Combines inputs from USCYBERCOM with information about CCMD tactical and/or constructed networks to develop a regional/functional situational awareness/COP tailored to CCMD requirements.

2. Facilitates, through USCYBERCOM, coordination and deconfliction of CCDR-directed CO which may impact or conflict with other DOD or other USG cyberspace activities or operations within the AOR. As early as possible in the planning process, provide USCYBERCOM with sufficient information about CCDR-planned CO to enable deconfliction with other USG CO.

(b) USCYBERCOM CO-IPEs are organized to meet individual CCMD requirements and facilitate planning and coordination of all three cyberspace missions, as required. USCYBERCOM CO-IPEs remain in direct support of and are integrated with CCMD CO staff to provide a bridge for USCYBERCOM and its subordinate HQ to enable theater/tactical and global/national integration of cyberspace forces and operations.

g. **C2 of Multinational CO.** Although the US military will likely enter future conflicts as part of a multinational force (MNF), the level of integration of US cyberspace forces with foreign cyberspace forces will vary depending upon in-place agreements with each partner and may not mirror the level of integration of other types of forces. Planning for the specific C2 elements desired by the US commander depends upon the type and scale

of the operation, the cyberspace presence or sophistication of the adversary, and the types of targets identified. Regardless of which elements are established, the overlaps between global and theater missions in cyberspace, and relevant operational limitations, necessitate close coordination, and potentially, some level of integration, among CCDRs conducting multinational operations, CDRUSCYBERCOM, and other multinational and interagency partners. See paragraph 9, "Multinational Considerations," for additional information on multinational CO.

6. Synchronization of Cyberspace Operations

a. The pace of CO requires significant pre-operational collaboration and constant vigilance after initiation, for effective coordination and deconfliction throughout the OE. Keys to this synchronization are maintaining cyberspace situational awareness and assessing the potential impacts to the joint force of any planned CO, including the protection posture of the DODIN, changes from normal network configuration, or observed indications of malicious activity. The timing of planned CO should be determined based on a realistic assessment of their ability to create effects and support operations throughout the OE. This may require use of cyberspace capabilities in earlier phases of an operation than the use of other types of capabilities. Effective planners and operators understand how other operations within the OE may impact the CO. For example, the joint force uses fire support coordination measures in air, land, and maritime operations to facilitate the rapid engagement of targets and simultaneously provide safeguards for friendly forces. CO deconfliction and coordination efforts with other operations should include similar measures.

b. **Deconfliction.** For CO, deconfliction is the act of coordinating the employment of cyberspace capabilities to create effects with applicable DOD, interagency, and multinational partners to ensure operations do not interfere, inhibit, or otherwise conflict with each other. The commander's intended effects in cyberspace, and the capabilities planned to create these effects, require deconfliction with other commands and agencies that may have equities in the same area of cyberspace. This critical step is managed from multiple aspects. From a purely technical perspective, it can be shown that two cyberspace capabilities can either interoperate without interference in the same environment or they cannot. However, from an operational risk perspective, even if multiple capabilities can operate without interference, it may not be wise to use them together. For example, the effect of one capability may draw the adversary's attention on the target system in a way that jeopardizes another previously unnoticed US or mission partner capability. Technical deconfliction uses the results of technical assurance evaluations and includes detailed interoperability analysis of each capability and the cyberspace aspects of the OE. CDRUSCYBERCOM is the DOD focal point for interagency deconfliction of all actions proposed for OCO and DCO-RA missions. Commander, JFHQ-DODIN, is the focal point for interagency deconfliction of global DODIN operations and DCO-IDM activities which may affect more than one DOD component. The timelines required for analysis and coordination should be considered and included in the plan. Interagency coordination often takes longer than concomitant DOD coordination. CO may also require deconfliction and synchronization with integrated joint special technical operations (IJSTO). Information

and processes related to IJSTO and its contribution to CO can be obtained from the IJSTO planners at CCMD or Service component HQ.

c. **EMS Factors**

(1) **EMS Dependencies.** Advancements in technology, including an ever-increasing shift to mobile technologies, have created a progressively complex EMS portion of the OE. This has significant implications for CO. The JFC uses joint EMS operations to coordinate elements of CO, space operations, electronic warfare (EW), navigation warfare, various forms of EMS-dependent information collection, and C2. Although these activities can be integrated with other information-related capabilities (IRCs) as part of information operations synchronization, the offensive aspects of CO, space operations, and EW operations are often conducted under different specific authorities. Likewise, some IRCs enabled by CO, such as MISO and MILDEC, have their own execution approval process. Therefore, synchronizing IRCs that use the EMS is a complex process that requires significant foresight and awareness of the various applicable policies. Planners should also maintain awareness of their operational dependencies on mobile devices and wireless networks, including cellular, wireless local area networks, Global Positioning System, and other commercial and military uses of the EMS. Plans that assume access to the EMS for effects in cyberspace should consider contingencies for when bandwidth or interference issues preclude access to the required portion of the EMS.

(2) **Fires in and through the EMS.** Cyberspace attack, EA, and offensive space control (OSC) are deconflicted to maximize the impact of each type of fires. Uncoordinated EA may significantly impact EMS-enabled cyberspace attack actions, and vice-versa. Depending upon power levels, the geographic terrain in which they are used, and the nature of the system being targeted, unintended effects of EA and OSC could also occur outside of a local commander's OA, just as higher-order effects of CO may be possible outside the OA. The JFC and staff may need to comply with different coordination requirements for the various types of fires that depend upon the EMS, forwarding requests for execution as early in the planning process as possible to comply with US law and to facilitate effective and timely effects. To minimize overlap, the primary responsibility for cyberspace attack coordination between USCYBERCOM and the joint force resides with the applicable JFHQ-C and USCYBERCOM CO-IPEs in coordination with the CCMD CO staff. Refer to respective doctrine and policy documents of supported IRCs for specifics on their authorities.

See JP 3-13.1, Electronic Warfare; *JP 3-14,* Space Operations; *and JP 6-01,* Joint Electromagnetic Spectrum Management Operations, *for more information on EMS factors.*

d. **Integration of Cyberspace Fires.** Cyberspace attack capabilities, although they can be used in a stand-alone context, are generally most effective when integrated with other fires. Some examples of integrating cyberspace fires are: disruption of enemy air defense systems using EMS-enabled cyberspace attack, insertion of messages into enemy leadership's communications, degradation/disruption of enemy space-based and ground-based precision navigation and timing systems, and disruption of enemy C2. Effects in cyberspace can be created at the strategic, operational, or tactical level, in any phase of the

military operation, and coordinated with lethal fires to create maximum effect on target. Integrated fires are not necessarily simultaneous fires, since the timing of cyberspace attack effects may be most advantageous when placed before or after the effects of lethal fires. Each engagement presents unique considerations, depending upon the level and nature of the enemy's dependencies upon cyberspace. Supporting cyberspace fires may be used in a minor role, or they can be a critical component of a mission when used to enable air, land, maritime, space, and special operations. Forces operating lethal weapons and other capabilities in the physical domains cannot use cyberspace fires to best advantage unless they clearly understand the type and timing of planned effects in cyberspace. Properly prepared and timed cyberspace fires can create effects that cannot be created any other way. Poorly timed fires in cyberspace can be useless, or even worse, interfere with an otherwise effective mission.

e. **Risk Concerns.** JFCs should continuously seek to minimize risks to the joint force, as well as to friendly and neutral nations, societies, and economies, caused by use of cyberspace. Coordinated joint force operations benefit from the use of various cyberspace capabilities, including unclassified Web sites and Web applications used for communication efforts with audiences internal and external to DOD. Forward-deployed forces use the Internet, mobile phones, and instant messaging for logistics and morale purposes, including communication with friends and family. These uses of cyberspace are targeted by myriad actors, from foreign nations to malicious insiders. The JFC works with JFHQ-DODIN and the Services, as well as with assigned cyberspace forces, to limit the threat to the DODIN and mission partners' cyberspace. Several areas of significant risk exist for the JFC:

(1) **Insider threats** are a significant concern to the joint force. Because insiders have a trusted relationship with access to the DODIN, the effects of their malicious or careless activity can be far more serious than those of external threat actors. Any user who does not closely follow cybersecurity policy can become an insider threat. Malicious insiders may exploit their access at the behest of foreign governments, terrorist groups, criminal elements, unscrupulous associates, or on their own initiative. Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DOD and national security can be devastating. JFCs use risk mitigation measures for this threat, such as reinforcing training of the joint force to be alert for suspicious insider activity and use of two-person controls on particularly sensitive hardware, software, or data.

(2) **Internet-based capabilities,** including e-mail, social networking, Web sites, and cloud-based repositories, are used for both official and unofficial purposes and pose continuously evolving security risks that are not fully understood. The security risks of Internet-based capabilities are often obscured, and our ability to mitigate these risks is limited, due to the commercial ownership of the majority of the supporting information systems or sites. These cyberspace and information security concerns, combined with bandwidth requirements of Internet applications, create an imperative for the commander to be aware of and actively manage the impact of official and unofficial use of Internet-based capabilities.

(3) **Cross-domain (network) solutions** that connect systems operating at different classification levels can provide significant operational value to the JFC but complicate cryptographic and other security support considerations and should be included as a planning consideration. Cross-domain solutions are often required in multinational operations and at the tactical level. The pace of operations and increasing demand for information from commanders and their staffs can sometimes pressure end-users into using poor security practices. Likewise, emergent tasking for information sharing has sometimes caused network managers to build ad hoc links over existing commercial infrastructure or connect non-DOD US and partner cyberspace without adequate security controls. The security risk of these behaviors is significant. USCYBERCOM, through JFHQ-DODIN, works with JFCs to develop appropriate technical solutions and detailed security policies to address the operational requirements without adding unnecessary risk. Planners should include requirements for early coordination so the security features included are appropriate for the commander's needs.

7. Assessment of Cyberspace Operations

a. Assessment measures progress of the joint force toward mission accomplishment. Commanders continuously assess the OE and the progress of CO and compare them to their vision and intent. Measuring this progress toward the end state, and delivering timely, relevant, and reliable feedback into the planning process to adjust operations during execution, involves deliberately comparing the forecasted effects of CO with actual outcomes to determine the overall effectiveness of cyberspace force employment. More specifically, assessment helps the commander determine progress toward attaining the desired end state, achieving objectives, or performing tasks.

b. The assessment process for external CO missions begins during planning and includes measures of performance (MOPs) and measures of effectiveness (MOEs) of fires and other effects in cyberspace, as well as their contribution to the larger operation or objective. Historically, combat assessment has emphasized the battle damage assessment (BDA) component of measuring physical and functional damage, but this approach does not always represent the most complete effect, particularly with respect to CO. CO effects are often created outside the scope of battle and often do not create physical damage. Assessing the impact of CO effects requires typical BDA analysis and assessment of physical, functional, and target system components. However, the higher-order effects of cyberspace actions are often subtle, and assessment of second- and third-order effects can be difficult. Therefore, assessment of fires in and through cyberspace frequently requires significant intelligence collection and analysis efforts. Incorporating pre-strike prediction and post-strike assessment for CO into the existing joint force staff processes increases the likelihood that all objectives are met.

c. Assessment of CO at the Operational Level

(1) The operational-level planner is concerned with the accumulation of tactical effects into an overall operational effect. At the operational level, planning and operations staffs develop objectives and desired effects for the JFC to assign to subordinates. Subordinate staffs use the assigned operational objectives to develop tactical-level

objectives, tasks, and subordinate targeting objectives and effects and to plan tactical actions and MOPs/MOEs for those actions. Individual tactical actions typically combine with other tactical actions to create operational-level effects; however, they can have operational or strategic implications. Usually, the summation of tactical actions in an operational theater is used to conduct an operational-level assessment principally operation assessments (see JP 3-0, *Joint Operations,* and JP 5-0, *Joint Planning*), which in turn supports the strategic-level assessment (as required). Operational MOPs/MOEs avoid tactical information overload by providing commanders a shorthand method of tracking tactical actions and maintaining situational awareness. MOPs and MOEs are clearly definable and measurable, are selected to support and enhance the commander's decision process, and guide future actions that achieve objectives and attain end states.

(a) **MOEs.** MOEs are used to assess changes in targeted system behavior or in the OE. They measure progress toward the attainment of an end state, achievement of an objective, or creation of an effect. Data gathered on the target from its pre-mission state through access, execution, and possibly long-term post-operations analysis may enable later, more comprehensive assessment, including that of higher-order effects. MOEs generally reflect a trend or show progress toward or away from a measurable threshold. While MOEs may be harder to derive than MOP for a discrete task, they are nonetheless essential to effective assessment. For example, a MOE for a cyberspace attack action might be a meaningful reduction in the throughput of enemy data traffic or their shift to a more interceptable means of communication. Assessment of CO takes place both inside and outside of cyberspace. For instance, an OCO mission to disrupt electric power might be assessed through visual observation to determine that the power is actually out.

(b) **MOP.** MOPs are criteria for measuring task performance or accomplishment. MOPs are generally quantitative and are used in most aspects of combat assessment, which typically seeks specific quantitative data or a direct observation of an event to determine accomplishment of tactical tasks. An example of a MOP for a cyberspace exploitation action might be gaining a required access or emplacing a cyberspace capability on a targeted system.

(2) Development of operational-level MOPs/MOEs for CO is still an emerging aspect of operational art. In some cases, activities in cyberspace alone have operational-level effects; for example, the use of a cyberspace attack to bring down or corrupt the enemy HQ network could very well reverberate through the entire JOA. A CO option may be preferable in some scenarios if its effects are temporary or reversible. In such cases, accurate assessment requires the ability to effectively track the current status of the potentially changing effect using MOE indicators.

(3) CO often involve multiple commanders. Additionally, with CO typically conducted as part of a larger operation, assessment of CO is usually done in the context of supporting the overarching objectives. Therefore, CO assessments require close coordination within each staff and across multiple commands. Coordination and federation of the assessment efforts may require prior arrangements before execution. CO planners submit assessment requests as early as possible and provide sufficient justification to support priority allocation of relevant collection capabilities, including those outside of cyberspace.

See JP 5-0, Joint Planning, *for a detailed description of assessment. See JP 3-60,* Joint Targeting, *and Defense Intelligence Agency Publication 2820-4-03,* Battle Damage Assessment (BDA) Quick Guide, *for more information on the assessment process related to targeting, BDA, and munitions effectiveness assessment.*

8. Interorganizational Considerations

a. When appropriate, JFCs coordinate and integrate their CO with interagency partners during planning and execution. Effective integration of interagency considerations is vital to successful military operations, especially when the joint force conducts shaping, stability, and transition to civil authority activities. Just as JFCs and their staffs consider how the capabilities of other USG components and NGOs can be leveraged to assist in accomplishing military missions and broader national strategic objectives, JFCs should also consider the capabilities and priorities of interagency partners in planning and executing CO. In collaboration with interagency representatives, JS, and USCYBERCOM, JFCs should coordinate with interagency partners during CO planning to help ensure appropriate agreements exist to support their plans.

b. At the national level, the National Security Council, with its policy coordination committees and interagency working groups, advises and assists the President on all aspects of national security policy. OSD and JS, in consultation with the Services and CCMDs, coordinate interagency support required to support the JFC's plans and orders. While supported CCDRs are the focal points for interagency coordination in support of operations in their AORs, interagency coordination with supporting commanders is also important. For integration into their operational-level estimates, plans, and operations, commanders should only consider interagency capabilities and capacities that interagency partners can realistically commit to the effort.

c. Military leaders work with the other members of the national security team to promote unified action. A number of factors can complicate the coordination process, including various agencies' different and sometimes conflicting policies, overlapping legal authorities, roles and responsibilities, procedures, and decision-making processes for CO. A supported commander develops interagency coordination requirements and mechanisms for each OPLAN. The JFC's staff requires a clear understanding of military CO capabilities, requirements, operational limitations, liaison, and legal considerations. Additionally, planners should understand the nature of this relationship and the types of CO support interagency partners can provide. In the absence of a formal interagency command structure, JFCs are required to build consensus to achieve unity of effort. Robust liaison facilitates understanding, coordination, and mission accomplishment.

d. Interagency command relationships, lines of authority, and planning processes vary greatly from those of DOD. Interagency management techniques often involve committees, steering groups, and/or interagency working groups organized along functional lines. During joint operations, use of a JIACG provides the CCDR and subordinate JFCs with an increased capability to coordinate with other USG departments and agencies. The JIACG is composed of USG civilian and military experts tailored to meet the CCDR's specific needs and accredited to the CCDR. The JIACG establishes regular, timely, and collaborative working

relationships between civilian and military planners, providing a CCDR with the capability to collaborate at the operational level with other USG departments and agencies. JIACG members participate in all appropriate planning efforts. Additionally, they provide a collaborative conduit back to their parent organizations to help synchronize joint operations with the efforts of nonmilitary organizations. In the absence of a JIACG focused on CO, planners may find it more difficult to verify that all mission partner equities in cyberspace are accounted for and, therefore, should begin to develop contacts with relevant departments and agencies as soon as the planning process begins.

9. Multinational Considerations

a. Collective security is a strategic objective of the US, and joint planning is frequently accomplished within the context of planning for multinational operations. There is no single doctrine for multinational action, and each alliance or coalition develops its own protocols and plans. US planning for joint operations accommodates and complements such protocols and plans for potential use of US cyberspace forces to protect MNF networks. JFCs also anticipate and incorporate mission partner planning factors, such as their domestic laws, regulations, and operational limitations on the use of various cyberspace capabilities and tactics.

b. When working within an MNF, each nation and Service can expect to be tasked by the commander with the mission(s) most suited to their particular capability and capacity. For example, a CPT supporting a CCMD could be tasked, with the agreement of all nations involved, to investigate and mitigate the effects of malicious cyberspace activity on a multinational network. CO planning, coordination, and execution items that require consideration when an MNF operation or campaign plan is developed include:

(1) National agendas of the PNs on an MNF may differ significantly from those of the US, creating potential difficulties in determining the CO objectives.

(2) Differing national standards and foreign laws, as well as interpretation of international laws pertaining to operations in cyberspace, may affect their ability to participate in certain CO. These differences may result in partner policies or capabilities that are either narrower or broader than those of the US.

(3) Nations without established CO doctrine may need to be advised of the potential benefits of CO and assisted in integrating CO into the planning process.

(4) Nations in an MNF often require approval for the CO portion of plans and orders from higher authority, which may impede CO implementation. This national-level approval requirement increases potential constraints and restraints upon the participating national forces and further lengthens the time required to gain approval for their participation. Commanders and planners should be proactive in seeking to understand PNs' laws, policies, and other matters that might affect their use of CO and anticipate the additional time required for approval through parallel national command structures. Partners' national caveats and ROE are often not transmitted thoroughly to commanders and planners, potentially leading to misunderstanding, delays, and incompleteness in execution.

(5) Security restrictions may prevent full disclosure of individual CO plans and orders between multinational partners; this may complicate cyberspace synchronization efforts. Therefore, the JFC's staff should seek approval for sharing required information among partners and then issue specific guidance on the release of classified US material to the MNF as early as possible during planning. Likewise, once these information-sharing restrictions are identified by each nation, policy should be established and mechanisms put in place to encourage appropriate CO-related information sharing across the force. These considerations further highlight the importance of ensuring CO material is not over classified and is releasable to partners to the greatest extent possible.

(6) To effectively conduct multinational operations, mission partners require appropriate access to systems, services, and information. Emerging standards for the technologies and applications applied to DODIN segments used in a joint environment are designed to allow seamless and secure interaction with multinational partners. Until such technology is widespread, the US joint force strives to provide necessary and appropriate access and support at the lowest appropriate security classification level on the infrastructure they have available. Commanders involved in multinational operations can enable this shared access by coordinating with proper authorities early to determine appropriate access levels, necessary services, and satisfactory means for expediting the process for foreign disclosure of appropriate intelligence information consistent with National Disclosure Policy, and Director of National Intelligence guidance, as applicable. Hardware and software incompatibilities can still be expected and may cause a slowdown in the sharing of information among multinational partners. Failure to bridge these incompatibilities may introduce seams, gaps, and vulnerabilities requiring additional cyberspace security and defense efforts.

(7) Responsibility for cyberspace security and cyberspace defense actions to protect multinational networks should be made clear before the network is activated. If responsibility for these actions is to be shared amongst PNs, explicit agreements, including expectations and limitation of action of each partner, should be in place. Unless otherwise agreed, US cyberspace forces or other DOD personnel protect DODIN segments of multinational networks.

c. **Integration.** In support of each MNF, an established hierarchy of bilateral or multilateral bodies defines objectives, develop strategies, and coordinates strategic guidance for planning and executing multinational operations, including CO. Through dual involvement in national and multinational security processes, USG leaders integrate national and theater strategic CO planning with the MNF whenever possible. Within the multinational structure, US participants work to ensure objectives and strategy complement US interests and are compatible with US capabilities. Within the US national structure, US participants verify international commitments are reflected in national military strategy and are adequately addressed in strategic guidance for joint planning. Planning with international organizations and NGOs is often necessary, particularly if CO support foreign humanitarian assistance, peace operations, and other stability efforts. Incorporating NGOs and their capabilities into the planning process requires the JFC and staff to balance NGOs' information requirements with the organization's need to know. Additionally, many NGOs are hesitant to become associated with military organizations in any form of formal

relationship, especially in the case of conducting CO, because doing so could compromise their status as an independent entity, restrict their freedom of movement, and even place their members at risk in uncertain or hostile environments.

d. Multinational partners often use a different lexicon, assumptions, decision thresholds, and operational limitations pertaining to CO. All of these factors affect coordination, integration, and execution and should be taken into consideration during planning.

See JP 3-16, Multinational Operations, *for more information on multinational operations.*

APPENDIX A
(U) CLASSIFIED PLANNING CONSIDERATIONS FOR CYBERSPACE OPERATIONS

(PUBLISHED SEPARATELY)

Intentionally Blank

APPENDIX B
CYBERSPACE OPERATIONS POINTS OF CONTACT

Joint Staff/J7/Doctrine Division

Web Site:	http://www.jcs.mil/doctrine/
Email Support:	js.pentagon.j7.jedd-support@mail.mil
Phone number:	1-703-692-7276 (DSN 222)

Joint Staff Doctrine Sponsor/J39

Comm:	1-703-571-1899

United States Cyber Command (USCYBERCOM)

Mailing Address:	US Cyber Command / J5 9800 Savage Road, Suite 6171 Fort George G. Meade, MD 20755
Comm:	1-443-654-2213 (DSN 840-2213)

USCYBERCOM Watch Center: 1-443-654-3951

Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN)

Mailing Address:	Joint Force Headquarters-DODIN 6910 Cooper Ave Fort George G. Meade, MD 20755

DODIN Watch Center: 1-301-225-0720/0721

Intentionally Blank

APPENDIX C
REFERENCES

The development of JP 3-12 is based upon the following primary references:

1. General

a. Title 10, USC.

b. Title 32, USC.

c. Title 50, USC.

d. *Goldwater-Nichols Department of Defense Reorganization Act of 1986.*

e. Executive Order 12333, *US Intelligence Activities.*

f. Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*

g. Homeland Security Presidential Directive-5, *Management of Domestic Incidents.*

h. PPD-20, *US Cyber Operations Policy.*

i. PPD-21, *Critical Infrastructure Security and Resilience.*

j. PPD-41, *United States Cyber Incident Coordination.*

k. *International Strategy for Cyberspace.*

l. *Trilateral Memorandum of Agreement Among the Department of Defense and the Department of Justice and the Intelligence Community Regarding Computer Network Attack and Computer Network Exploitation Activities,* 9 May 2007.

m. *National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments.*

n. *National Security Presidential Directive 54/Homeland Security Presidential Directive 23.*

o. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems.*

p. *Memorandum of Agreement Between The Department of Defense and The Department of Homeland Security Regarding Department of Defense and US Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, 27 September 2010.*

2. Department of Defense Publications

a. *Unified Command Plan.*

b. *National Military Strategy.*

c. *The Department of Defense Cyber Strategy.*

d. *Department of Defense Strategy for Operating in the Information Environment.*

e. Deputy Secretary of Defense Memorandum, *Policy for Department of Defense (DOD) Interactive Internet Activities, June 8, 2007.*

f. *National Infrastructure Protection Plan.*

g. *Defense Strategic Guidance.*

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

i. DODD 3025.18, *Defense Support of Civil Authorities (DSCA)*

j. DODD 3600.01, *Information Operations (IO).*

k. DODD 5143.01, *Under Secretary of Defense for Intelligence (USD(I))*.

l. DODD 5205.15E, *DOD Forensic Enterprise (DFE).*

m. DODD 5505.13E, *DOD Executive Agent (EA) for the DOD Cyber Crime Center (DC3).*

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

o. DODI O-3600.03, *Technical Assurance Standard (TAS) for Computer Network Attack (CNA) Capabilities.*

p. DODI 3607.02, *Military Information Support Operations*

q. DODI 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities.*

r. DODI 8500.01, *Cybersecurity.*

s. DODI 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations.*

t. DODI 8560.01, *Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing.*

u. *Department of Defense Law of War Manual.*

v. Defense Intelligence Agency Publication 2820-4-03, *Battle Damage Assessment (BDA) Quick Guide*.

3. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 3121.01B, *(U) Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces.*

b. CJCSI 3210.01C, *Joint Information Operations Proponent.*

c. CJCSI 3370.01B, *Target Development Standards.*

d. CJCSI 5810.01D, *Implementation of the DOD Law of War Program.*

e. CJCSM 3122.07A, *Integrated Joint Special Technical Operations (IJSTO) Supplement to Joint Operation Planning and Execution System (JOPES), Volume I (Planning and Procedures).*

f. CJCSM 3122.08A, *(U) IJSTO Supplement to Joint Operation Planning and Execution System (Volume II) Planning Formats and Guidance.*

g. CJCSM 3139.01, *(U) Review and Approval Process for Cyberspace Operations.*

h. CJCSM 3314.01A, *Intelligence Planning.*

i. CJCS 011612Z February 2016, *EXORD to Implement Updated Cyberspace Operations Command and Control Framework.*

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

k. JP 1-04, *Legal Support to Military Operations.*

l. JP 2-0, *Joint Intelligence.*

m. JP 2-01, *Joint and National Intelligence Support to Military Operations.*

n. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment.*

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

p. JP 3-07, *Stability.*

q. JP 3-08, *Interorganizational Cooperation.*

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

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

t. JP 3-13.2, *Military Information Support Operations.*

u. JP 3-13.3, *Operations Security.*

v. JP 3-13.4, *Military Deception.*

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

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

y. JP 3-27, *Homeland Defense.*

z. JP 3-28, *Defense Support of Civil Authorities.*

aa. JP 3-60, *Joint Targeting.*

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

cc. JP 6-0, *Joint Communications System.*

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

APPENDIX D
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

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

2. Authorship

a. The lead agent for this publication is USCYBERCOM, and the JS doctrine sponsor for this publication is the Director for Global Operations (J-39).

b. The following staff, in conjunction with the Joint Doctrine Development Community, made a valuable contribution to the revision of this Joint Publication: Lead Agent Mr. Paul Schuh, USCYBERCOM; Joint Staff Doctrine Sponsor CDR Holly Yudisky, Joint Staff J-39; Mr. Mark Brown, Joint Staff J-7, Joint Doctrine Analysis Division; and MAJ Josh Darling, Joint Staff J-7, Joint Doctrine Division.

3. Supersession

This publication supersedes JP 3-12, *Cyberspace Operations,* 05 February 2013.

4. Change Recommendations

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

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

5. Lessons Learned

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

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

6. Distribution of Publications

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

7. Distribution of Electronic Publications

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

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

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

GLOSSARY

PART I—ABBREVIATIONS, ACRONYMS, AND INITIALISMS

AOR	area of responsibility
BDA	battle damage assessment
C2	command and control
CCDR	combatant commander
CCMD	combatant command
CCMF	Cyber Combat Mission Force
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CI	counterintelligence
CI/KR	critical infrastructure and key resources
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
CMF	Cyber Mission Force
CMT	combat mission team
CNMF	Cyber National Mission Force
CNMF-HQ	Cyber National Mission Force Headquarters
CO	cyberspace operations
COCOM	combatant command (command authority)
CO-IPE	cyberspace operations-integrated planning element
CONOPS	concept of operations
CONPLAN	concept plan
COP	common operational picture
CPF	Cyber Protection Force
CPT	cyberspace protection team
CSA	combat support agency
CSSP	cybersecurity service provider
CST	combat support team
DACO	directive authority for cyberspace operations
DC3	Department of Defense Cyber Crime Center
DCI	defense critical infrastructure
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations-internal defensive measures
DCO-RA	defensive cyberspace operations-response actions
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	defense industrial base
DISA	Defense Information Systems Agency

DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODIN	Department of Defense information network
DOJ	Department of Justice
DSCA	defense support of civil authorities
EA	electronic attack
EMS	electromagnetic spectrum
EW	electronic warfare
EXORD	execute order
FBI	Federal Bureau of Investigation (DOJ)
GCC	geographic combatant commander
GFMIG	Global Force Management Implementation Guidance
HQ	headquarters
IAW	in accordance with
IC	intelligence community
IGL	intelligence gain/loss
IJSTO	integrated joint special technical operations
IP	Internet protocol
IR	intelligence requirement
IRC	information-related capability
ISP	Internet service provider
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
JFC	joint force commander
JFHQ-C	joint force headquarters-cyberspace
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network
JIACG	joint interagency coordination group
JOA	joint operations area
JP	joint publication
JPP	joint planning process
JS	Joint Staff
JTL	joint target list
LE	law enforcement
LOC	line of communications
MILDEC	military deception
MISO	military information support operations

MNF	multinational force
MOE	measure of effectiveness
MOP	measure of performance
MTFP	mission-tailored force package
NG	National Guard
NGB	National Guard Bureau
NGO	nongovernmental organization
NIPRNET	Non-classified Internet Protocol Router Network
NMT	national mission team
NST	national support team
OA	operational area
OCO	offensive cyberspace operations
OE	operational environment
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSC	offensive space control
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
PIT	platform information technology
PN	partner nation
PPD	Presidential policy directive
RC	Reserve Component
RFI	request for information
ROE	rules of engagement
SATCOM	satellite communications
SCC	Service cyberspace component
SecDef	Secretary of Defense
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
TACON	tactical control
TCPED	tasking, collection, processing, exploitation, and dissemination
TST	time-sensitive target
USC	United States Code
USCYBERCOM	United States Cyber Command
USD(P)	Under Secretary of Defense for Policy
USG	United States Government

PART II—TERMS AND DEFINITIONS

cyberspace. A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (DOD Dictionary. Source: JP 3-12)

cyberspace attack. Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain, and is considered a form of fires. (Approved for inclusion in the DOD Dictionary.)

cyberspace capability. A device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. (Approved for inclusion in the DOD Dictionary.)

cyberspace defense. Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. (Approved for inclusion in the DOD Dictionary.)

cyberspace exploitation. Actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations. (Approved for inclusion in the DOD Dictionary.)

cyberspace security. Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (Approved for inclusion in the DOD Dictionary.)

cyberspace superiority. The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force and its related land, air, maritime, and space forces at a given time and place without prohibitive interference. (Approved for incorporation into the DOD Dictionary.)

defensive cyberspace operations. Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. Also called **DCO.** (Approved for incorporation into the DOD Dictionary.)

defensive cyberspace operations-internal defensive measures. Operations in which authorized defense actions occur within the defended portion of cyberspace. Also called **DCO-IDM.** (Approved for inclusion in the DOD Dictionary.)

defensive cyberspace operations-response actions. Operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. Also called **DCO-RA.** (Approved for replacement of "defensive cyberspace operation response action" and its definition in the DOD Dictionary.)

Department of Defense information network operations. Operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network. Also called **DODIN operations.** (Approved for incorporation into the DOD Dictionary.)

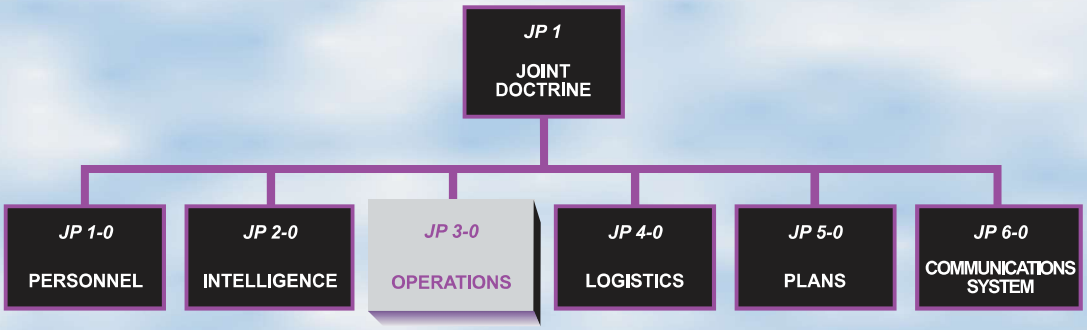
directive authority for cyberspace operations. The authority to issue orders and directives to all Department of Defense components to execute global Department of Defense information network operations and defensive cyberspace operations internal defensive measures. Also called **DACO.** (Approved for inclusion in the DOD Dictionary.)

information assurance. None. (Approved for removal from the DOD Dictionary.)

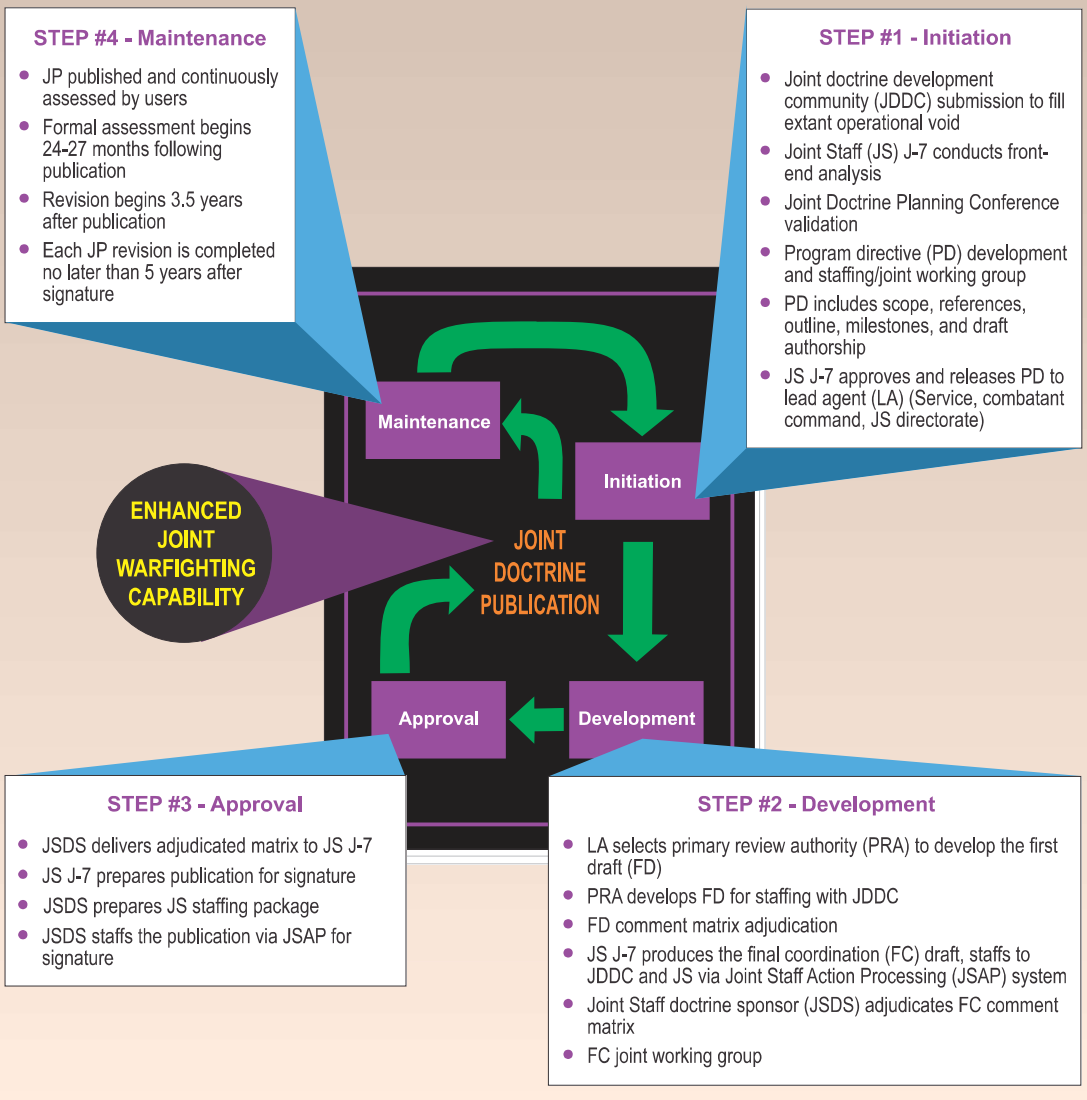
offensive cyberspace operations. Missions intended to project power in and through cyberspace. Also called **OCO.** (Approved for incorporation into the DOD Dictionary.)

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-12** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:




JOINT
CHIEFS OF STAFF