Joint Publication 3-12 (R)

Cyberspace Operations

5 February 2013

PREFACE

1. Scope

This publication provides joint doctrine for the planning, preparation, execution, and assessment of joint cyberspace operations across the range of military operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and 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, and the Services.

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 Chairman of the Joint Chiefs of Staff, 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 US. 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:

CURTIS M. SCAPARROTTI
Lieutenant General, U.S. Army
Director, Joint Staff

Intentionally Blank

TABLE OF CONTENTS

PAGE

GLOSSARY

FIGURE

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Introduces cyberspace and its integration into joint operations.**
- **Explains cyberspace operations and their relationship to joint functions.**
- **Covers authorities, roles, and responsibilities.**
- **Discusses planning and coordination of cyberspace operations.**

Introduction

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

Most aspects of joint operations rely in part on cyberspace, the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Developments in cyberspace provide the means for the US military, its allies, and partner nations to gain and maintain a strategic, continuing advantage in the operational environment (OE), and can be leveraged to ensure the nation's economic and physical security. Access to the Internet provides adversaries the capability to compromise the integrity of US critical infrastructures in direct and indirect ways. These characteristics and conditions present a paradox within cyberspace: the prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace, for the US in general and the joint force in particular.

Cyberspace

Cyberspace, while a global domain within the information environment, is one of five interdependent domains, the others being the physical domains of air, land, maritime, and space.

Cyberspace consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an Internet protocol address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them. Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona. The **physical network** layer of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel. The **logical network** layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node. A simple example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator. The **cyber-persona** layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network.

Integrating CO

While it is possible that some military objectives can be achieved by CO alone, CO capabilities should be considered during joint operation planning, integrated into the joint force commander's plan, and synchronized with other operations during execution.

Commanders conduct cyberspace operations (CO) to retain freedom of maneuver in cyberspace, accomplish the joint force commander's (JFC's) objectives, deny freedom of action to adversaries, and enable other operational activities. Conflicts that may need to be addressed to fully integrate CO into joint operation planning and execution include: centralized CO planning for Department of Defense information network (DODIN) operations and defense; the JFC's need to synchronize operations and fires, including CO; deconfliction requirements between government entities; partner nation relationships; and the relationships between CO and information operations, between CO and operations conducted in the physical domains, and the wide variety of legal issues that relate to CO.

The Joint Force and Cyberspace

The JFC faces a unique set of challenges while executing CO in a complex global security environment. CO are enabled by the DODIN. The DODIN is a global infrastructure of Department of Defense (DOD) systems carrying DOD, national security, and related intelligence community information and intelligence. Cyberspace presents the JFC with many threats ranging from nation states to individual actors. Perhaps the most challenging aspect of attributing actions in cyberspace is connecting a cyberspace actor (cyber-persona) or action to an actual individual, group, or state actor, with sufficient confidence and verifiability to hold them accountable. CO may not require physical proximity; many CO can be executed remotely. Moreover, the effects of CO may extend beyond a target, a joint operations area, or even an area of responsibility (AOR).

Cyberspace Operations

Introduction

CO are composed of the military, intelligence, and ordinary business operations of DOD in and through cyberspace. The military component of CO, which is the only component guided by joint doctrine, is the primary focus of this publication. CO enhance operational effectiveness and leverage various capabilities from physical domains to create effects, which may span multiple geographic combatant commanders' (GCCs') AORs.

Military Operations In and Through Cyberspace

The successful execution of CO requires the integrated and synchronized employment of offensive, defensive, and DODIN operations, underpinned by effective and timely operational preparation of the environment. **CO missions are categorized as offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DODIN based on their intent. OCO** are CO intended to project power by the application of force in and through cyberspace. **DCO** are CO intended to defend DOD or other friendly cyberspace. **DODIN operations** are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation.

National Intelligence Operations In and Through Cyberspace

National level intelligence organizations, including major DOD agencies, conduct intelligence activities for 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 those non-warfighting capabilities and functions used to support and sustain DOD forces in their normal day-to-day functions, but that are not normally under the control of a JFC. This includes the CO of the civilian-run DOD agencies, such as the Defense Finance and Accounting Service and the Defense Commissary Agency. These organizations conduct routine uses of cyberspace, as well as DODIN operations and some internal defensive measures.

The Joint Functions and CO

Joint Publication 3-0, *Joint Operations*, delineates joint functions common to joint operations at all levels of war into six basic groups: command and control (C2), intelligence, fires, movement and maneuver, protection, and sustainment.

Command and Control

C2 of operations in and through cyberspace encompasses the exercise of authority and direction by commanders over assigned and attached forces in the accomplishment of their mission.

Intelligence

Intelligence collected in cyberspace may come from DOD and/or national-level sources and may serve strategic, operational, or tactical requirements.

Fires

Depending on the objective, cyberspace fires can be offensive or defensive, supporting or supported. Like all forms of power projection, fires in and through cyberspace should be included in the joint planning and execution processes from inception in order to facilitate synchronization and unity of effort.

Movement and Maneuver

A significant factor in maneuverability in cyberspace is access to the target node. Movement and maneuver in cyberspace can occur in all three layers: the physical network, logical network, and the cyber-persona layer.

Sustainment

JFCs must identify required forces and capabilities, critical cyberspace assets, assess risk, ensure redundancy (including non-cyberspace alternatives), and actively exercise continuity of operations plans to respond to outages or adversary actions that degrade or compromise cyberspace access or reliability.

Protection

Cyberspace capabilities requiring protection include not only the infrastructure (computers, cables, antennas, and switching and routing equipment), as well as parts of the EMS (e.g., datalink frequencies to include satellite downlink, cellular, and wireless), and the content (both data and applications) on which military operations rely.

Authorities, Roles, and Responsibilities

Introduction

Under the authorities of the Secretary of Defense (SecDef), DOD uses cyberspace capabilities to shape cyberspace and provide integrated offensive and defensive options. As directed by United States Strategic Command (USSTRATCOM), United States Cyber

Command (USCYBERCOM) synchronizes and directs transregional operations and, in coordination with combatant commands (CCMDs), Joint Staff (JS), and Office of Secretary of Defense, liaises with other United States Government (USG) departments and agencies, and members of the defense industrial base in conjunction with the Department of Homeland Security. Similarly, as directed, DOD will deploy necessary resources to support efforts of other USG departments and agencies.

Authorities

Authority for actions undertaken by the Armed Forces of the United States is derived from the US Constitution and Federal law. These authorities establish roles and responsibilities that provide focus for organizations to develop capabilities and expertise, including those for cyberspace.

Roles and Responsibilities

SecDef directs the military, intelligence, and ordinary business operations of DOD in cyberspace; and, provides policy guidance and authority for employment of assigned, attached, and supporting military forces conducting cyberspace missions.

Chairman of the Joint Chiefs of Staff (CJCS) ensures that cyberspace plans and operations are compatible with other military plans.

Service Chiefs [Services] will provide CO capabilities for deployment/support to CCMDs as directed by SecDef; and, remain responsible for compliance with USSTRATCOM’s direction for operation and defense of the DODIN.

Commander, United States Strategic Command (CDRUSSTRATCOM), has overall responsibility for DODIN operations and defense in coordination with CJCS, the Service Chiefs, and CCDRs. CDRUSSTRATCOM is responsible for CO to secure, operate, and defend the DODIN, and to defend US critical cyberspace assets, systems, and functions as directed by the President or SecDef, against any intrusion or attack, and does so through a subunified command, USCYBERCOM.

Other Combatant Commanders operate and defend tactical and constructed networks within their commands; and, integrate CO capabilities into all military operations;

integrate CO into plans (concept plans and operation plans [OPLANs]); and work closely with the joint force, USSTRATCOM/USCYBERCOM, Service components, and DOD agencies to create fully integrated capabilities.

Legal Considerations

The legal framework applicable to CO depends on the nature of the activities to be conducted, such as offensive or defensive military operations; defense support of civil authorities; service provider actions; law enforcement and counterintelligence activities; intelligence operations; and defense of the homeland. Before conducting CO, commanders, planners, and operators must understand the relevant legal framework in order to comply with laws and policies, the application of which may be challenging given the ubiquitous nature of cyberspace and the often geographic orientation of domestic and international law.

Planning and Coordination

Joint Operation Planning Process and CO

Commanders integrate cyberspace capabilities at all levels and in all military operations. Plans should address how to effectively integrate cyberspace capabilities, counter an adversary's use of cyberspace, secure mission critical networks, operate in a degraded environment, efficiently use limited cyberspace assets, and consolidate operational requirements for cyberspace capabilities.

CO Planning Considerations

CO planners are presented the same considerations and challenges that are present in planning for other joint capabilities and functions, as well as some unique considerations. Targeting, deconfliction, commander's intent, political/military assessment, and collateral effects considerations all play into the calculations of the CO planner's efforts. CO planning considerations include: cyberspace-related intelligence requirements, targeting, and DODIN operations.

Command and Control of CO

Clearly established command relationships are crucial for ensuring timely and effective employment of forces. As authorized by CDRUSSTRATCOM, Commander, United States Cyber Command (CDRUSCYBERCOM) manages day-to-day global CO. Typically, CO require coordination between theater and global operations, creating a dynamic C2 environment. CO are integrated and synchronized by the supported commander into their concept of operations, detailed plans and orders, and specific joint offensive and defensive operations. The GCC is generally the supported commander for CO with first order effects within their AOR. Similarly, CDRUSSTRATCOM/ CDRUSCYBERCOM is generally the supported commander at the global or transregional (across AOR boundaries) level. C2 of DODIN operations and DCO may require pre-determined and preauthorized actions based on meeting particular conditions and triggers, executed either manually or automatically if the nature of the threat requires instantaneous response.

Synchronization of CO

The pace of CO requires significant pre-operational collaboration, as well as constant vigilance upon initiation, to ensure that activities in cyberspace and throughout the OE are coordinated and deconflicted in advance.

Assessment of CO

Assessments in cyberspace may be unique in that the normal assessment cell will not typically have the capabilities or expertise to assess CO; CO will typically involve multiple commands, such as the supported JFC, CDRUSCYBERCOM, and possibly other functional supporting JFCs. Additionally, with CO typically being conducted as part of a larger operation, assessment of CO will need to be conducted in the context of supporting the overarching JFC objectives.

Interorganizational Considerations

Just as JFCs and their staffs must consider how the capabilities of other USG and nongovernmental organizations 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. Through JS and USCYBERCOM, JFCs should coordinate with interagency representatives during planning to ensure appropriate agreements exist to support their plans.

Multinational Considerations

CO planning, coordination, and execution items that must be considered when a multinational force campaign or OPLAN is developed include:

Through dual involvement in national and multinational security processes, US national

- National agendas for each country of the multinational force may differ significantly from those of the US, creating potential difficulties in

leaders integrate national and theater strategic CO planning with that of the multinational force whenever possible.

determining the CO objectives.

- Differing national standards and laws pertaining to sovereignty in cyberspace may affect willingness or the legality of their participation in certain CO.

- Security restrictions may prevent full disclosure of individual CO plans and orders with multinational partners; this may severely hamper cyberspace synchronization efforts.

CONCLUSION

This publication provides joint doctrine for the planning, preparation, execution, and assessment of joint CO across the range of military operations.

CHAPTER I
INTRODUCTION

> *"Cyberspace and its associated technologies offer unprecedented opportunities to the US and are vital to our Nation's security, and by extension, to all aspects of military operations."*
>
> **Secretary of Defense Robert Gates, 2011**

1. Introduction

a. This publication provides fundamental constructs and guidance to assist joint force commanders (JFCs), their staffs, and supporting and subordinate commanders in the planning, execution, and assessment of cyberspace operations (CO). CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

b. This publication discusses military operations in and through cyberspace; explains the Joint Staff (JS), combatant command (CCMD), United States Strategic Command (USSTRATCOM), United States Cyber Command (USCYBERCOM), functional and Service component relationships and responsibilities; and establishes a framework for the employment of cyberspace forces and capabilities.

c. Most aspects of joint operations rely in part on cyberspace, the global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Developments in cyberspace provide the means for the US military, its allies, and partner nations to gain and maintain a strategic, continuing advantage in the operational environment (OE), and can be leveraged to ensure the nation's economic and physical security. Cyberspace reaches across geographic and geopolitical boundaries, much of it residing outside of US control, and is integrated with the operation of critical infrastructures, as well as the conduct of commerce, governance, and national security. Access to the Internet provides adversaries the capability to compromise the integrity of US critical infrastructures in direct and indirect ways. These characteristics and conditions present a paradox within cyberspace: the prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace, for the US in general and the joint force in particular.

d. While CO can produce stand-alone tactical, operational, and strategic effects and achieve objectives, they must be integrated with the employment of the JFC's other capabilities to create synergistic effects in support of the JFC's plan.

e. CO takes place in a complex environment: large parts of cyberspace are not under the any nations' control; the array of state and non-state actors is extremely broad; the costs of entry are low; and technology proliferates rapidly and often unpredictably. Conversely, they should also be prepared to conduct operations under degraded cyberspace conditions.

They should develop mitigation and recovery measures, defensive cyberspace operations (DCO) priorities, primary/secondary/tertiary communication means, and measures to ensure critical data reliability. When the staff perceives that they cannot trust data on a network, or segment of the network, they should stop using the network/segment. In fact, the perception of data unreliability may unnecessarily extend beyond the specific degraded segment. Therefore, it is imperative that the staff be informed of network/segment status as quickly as possible.

2. Cyberspace

a. Cyberspace, while a global domain within the information environment, is one of five interdependent domains, the others being the physical domains of air, land, maritime, and space. Much as air operations rely on air bases or ships in the land and maritime domains, CO rely on an interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers, and the content that flows across and through these components. CO rely on links and nodes that reside in the physical domains and perform functions experienced both in cyberspace and the physical domains. For example, network servers may reside in a land-based data complex or at sea aboard warships, and wireless network transmissions pass through air and space and even underwater. Similarly, activities in cyberspace can enable freedom of action for activities in the physical domains. 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 can only be provided via space operations. Space provides a key global connectivity option for CO. Conversely, CO provide a means by which space support is executed. These inter-relationships are important considerations across the spectrum of CO, and particularly when conducting targeting in cyberspace (see Chapter IV, “Planning and Coordination”).

b. Cyberspace consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an internet protocol [IP] address or other analogous identifier) on those networks, and the system data (such as routing tables) that support them. Though not all nodes and networks are globally connected or accessible, cyberspace continues to become increasingly interconnected. Networks can be intentionally isolated or subdivided into enclaves using access controls, encryption, disparate protocols, or physical separation. With the exception of physical separation, none of these approaches eliminate underlying physical connectivity; instead they limit access. Achieving CO access may be affected by legal, sovereignty, policy, informational environment, or operational limitations; however, adjusting to limitations does not necessarily allow access to a target.

c. Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona (Figure I-1). Each of these represents a level on which CO may be conducted.

(1) The physical network layer of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel. The geographic component is the location in land, air, sea, or space where elements of the

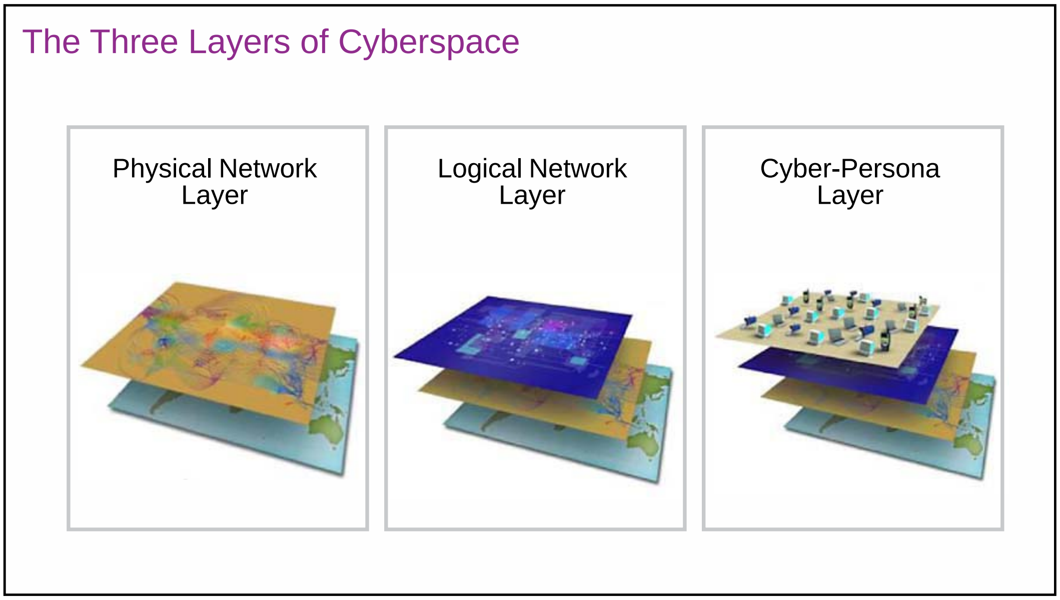


Figure I-1. The Three Layers of Cyberspace

network reside. While geopolitical boundaries can easily be crossed in cyberspace at a rate approaching the speed of light, there are still sovereignty issues tied to the physical domains. The physical network component is comprised of the hardware, systems software, and infrastructure (wired, wireless, cabled links, EMS links, satellite, and optical) that supports the network and the physical connectors (wires, cables, radio frequency, routers, switches, servers, and computers). However, the physical network layer uses logical constructs as the primary method of security (e.g., information assurance [IA]) and integrity (e.g., virtual private networks that tunnel through cyberspace). This is a primary target for signals intelligence (SIGINT), including computer network exploitation (CNE), measurement and signature intelligence, open source intelligence, and human intelligence. It is the first point of reference for determining jurisdiction and application of authorities. It is also the primary layer for geospatial intelligence, which can also contribute useful targeting data in cyberspace.

(2) The **logical network** layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node. A simple example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator (URL). For example, Defense Knowledge Online exists on multiple servers in multiple locations in the physical domains, but is represented as a single URL on the World Wide Web. A more complex example of the logical layer is the DOD's Nonsecure Internet Protocol Router Network (NIPRNET).

(3) The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network. Cyber-personas may relate fairly directly to an actual person or entity, incorporating some biographical or corporate

data, e-mail and IP address(es), Web pages, phone numbers, etc. However, one individual may have multiple cyber-persona, which may vary in the degree to which they are factually accurate. A single cyber-persona can have multiple users. Consequently, attributing responsibility and targeting in cyberspace is difficult. Because cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form, significant intelligence collection and analysis capabilities are required for the joint forces to gain sufficient insight and situational awareness (SA) of a cyber-persona to enable effective targeting and creation of the JFC's desired effect.

d. The Department of Defense information networks (DODIN) are a globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The DODIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

Department of Defense information networks (DODIN) replace Global Information Grid (GIG) terminology, which remains in legacy Department of Defense (DOD) policy and doctrinal publications. Likewise, DODIN operations replace the previous use of DGO [DOD GIG operations].

e. **The Operational Environment.** The OE is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. The continuing advancement of communications and computer technology has significantly reduced acquisition costs leading to the rapid proliferation of cyberspace capabilities, considerably complicating the OE. The OE factors affecting CO vary in importance according to mission. Fully understanding cyberspace and its relationship to the physical domains is the first step in planning military operations in cyberspace.

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

(2) ICT and other advanced technologies are used by a wide range of state and non-state actors, and 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 result in disproportionate effects against a technology-dependent nation or organization. This provides actors who could not otherwise effectively oppose the US using traditional military forces with an asymmetric alternative. Potential adversaries see these technology options as much cheaper alternatives to building expensive weapons, such as stealth fighters or aircraft carriers, to pose a significant threat to US national security.

Additionally, sophisticated cyberspace capabilities of organized crime or other non-state, extralegal organizations may benefit adversaries. This relationship to organized criminal elements may be for financial purposes, with the rise of illicit vendors providing malicious software (malware) as a service. Due to minimal barriers to entry and the potentially high payoff, the US can expect adversaries to resort to asymmetric means to negate US advantages in military capabilities.

f. **The Information Environment.** The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is broken down into the physical, informational, and cognitive dimensions.

(1) **The Physical Dimension.** The physical dimension is composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organizations to conduct operations. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computers, laptops, smart phones, tablet computers, or any other entities that are subject to empirical measurement.

(2) **The Informational Dimension.** The informational dimension is the place where information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of modern military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information.

(3) **The Cognitive Dimension.** The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. In this dimension people think, perceive, visualize, understand, and decide.

g. **The Relationship Between IO and CO**

(1) It is important to address the relationship between IO and CO. CO are concerned with using cyberspace capabilities to create effects which support operations across the physical domains and cyberspace. IO is more specifically concerned with the integrated employment of information-related capabilities during military operations, in concert with other lines of operation (LOOs), to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. Thus, cyberspace is a medium through which some information-related capabilities, such as military information support operations (MISO) or military deception (MILDEC), may be employed. However, IO also uses capabilities from the physical domains to accomplish its objectives.

(2) While some CO may support IO objectives, other CO will be conducted in support of target objectives, or to support operations in the physical domains to achieve objectives. This relationship represents an evolution both in IO, transitioning from a collection of capabilities to a broader integrating function focused on the adversary, and in CO, evolving from its computer network operations roots into a way to operationally

integrate CO within joint operations. In the past, CO have been considered a subset of IO and those operations incorporated in the terms of computer network operations, computer network attack, computer network defense, and CNE. Refer to Director of Central Intelligence Directive 7/3, Information Operations and Intelligence Community Related Activities, for more information on CNE. The terminology used for the training, planning, and execution of military CO includes: offensive cyberspace operations (OCO), DCO, and DODIN operations. OCO and DCO are covered in detail in Chapter II, "Cyberspace Operations."

3. Integrating Cyberspace Operations

a. CO are conducted across the range of military operations. While it is possible that some military objectives can be achieved by CO alone, CO capabilities should be considered during joint operation planning, integrated into the JFC's plan, and synchronized with other operations during execution. Commanders conduct CO to retain freedom of maneuver in cyberspace, accomplish the JFC's objectives, deny freedom of action to adversaries, and enable other operational activities.

b. The importance of CO support to all military operations is growing in tandem with the joint force's increasing reliance on cyberspace, especially for C2, but also for critical logistics functions that often rely on non-DOD networks. However, conflicts that may need to be addressed to fully integrate CO into joint operation planning and execution include: centralized CO planning for DODIN operations and defense; the JFC's need to synchronize operations and fires, including CO; deconfliction requirements between government entities; partner nation relationships; and the relationships between CO and IO, between CO and operations conducted in the physical domains, and the wide variety of legal issues that relate to CO.

4. The Joint Force and Cyberspace

a. The JFC faces a unique set of challenges while executing CO in a complex global security environment. CO are enabled by the DODIN. The DODIN is a global infrastructure of DOD systems carrying DOD, national security, and related intelligence community (IC) information and intelligence.

(1) Threats. Cyberspace presents the JFC with many threats ranging from nation states to individual actors.

(a) **Nation State Threat.** This threat is potentially the most dangerous because of access to resources, personnel, and time that may not be available to other actors. Other nations may employ cyberspace to either attack or conduct espionage against the US. Nation state threats involve traditional adversaries and sometimes, in the case of espionage, even traditional allies. Nation states may conduct operations directly or may outsource them to third parties to achieve their goals.

A cyberspace capability is a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

(b) **Transnational Actor Threat.** Transnational actors are formal and informal organizations that are not bound by national borders. These actors use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, destabilize confidence in governments, and conduct direct terrorist actions within cyberspace.

(c) **Criminal Organization Threat.** Criminal organizations may be national or transnational in nature. Criminal organizations steal information for their own use or, in turn, to sell to raise capital. They also may be used as surrogates by nation states or transnational actors to conduct attacks or espionage through CO.

(d) **Individual Actors or Small Group Threat.** Individual actors or small groups of people can illegally disrupt or gain access to networks or computer systems. Their intentions are as varied as the number of groups and individuals. These actors gain access into systems to discover vulnerabilities, sometimes sharing the information with the owners; however, they also may have malicious intent. Political motivations often drive their operations, and they use cyberspace to spread their message. They may also create and then install malware on commercial or government systems. These actors can be exploited by others, such as criminal organizations or nation states, in order to execute concealed operations against targets in order to preserve their identity or create plausible deniability.

(2) **Anonymity and Difficulties with Attribution.** Perhaps the most challenging aspect of attributing actions in cyberspace is connecting a cyberspace actor (cyber-persona) or action to an actual individual, group, or state actor. This effort requires significant analysis and collaboration with non-cyberspace agencies or organizations. The nature of cyberspace presents challenges to determining the origin of cyberspace threats.

(3) **Additional Challenges.** CO may not require physical proximity; many CO can be executed remotely. Moreover, the effects of CO may extend beyond a target, a joint operations area (JOA), or even an area of responsibility (AOR). Because of transregional considerations or the requirement for high-demand, low-density resources, CO may be coordinated, integrated, and synchronized with centralized execution from a location outside the AOR of the supported commander. Another challenge facing the JFC is that the use of a capability may reveal its functionality and compromise future effectiveness. This has implications for OCO, but it also affects DCO as the same capabilities may have a role in both OCO and DCO. OCO and DCO are covered in detail in Chapter II, "Cyberspace Operations."

b. **Cyberspace Integration/Synchronization**. CO encompass more than just the network connections upon which the joint force relies. Cyberspace effects are created through the integration of cyberspace capabilities with air, land, maritime, and space capabilities. The boundaries within which CO are executed and the priorities and restrictions on its use should be identified in coordination between the JFC, non-DOD government departments and agencies, and national leadership. Effects in cyberspace may have the potential to impact intelligence, diplomatic, and law enforcement (LE) efforts and therefore will often require coordination across the interagency.

c. **Private Industry.** Many of DOD's critical functions and operations rely on commercial assets, including Internet service providers and global supply chains, over which DOD has no direct authority to mitigate risk effectively. Therefore, DOD will work with the Department of Homeland Security (DHS), other interagency partners, and the private sector to improve cybersecurity. One example of such cooperation is the 2010 memorandum of agreement signed by DOD and DHS to align and enhance cybersecurity collaboration. The memorandum formalizes joint participation in program planning and improves a shared understanding of cybersecurity. Under this memorandum USCYBERCOM and DHS exchange liaison personnel. DOD supports DHS in leading interagency efforts to identify and mitigate cyberspace vulnerabilities in the nation's critical infrastructure. DOD has the lead for the defense industrial base (DIB) sector, but will continue to support the development of whole-of-government approaches for managing risks associated with the globalization of the ICT sector. The global technology supply chain affects mission critical aspects of the DOD enterprise and IT risks must be mitigated through strategic public-private sector cooperation. DOD is partnering with the DIB to increase the safeguarding of DOD program information residing or transiting DIB unclassified networks. To increase protection of DIB networks, DOD launched the DIB Cybersecurity and Information Assurance Program. The DOD Cyber Crime Center serves as DOD's operational focal point for this voluntary cyberspace information sharing and incident reporting program.

d. As the JFC integrates CO capabilities into joint operations, careful consideration must be given to some of the unique aspects of cyberspace, as well as its commonalities and synergies with operations in the physical domains: the relationship with IO; legal, political, and technical drivers and constraints; and the role of non-DOD actors in US CO. The employment of cyberspace capabilities and their effective integration with other military operations are discussed in detail in the next chapter.

CHAPTER II
CYBERSPACE OPERATIONS

> *"DOD [Department of Defense] will execute an active cyber [space] defense capability to prevent intrusions into DOD networks and systems…and is developing new defense operating concepts and computing architectures for its cyberspace operations that go beyond the current operational and technical paradigms. All of these components combine to form adaptive and dynamic defense of DOD networks and systems."*
>
> **Department of Defense Strategy for Operating in Cyberspace, May 2011**

1. Introduction

a. CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. CO are composed of the military, intelligence, and ordinary business operations of DOD in and through cyberspace. The military component of CO, which is the only one guided by joint doctrine, is the focus of this publication. Combatant commanders (CCDRs) use CO in and through cyberspace in support of military objectives.

b. **Domain Overlap.** CO enhance operational effectiveness and leverage various capabilities from physical domains to create effects, which may span multiple geographic combatant commanders' (GCCs') AORs. Some of the capabilities the JFC may employ in conjunction with, or to enable CO, include significant portions of electronic warfare (EW), EMS management, C2, intelligence, surveillance, and reconnaissance (ISR), navigation warfare (NAVWAR), and some space mission areas. Advancements in technology have created an increasingly complex OE. CO, space operations, and EW operations can be conducted against targets using portions of the EMS. They can be integrated with other information related capabilities as part of IO. CO, space operations, and EW operations are often conducted under specific authorities. Likewise, some information-related capabilities supported by CO, such as MISO, MILDEC, and special technical operations (STO), have their own execution approval process. The JFC and staff must be familiar with the different coordination requirements, and forward requests for execution as early in the planning process as possible in order to comply with US law and to facilitate effective and timely CO. To minimize overlap, the primary responsibility for CO coordination between USCYBERCOM and JFCs will reside with the cyberspace support element (CSE) in coordination with the CCMD joint cyberspace centers (JCCs). For National Guard matters, USSTRATCOM/USCYBERCOM coordinates with the Chief, National Guard Bureau. Refer to Chapter III, "Authorities, Roles, and Responsibilities," for specifics on CO authorities. Refer to respective doctrine and policy documents of supported information-related capabilities for specifics on their authorities.

For more information, see Joint Publication (JP) 3-13.1, Electronic Warfare*, and JP 6-0,* Joint Communications System.

c. **Authorities Overlap.** Like other military operations conducted by the JFC or Service elements, CO are covered by appropriate authorities, such as military orders, standing or supplemental rules of engagement, DOD policy, etc. This includes military intelligence activities that provide ISR in cyberspace. The JFC also receives support from DOD intelligence agencies, such as NSA, in accordance with national and departmental policies and guidance. Likewise, DOD ordinary business operations in cyberspace are accomplished by DOD agencies following DOD policy.

2. Military Operations In and Through Cyberspace

a. **Cyberspace Operations.** The successful execution of CO requires integrated and synchronized offensive, defensive, and DODIN operations, underpinned by effective and timely operational preparation of the environment (OPE). CO missions are categorized as OCO, DCO, and DODIN operations based on their intent. Specific actions are discussed in paragraph 2.e, “Cyberspace Actions.” All CO missions are informed by timely intelligence and threat indicators from traditional and advanced sensors, vulnerability information from DOD and non-DOD sources, and accurate assessments.

See JP 5-0, Joint Operation Planning*, Appendix D, “Assessment,” for more information on assessment and battle damage assessment (BDA).*

(1) **Offensive Cyberspace Operations.** OCO are CO intended to project power by the application of force in and through cyberspace. OCO will be authorized like offensive operations in the physical domains, via an execute order (EXORD). OCO requires deconfliction in accordance with (IAW) current policies.

(2) **Defensive Cyberspace Operations.** DCO are CO intended to defend DOD or other friendly cyberspace. Specifically, they are passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. DCO responds to unauthorized activity or alerts/threat information against the DODIN, and leverages intelligence, counterintelligence (CI), LE, and other military capabilities as required. DCO includes outmaneuvering adversaries taking or about to take offensive actions against defended networks, or otherwise responding to internal and external cyberspace threats. Most DCO occurs within the defended network. Internal defensive measures include mission assurance actions to dynamically reestablish, re-secure, reroute, reconstitute, or isolate degraded or compromised local networks to ensure sufficient cyberspace access for JFC forces. DCO also includes actively hunting for advanced internal threats that evade routine security measures. However, some adversary actions can trigger DCO response actions (DCO-RA) necessary to defend networks, when authorized, by creating effects outside of the DODIN. DCO consists of those actions designed to protect friendly cyberspace from adversary actions. DCO may be conducted in response to attack, exploitation, intrusion, or effects of malware on the DODIN or other assets that DOD is directed to defend. DOD’s DCO mission is accomplished using a layered, adaptive, defense-in-depth approach, with mutually supporting elements of digital and physical protection. A key characteristic of DOD’s DCO activities is a construct of active cyberspace defense. The Department of Defense Strategy for Operating in Cyberspace describes active cyberspace

defense as DOD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities to defend networks and systems. Leveraging the full range of DCO, active cyberspace defense builds on traditional approaches to defending DOD networks and systems to address advanced persistent threats. Defense of the DODIN and other elements of cyberspace requires SA and automated, agile, and synchronized preapproved defenses. Types of DCO consist of:

(a) **Internal Defensive Measures.** Internal defensive measures are those DCO that are conducted within the DODIN. They include actively hunting for advanced internal threats as well as the internal responses to these threats. Internal defensive measures respond to unauthorized activity or alerts/threat information within the DODIN, and leverage intelligence, CI, LE, and other military capabilities as required.

(b) **DCO Response Actions.** DCO-RA are those deliberate, authorized defensive actions which are taken external to the DODIN to defeat ongoing or imminent threats to defend DOD cyberspace capabilities or other designated systems. DCO-RA must be authorized IAW the standing rules of engagement and any applicable supplemental rules of engagement and may rise to the level of use of force. In some cases, countermeasures are all that is required, but as in the physical domains, the effects of countermeasures are limited and will typically only degrade, not defeat, an adversary's activities.

1. **Countermeasures.** 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, countermeasures are intended to identify the source of a threat to the DODIN and use non- intrusive techniques to stop or mitigate offensive activity in cyberspace. Countermeasures extend beyond the DOD perimeters against a specific adversary activity. Countermeasures are nondestructive in nature, typically impact only malicious activity but not the associated threat systems, and are terminated when the threat stops. Countermeasures in cyberspace should not destroy or significantly impede the operations or functionality of the network they are being employed against, nor should they intentionally cause injury or the loss of life. Any DOD authorized use of countermeasures must be in compliance with US domestic law, international law, and applicable rules of engagement. Countermeasures require deconfliction with other USG departments and agencies to the maximum extent practicable.

(3) **DOD Information Network Operations.** DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation. These include proactive actions which address the entire DODIN, including configuration control and patching, IA measures and user training, physical security and secure architecture design, operation of host-based security systems and firewalls, and encryption of data. Although many DODIN operations activities are regularly scheduled events, they should not be considered routine or unimportant, since their aggregate effect establishes the security framework on which all DOD missions ultimately depend.

b. **Security of Non-DOD Information Networks.** While DCO are generally focused on the DODIN, which includes all networks owned or leased by DOD, DOD relies on many other networks, including private sector networks, to support DOD operations. Responsibility for these non-DOD information networks and systems falls to the network owners, which include other USG departments and agencies and private sector entities. Since all DOD-associated networks are known targets for our adversaries, protection of these non-DOD information networks and systems is just as important as protection of the DODIN. Unfortunately, DOD cannot guarantee the level of security of non-DOD information networks or the robustness of the security standards governing such networks. The JFC's mission risk analysis should account for this uncertainty in security of non-DOD networks. It is essential that planners and those supporting CO coordinate with non-DOD essential network owners to better secure those networks. USCYBERCOM liaises with other USG departments and agencies that can facilitate necessary planning.

c. **Routine Uses of Cyberspace.** Most military CO are routine uses of cyberspace. Routine uses of cyberspace, such as operating C2 or logistics systems, sending an e-mail, using the Internet to complete an on-line training course, and developing a briefing or document, employ cyberspace capabilities and complete tasks in cyberspace, but they do not amount to OCO, DCO, or DODIN operations. Other than being an authorized user of the network, DOD members need no special authorities to conduct these activities. However, it is through these routine uses of cyberspace where a majority of the vulnerabilities on our networks are exposed to, and exploited by, our adversaries. As such, the importance of cultivating a culture of cyber security among all DODIN users cannot be overstated. The challenge is to train DODIN users to recognize the trade craft of adversaries so that routine cyberspace uses do not continue to represent a source of unnecessary risk to the mission. DODIN operations functions, particularly interagency policies and training, are critical to the success of all types of DOD CO.

d. **Intelligence Operations.** See JP 2-01, *Joint and National Intelligence Support to Military Operations,* for a more complete discussion of activities that fall under intelligence operations.

e. **Cyberspace Actions.** While the JFC's military missions in cyberspace (OCO, DCO, and DODIN operations) are categorized by intent, as described above, these missions will require the employment of various capabilities to create specific effects in cyberspace. To plan for, authorize, and assess these actions, it is important the JFC and staff understand how they are distinguished from one another.

(1) **Cyberspace Defense.** Actions normally created within DOD cyberspace for securing, operating, and defending the DODIN. Specific actions include protect, detect, characterize, counter, and mitigate. Such defensive actions are usually created by the JFC or Service that owns or operates the network, except in such cases where these defensive actions would impact the operations of networks outside the responsibility of the respective JFC or Service.

(2) **Cyberspace ISR.** An intelligence action conducted by the JFC authorized by an EXORD or conducted by attached SIGNT units under temporary delegated SIGINT

operational tasking authority. Cyberspace ISR includes ISR activities in cyberspace conducted to gather intelligence that may be required to support future operations, including OCO or DCO. These activities synchronize and integrate the planning and operation of cyberspace systems, in direct support of current and future operations. Cyberspace ISR focuses on tactical and operational intelligence and on mapping adversary cyberspace to support military planning. Cyberspace ISR requires appropriate deconfliction, and cyberspace forces that are trained and certified to a common standard with the IC. ISR in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other USG departments and agencies.

(3) **Cyberspace Operational Preparation of the Environment.** OPE consists of the non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations. OPE requires cyberspace forces trained to a standard that prevents compromise of related IC operations. OPE in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other USG departments and agencies.

(4) **Cyberspace Attack.** Cyberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. These specific actions are:

(a) **Deny.** To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents adversary use of resources.

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

2. **Disrupt.** To completely but temporarily deny (a function of time) 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 selected is 100 percent.

3. **Destroy.** To permanently, completely, and irreparably deny (time and amount are both maximized) access to, or operation of, a target.

(b) **Manipulate.** To control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives.

3. National Intelligence Operations In and Through Cyberspace

National level intelligence organizations, including major DOD agencies, conduct intelligence activities for national intelligence priorities. This intelligence can support a military commander's planning and preparation.

See JP 2-01, Joint and National Intelligence Support to Military Operations, *for a more complete discussion of activities that fall under intelligence operations.*

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

Ordinary business operations in and through cyberspace are those non-warfighting capabilities and functions used to support and sustain DOD forces in their normal day-to-day functions, but that are not normally under the control of a JFC. This includes the CO of the Services and civilian-run DOD agencies, such as the Defense Finance and Accounting Service and the Defense Commissary Agency. These organizations conduct routine uses of cyberspace, as well as DODIN operations and some internal defensive measures. Since the conduct of DOD ordinary business operations in cyberspace is not generally guided by joint doctrine, they are not discussed here in detail. However, vulnerabilities that occur in DOD ordinary business operations processes can easily become vulnerabilities that directly impact the JFC's mission. A compromise in any area of cyberspace might result in an exposure to other areas.

5. The Joint Functions and Cyberspace Operations

a. JP 3-0, *Joint Operations,* delineates joint functions common to joint operations at all levels of war into six basic groups: C2, intelligence, fires, movement and maneuver, protection, and sustainment. These joint functions comprise related capabilities and activities grouped together to help JFCs integrate, synchronize, and direct joint operations. This section presents an overview of how each of these functions applies to effective joint operations in and through cyberspace.

b. **Command and Control.** C2 of operations in and through cyberspace encompasses the exercise of authority and direction by commanders over assigned and attached forces in the accomplishment of their mission. The JFC provides operational vision, guidance, and direction to the joint force. In their role to provide a communications pathway, planning and decision-support aids, and cyberspace related ISR, CO can provide timely access to critical information which can enable JFCs to make and execute decisions more rapidly than the adversary, giving commanders more control over the timing and tempo of operations.

(1) CO requires unity of effort to synchronize forces toward a common objective. However, the dual nature of CO as simultaneously providing actions at the global level and at the theater or JOA level necessitates adaptations to traditional C2 structures. Joint forces principally employ centralized planning with decentralized execution of operations. Certain CO functions, particularly global defense, lend themselves to centralized execution to meet multiple, near-instantaneous requirements for response. However, those CO must be integrated and synchronized with the JFC's regional or local CO, conducted by forces assigned or attached to the JFC. For these reasons, there may be times when C2 of global CO and of theater CO are conducted using a support command relationship under two separate, but mutually supporting/supported chains of command. USSTRATCOM/ USCYBERCOM is the supported command for global or trans-regional CO even as it supports one or more JFC's operations. For specific CO, the supported/supporting command relationship will be established in the EXORD. A supported relationship for CO does not

exempt either command from coordinating response options with affected JFCs prior to conducting an operation. Regardless of which model is employed for any particular operation, unless otherwise specified in supplemental orders or directives, effective C2 for CO will be standardized, integrated, and synchronized IAW the 15 March 2012 Joint Staff Transitional Cyberspace Operations Command and Control (C2) Concept of Operations (CONOPS) to ensure effective coordination of joint forces and to provide a common construct for JFCs to execute their mission within a global context.

(2) Differing C2 structures can provide a unique organization and array of forces for the JFC. C2 of DOD forces conducting CO activities are defined by the JFC and enumerated in the concept of operations (CONOPS)/operation order (OPORD).

(a) DODIN operations require centralized coordination because they have the potential to impact the integrity and operational readiness of the DODIN. Although execution will generally be decentralized, Commander, United States Strategic Command (CDRUSSTRATCOM) is the supported commander for CO to secure, operate, and defend the DODIN, and to defend US critical cyberspace assets, systems, and functions.

(b) Theater-level DODIN operations are those activities occurring within a theater that have the potential to impact only operations in that theater. The CCMD JCC should coordinate actions with the USCYBERCOM CSE located on site to ensure effects are constrained within authorized areas. Examples may include operations on mission networks, the timing of centrally directed network configuration, establishing MINIMIZE to limit outbound traffic flow or other prioritization of theater resources. The affected GCC is the supported command for theater-level DODIN operations with CDRUSSTRATCOM/ Commander, United States Cyber Command (CDRUSCYBERCOM) supporting, as required.

(c) CDRUSSTRATCOM is the supported commander for global CO, and may delegate authority where appropriate to CDRUSCYBERCOM.

(d) **C2 for Theater CO Fires and Maneuver.** These CO support JFC objectives and the JFC is the supported commander, with USCYBERCOM supporting as necessary. The JFC is responsible for integrating and synchronizing CO fires with other fires, and may use either assigned or attached assets or supporting USCYBERCOM assets. JFCs coordinate their requirements with USCYBERCOM to ensure they are accounted for and prioritized in execution. CO maneuvers will become vital when a JFC's capabilities are under attack to the degree that subsets of friendly cyberspace are degraded, compromised, or lost. In such operations, the Defense Information Systems Agency (DISA) is in a supporting role, as required.

(3) Decision authority for most OCO and some DCO involves careful consideration of projected effects and geopolitical boundaries. However, some OCO and some DCO activities have inherent transregional effects, requiring interagency coordination to deconflict activities in cyberspace and assure appropriate consideration of nonmilitary factors such as foreign policy implications. For these reasons, OCO and some DCO require careful planning, in-depth intelligence support, and interagency coordination. The growing reliance

on cyberspace around the globe requires carefully controlling OCO, requiring national level approval. This requires commanders to remain cognizant of changes in national cyberspace policy and potential impacts on operational authorities.

(4) A common operational picture (COP) for cyberspace facilitates C2 of CO and real-time comprehensive SA. A cyberspace COP should include the ability to rapidly fuse, correlate, and display data from global network sensors to deliver a reliable picture of friendly, neutral, and adversary networks, including their physical locations and activities. In addition, the cyberspace COP should support real-time threat and event data from myriad sources (i.e., DOD, IC, interagency, private industry, and international partners) and improve commanders' abilities to identify, monitor, characterize, track, locate, and take action in response to cyberspace activity as it occurs both globally for USSTRATCOM/ USCYBERCOM and within the AOR for the GCC.

c. **Intelligence**

(1) Intelligence collected in cyberspace may come from DOD and/or national-level sources and may serve strategic, operational, or tactical requirements. JP 2-0, *Joint Intelligence*, covers the basics of military intelligence joint doctrine. This section addresses the unique challenges of military intelligence in cyberspace. Intelligence operations in cyberspace not associated with the JFC are covered in paragraph 3, "National Intelligence Operations In and Through Cyberspace."

(2) Understanding the OE is fundamental to all joint operations. Intelligence support to CO utilizes the same intelligence process (i.e., intelligence operations) as in all other military operations:

(a) Planning and direction, to include managing CI activities that protect against espionage, sabotage, and attacks against US citizens/facilities; and examining mission success criteria and associated metrics to assess the impact of CO and inform the commander's decisions.

(b) Collection, to include surveillance and reconnaissance.

(c) Processing and exploitation of collected data.

(d) Analysis of information and production of intelligence.

(e) Dissemination and integration of intelligence with operations quality.

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

(3) **Event Detection and Characterization.** Activities in cyberspace by a sophisticated adversary may be difficult to detect. Unlike adversary actions in the physical domains which may be detected by the presence of equipment or specific activity, adversary actions in cyberspace may not be easily distinguishable from legitimate activity. Capabilities for detecting and attributing activities in cyberspace are critical for enabling effective DCO and OCO. Equally important, rapid assessment of DOD operations in and through

cyberspace facilitates necessary rapid adaptation and changes in tactics, defensive measures, and other available response options.

(4) In order to minimize the effects of threats that exploit previously unknown vulnerabilities, joint forces should develop mitigation and recovery measures, to include exercising the capability to operate in a denied or compromised portion of cyberspace.

(5) **Analysis and Attribution.** Due to the characteristics of the physical network, logical network, and cyber-persona layers in CO, attribution of adversary OCO to people, criminal organization, non-state actors, or even responsible nation states is difficult.

(6) **Intelligence Gain/Loss (IGL).** Another concern is that CO could potentially compromise intelligence collection activities. An IGL assessment is required prior to executing a CO to the maximum extent practicable. The IGL assessment could be further complicated by the array of non-DOD USG and multinational partners operating in cyberspace. See Chapter IV, "Planning and Coordination," for further information regarding targeting in CO.

(7) **Indications and Warning (I&W).** Cyberspace intelligence on nation-state threats should include all-source analysis in order to factor in traditional political/military I&W. Adversary cyberspace actions will often occur outside, and often well in advance of, traditional adversary military activities. Additionally, cyberspace I&W may recognize adversary CO triggers with only a relatively short time available to respond. These factors make the inclusion of all-source intelligence analysis very important for the effective analysis of our adversaries' intentions in cyberspace.

d. **Fires.** Depending on the objective, cyberspace fires can be offensive or defensive, supporting or supported. Like all forms of power projection, fires in and through cyberspace should be included in the joint planning and execution processes from inception in order to facilitate synchronization and unity of effort. Fires in and through cyberspace encompass a number of tasks, actions, and processes, including:

(1) **Joint Targeting, Coordination, and Deconfliction.** The purpose of targeting is to integrate and synchronize fires 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 is pivotal to the success of targeting. Understanding the objectives, intentions, capabilities, and limitations of all actors within the OE enables the use of joint, interagency, and multinational means to create effects. Target development and selection are based on what the commander wants to achieve rather than on the available ways and means to achieve them. In other words, the focus should be on creating the desired target effects that accomplish targeting-related tasks and objectives. Deconfliction is the act of coordinating those targets with applicable DOD, interagency, and multinational partners. Therefore, cyberspace targets should be nominated, vetted, and validated within the established targeting process. The targeting process for CO requires close coordination within DOD, with interagency and multinational partners, and with key allies. Deconfliction of CO has both an operational and a technical component. If two USG entities have

requirements to create effects on the same target in cyberspace, their uncoordinated actions could expose or interfere with the actions of one or both. Assuming both effects can be created independently and are sufficiently well-justified, a technical analysis will still need to be conducted to determine if the proposed capabilities can operate in the same target environment without interference or increasing the chances of unwanted detection.

For more information on joint targeting, see JP 3-60, Joint Targeting.

(2) **Integration of Cyberspace Fires.** CO capabilities, though they may be used in a stand-alone context, are generally most effective when integrated with other capabilities to create the JFC's desired effects. Cyberspace capabilities can be used to manipulate adversary cyberspace targets through MILDEC, redirection, systems conditioning, etc., to assist with friendly mission objectives, or deny adversary functional use of cyberspace assets. These effects can be created at the strategic, operational, or tactical level.

(3) **Assessment.** The assessment process includes measuring the appropriate performance and effectiveness of fires, as well as their contribution to the larger operation or objective. Although traditional assessment of military operations has been in terms of first-order battle damage, ongoing and recent military operations suggest that physical damage is often not the most operationally or strategically important. BDA is composed of physical damage assessment, functional damage assessment, and target system assessment, typically taking a three-phased approach to proceed from a micro-level examination of the damage or effect inflicted on a specific target, to ultimately arriving at macro-level conclusions regarding the functional outcomes created in the target system. Likewise, first-order effects of CO are often subtle, and assessment of second- and third-order effects can be difficult. Thus assessment of fires in and through cyberspace frequently requires significant intelligence capabilities and collection efforts. Prediction and assessment for CO must be incorporated into existing joint force staff processes to ensure that JFC objectives are met.

e. **Movement and Maneuver**

(1) Movement and maneuver involves deploying forces into an operational area and moving within that area to gain operational advantage in support of operational objectives. An essential component of planning is the concept of key terrain, which is any locality or area, the seizure or retention of which affords a marked advantage to either combatant. These might include major lines of communications; key access points for the defense, observation, and launch points for the offense; or opportunities to create bottlenecks. In cyberspace, key terrain involves network links and nodes that are essential to a particular friendly or adversary capability. The ubiquitous nature of cyberspace creates another major consideration in CO, because it enables an adversary to establish key points of presence outside the physical operating area.

(2) Another component of maneuver in cyberspace is the movement of data. In this context, bandwidth (wired or wireless), the available data throughput that can be physically accommodated by the supporting infrastructure, can be considered as roughly analogous to lines of communications in the physical domains. The ability to maneuver the flow of data from one physical line to another, for example from terrestrial cables to satellite

communications (SATCOM) links, is an example of maintaining freedom of maneuver in cyberspace. Managing the EMS within the battle space is a key component for the JFC to consider in developing and executing operations.

(3) Movement and maneuver in cyberspace can occur in all three layers: the physical network, logical network, and the cyber-persona layer.

f. **Sustainment**

(1) Sustainment is the provision of logistics and personnel services required to maintain and prolong operations until successful mission accomplishment. Services and United States Special Operations Command (USSOCOM) organize, train, equip, and sustain forces for CO. JFCs must identify required forces and capabilities, critical cyberspace assets, assess risk, ensure redundancy (including non-cyberspace alternatives), and actively exercise continuity of operations plans to respond to outages or adversary actions that degrade or compromise cyberspace access or reliability.

(2) Advancements in IT continue to develop rapidly, which in turn requires the Services and USSOCOM to develop, field, and sustain cyberspace capabilities adaptable to the rapid changing OE. For example, new wireless mobile devices may provide greater Internet access, an adversary might update or change operating systems, or they may transition to the use of virtual machines in their network architecture. Joint forces need the capability to rapidly incorporate new cyberspace capabilities into their arsenal. Additionally, the joint force may need the capability to rapidly upgrade their own networks to leverage new technologies. Pressure to deploy new technology must be balanced against approved requirements and increased risks, and implementation must be carefully orchestrated to prevent divergence among Service-provisioned networks that could create gaps or seams in DOD’s global architecture.

(3) A key component of sustainment is the maintenance of a well-trained force. Most successful network intrusions and attacks can be traced to poor operator and/or administrator security practices. Assets deployed securely only remain secure if they are maintained accordingly.

(4) Many critical legacy systems are not built to be easily modified or patched. As a result, many of the risks incurred across DOD are introduced via unpatched (and effectively unpatchable) systems on the DODIN. This risk can be mitigated through additional layers of network protection, which must then be sustained. Additionally some hardware capabilities can also deteriorate over time, requiring component, software, or firmware upgrades. Replacement due to wear and tear or adversary discovery/compromise may be necessary to ensure sensors and other forward deployed cyberspace capabilities are ready when needed. This can be particularly problematic when physically inaccessible systems (such as those deployed to remote sites or on ships) must be replaced or upgraded. It is vital that commanders understand the risk created by leaving such vulnerabilities in place, not just to their operation, but to the future success of DOD missions worldwide. Finally, contingency software capabilities that are not often accessed may also require

periodic refreshing and retesting to ensure that they are still both secure and capable of creating the required effects despite changes in the targeted OE.

g. **Protection**

(1) Protection is somewhat unique within cyberspace because adversaries can create multiple, cascading effects that may not be restricted by physical geography, civil/military boundaries, and significantly expand the area requiring protection. Cyberspace capabilities requiring protection include not only the infrastructure (computers, cables, antennas, and switching and routing equipment), as well as parts of the EMS (e.g., 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 the DODIN and the ability to monitor, detect, and prevent hostile traffic from entering and exfiltration of information.

(2) Protection of friendly cyberspace uses a combination of defensive capabilities and OPSEC. Because of the speed of effects in cyberspace, automated technologies for securing networks, verifying approved network configurations, and discovering network vulnerabilities often provide a far better chance of success than their manual equivalents. However, the strongest encryption and most secure protocols cannot protect our networks from poorly trained/motivated users who do not employ proper security practices. Commanders should ensure personnel understand and are accountable for their roles in cybersecurity.

CHAPTER III
AUTHORITIES, ROLES, AND RESPONSIBILITIES

> *"The US Government has the responsibility to… ensure that the United States and its citizens, together with the larger community of nations, can realize the full potential of the Information Technology revolution."*
>
> **President Obama, 29 May 2009**

1. Introduction

a. Under the authorities of the Secretary of Defense (SecDef), DOD uses cyberspace capabilities to shape cyberspace and provide integrated offensive and defensive options. As directed by USSTRATCOM, USCYBERCOM synchronizes and directs transregional operations and, in coordination with CCMDs, JS, and Office of the Secretary of Defense (OSD), liaises with other USG departments and agencies, and members of DIB in conjunction with DHS. Similarly, as directed, DOD will deploy necessary resources to support efforts of other USG departments and agencies.

b. The National Military Strategy for Cyberspace Operations (NMS-CO) and the *Department of Defense Strategy for Operating in Cyberspace* provide requirements for national defense in cyberspace and DOD's role in defending US national interests through CO.

c. **DOD's Roles and Initiatives in Cyberspace.** The NMS-CO instructs DOD to be prepared to support DHS, as the lead USG agency, in the following cyberspace roles: national incident response and support to USG departments and agencies in CI/KR protection. To fulfill this mission, DOD conducts military operations to defend cyberspace, DOD elements of CI/KR, the homeland, or other vital US interests as directed. If defense of a national interest is required, DOD's national defense missions, when authorized by Presidential orders or standing authorities, take primacy over, and may subsume, the standing missions of other departments or agencies. *The Department of Defense Strategy for Operating in Cyberspace* 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.** In addition to DOD's responsibility to defend the Nation, DOD provides defense support of civil authorities (DSCA), as directed. DOD coordinates with DHS and other interagency partners, as described in the National Response Framework.

e. **Critical Infrastructure/Key Resources 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 DOD Cyber Crime Center. Concurrent with its national defense and incident response missions, DOD will also support DHS and other USG departments and agencies to ensure all sectors of cyberspace CI/KR are available to support national objectives. CI/KR protection relies on analysis, warning, information sharing, vulnerability identification and reduction, mitigation, and aiding of national recovery efforts. Defense critical infrastructure (DCI) refers to DOD and non-DOD assets essential to project, support, and sustain military forces and operations worldwide that are a subset of CI&KR. GCCs have the responsibility to prevent the loss or degradation of the DCI within their AORs and must 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 at the direction of SecDef IAW Department of Defense Directive (DODD) 3020.40, *DOD Policy and Responsibilities for Critical Infrastructure*. This action must be coordinated with the Chairman of the Joint Chiefs of Staff (CJCS) and the Under Secretary of Defense for Policy (USD[P]). The Director of DISA is responsible for matters pertaining to the identification, prioritization, and remediation of critical DODIN infrastructure issues, as the lead agent for the DODIN sector of the DCI. Likewise, DOD is responsible to support the DHS coordination of efforts to protect the DIB and the DODIN portion of the DIB.

2. Authorities

Authority for actions undertaken by the Armed Forces of the United States is derived from the US Constitution and Federal law. These authorities establish roles and responsibilities that provide focus for organizations to develop capabilities and expertise, including those for cyberspace. Key statutory authorities 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*. See Figure III-1 for a summary of applicable titles of USC as they apply to CO.

3. Roles and Responsibilities

a. Secretary of Defense

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

(2) Provide policy guidance and authority for employment of assigned, attached, and supporting military forces conducting cyberspace missions.

(3) Coordinate with secretaries of other USG departments to establish appropriate representation and participation of personnel on joint interagency coordination groups (JIACG), working groups, task forces, etc.

b. DOD Chief Information Officer (CIO)

(1) Serve as SecDef's principal staff assistant for information management (IM), and consequently develop and issue the DOD Information Resources Management Strategic Plan.

United States Code-Based Authorities

United States Code (USC)	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland security	Department of Homeland	Security of US cyberspace
Title 10	*Armed Forces*	National defense	Security Department of Defense	Man, train, and equip US forces for military operations in cyberspace
Title 18	*Crimes and Criminal 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 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-Based Authorities

(2) As the DODIN architect, develop, maintain, and enforce compliance with the DODIN architecture. Inherent in the CIO's architecture responsibility is the responsibility to enforce interoperability, IA, net-centric data sharing, use of enterprise services, and DOD information networks program synchronization.

c. **Chairman of the Joint Chiefs of Staff**

(1) Advise the President and SecDef on operational policies, responsibilities, and programs.

(2) Assist SecDef in implementing operational responses to threats or hostile acts.

(3) Translate SecDef guidance into OPORDs.

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

(5) Assist CCDRs in meeting their operational requirements that have been approved by SecDef.

d. **Service Chiefs**

(1) Provide appropriate administration of and support to cyberspace forces assigned or attached to CCMDs.

(2) Train and equip forces for CO for deployment/support to CCMDs as directed by SecDef. Services will provide CO capabilities for deployment/support to CCMDs as directed by SecDef.

(3) Remain responsible for compliance with USSTRATCOM's direction for operation and defense of the DODIN.

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

(5) Provide users of the EMS regulatory and operational guidance in the use of radio 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).

e. **Chief, National Guard Bureau**

(1) Serves as an advisor to CDRUSSTRATCOM on National Guard matters pertaining to the CCMD missions and support planning and coordination for such activities as requested by the CJCS or the CCDRs.

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

f. **Commander, US Strategic Command**

(1) Has overall responsibility for DODIN operations and defense in coordination with CJCS, the Service Chiefs, and CCDRs. CDRUSSTRATCOM is responsible for CO to secure, operate, and defend the DODIN, and to defend US critical cyberspace assets,

systems, and functions as directed by the President or SecDef, against any intrusion or attack, and does so through a subunified command, USCYBERCOM. At the headquarters level, USSTRATCOM advocates for national requirements and standards, and in coordination with other CCDRs, assesses and reports the operational readiness of the DODIN. Additionally, USSTRATCOM is responsible to establish compliance and enforce accountability across the department and, as required, to engage through CCMDs to build DOD partnering capacity with partner nations with respect to CO.

(2) Represents the DOD SATCOM community, coordinating and orchestrating consolidated user positions with CCMDs, Services, and DOD agencies and with international partners. CDRUSSTRATCOM has operational and configuration management authority for SATCOM on-orbit assets, control systems, and ground terminal infrastructure, including DOD gateways, deemed necessary for the effective and efficient operation of SATCOM for DOD. 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 provide authorized users with global SATCOM support as operations and evolving requirements dictate.

(3) Develops, coordinates, and executes SATCOM operations policies and procedures; constellation deployment plans; and satellite positioning, repositioning, and disposal plans. Assesses how these various plans impact communications support to current and future operations, OPORDs, operation plans (OPLANs), and concept plans (CONPLANs), and coordinates SATCOM actions prior to execution.

(4) In support of Unified Command Plan-assigned missions, CDRUSSTRATCOM:

(a) Coordinates with the IC, CCMDs, Services, agencies, and allied partners to facilitate development of improved cyberspace access to support planning and operations.

(b) Provides shared SA of CO and I&W.

(c) Provides military representation to US national agencies, US commercial entities, and international agencies for cyberspace matters, as directed.

(d) Notifies the CCMDs of ongoing or developing threats and anomalies via appropriate means to reduce potential risks and to ensure effective integration of systems, networks, services, use of the EMS, and to comply with DOD-mandated configuration standards.

(e) Performs analysis of threats to the DODIN, including threat analysis of foreign malicious activity. Changes the global information condition as warranted by threat assessments.

(f) Plans for and, as directed, coordinates DCO of CI&KR.

(g) For global events, USSTRATCOM will be the supported command.

(5) Commander, United States Cyber Command

(a) As USSTRATCOM's execution arm for CO, plan, coordinate, integrate, synchronize, and conduct activities to:

1. Direct the security, operations, and defense of the DODIN.

2. Prepare to, and when directed, conduct full-spectrum military CO.

(b) For global events, CDRUSSTRATCOM will be the supported commander. For theater events, CDRUSCYBERCOM may be a supporting commander.

(c) **Cyberspace Support Elements.** CSEs are organized from USCYBERCOM forces and deployed to CCMDs for full integration into their staffs. CSEs resources are provided by USCYBERCOM to provide the CCMDs with joint CO planners and other subject matter experts on CO. These personnel facilitate development of cyberspace requirements and coordinate, integrate, and deconflict CO into the command's planning process.

1. The CSE provides CCMDs an interface and reachback capability to USCYBERCOM to synchronize cyberspace fires with the commander's scheme of maneuver, develop SA, and facilitate acquiring timely threat information.

2. USCYBERCOM retains operational control of the CSE, and the CSE is in direct support to the JCC.

(e) Leverages the IC to establish and share comprehensive SA of cyberspace, both friendly and adversary, in support of DOD and CCDRs.

(f) Supports CCMDs in the development of and build of the cyberspace portion of joint intelligence preparation of the OE and target system analysis products.

(g) Submits target development nominations to the supported CCMD for inclusion into candidate target lists.

(h) Submits a target nomination list to the supported CCMD targeting staff.

g. **Other Combatant Commanders**

(1) Operate and defend tactical and constructed networks within their commands.

(2) Integrate CO capabilities into all military operations; integrate CO into plans (CONPLANs and OPLANs); and work closely with the joint force, USSTRATCOM/USCYBERCOM, Service components, and DOD agencies to create fully integrated capabilities.

(3) In coordination with USSTRATCOM/USCYBERCOM, GCCs orchestrate the planning efforts for CO, designate the desired effects of CO, and determine the timing and tempo for CO conducted in their AORs in support of GCC missions. Functional CCDRs direct DODIN operations and defense consistent with functional responsibilities.

(4) GCCs lead, prioritize, and direct theater-specific DCO in response to cybersecurity events through the unified command theater network control center or equivalent organization. For cybersecurity events that have been categorized as “global” by USCYBERCOM, CCDRs, when requested through CDRUSSTRATCOM and directed by SecDef, will support response efforts and tasking from CDRUSSTRATCOM as the supported commander.

(5) Serve as a focal point for DODIN operations with multinational partners.

(6) Plan for the 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 with theater impacts.

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

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

(10) Provide users of the EMS regulatory and operational guidance in the use of required frequencies IAW coordinated agreements between US forces and host nations.

h. **Commanders, US Pacific Command and US Northern Command.** In addition to responsibilities in paragraph 3(g), “Other Combatant Commanders,” fulfill specific responsibilities related to DSCA and homeland defense with CDRUSSTRATCOM and others.

i. **Director, Defense Information Systems Agency**

(1) Comply with USSTRATCOM’s direction for executing DODIN operations functions within DISA-operated portions of the DODIN.

(2) Provide engineering, architecture, and provisioning support for integrated DODIN operations, including DOD information network enterprise management, DOD information network content management, and DODIN assurance.

(3) Conduct DODIN operations and DCO at the global and enterprise level, as directed by CDRUSSTRATCOM.

(4) Provide shared SA of DISA-operated portions of the DODIN.

(5) Support compliance inspections IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01, *Information Assurance (IA) and Support to Computer Network Defense (CND)*.

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

(7) Plan, mitigate, and execute service restoration at the global and enterprise level, as directed by CDRUSSTRATCOM.

(8) Provide and maintain a critical nodes defense plan.

j. **Director, National Security Agency/Chief, Central Security Service.** Provides SIGINT support and IA guidance and assistance to DOD components and national customers, pursuant to Executive Order 12333, *US Intelligence Activities* and National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*.

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

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

(2) Provide the same all-source intelligence support to CO as for other joint operations, to include intelligence support to the JFC's intelligence preparation of the OE for operations in cyberspace and intelligence support to targeting.

(3) Through the DIA Office for Cyber threat Analysis:

(a) Assess foreign military C2 processes, networks, and information technologies.

(b) Provide all-source intelligence that looks beyond the current operational or tactical threat to warn of emerging adversary cyberspace capabilities and intent, national space strategy and foreign influence threats, as well as associated risks to DOD critical information infrastructures and national security interests.

(4) DIA's Office of Counterintelligence, Counterespionage Division is the DOD focal point for all CI cyberspace investigations and operations. The division strives to ensure all CI related cyberspace threats to the Services and DOD agencies are identified and neutralized. It supports CI operations in cyberspace to promote operational superiority over America's adversaries. It provides worldwide cyberspace CI SA and coordination.

(5) DIA is responsible for the engineering, development, implementation, and management of the sensitive compartmented information portion of the DODIN including the configuration of information, data, and communications standards for intelligence systems, in coordination with JS, Services, other agencies, and OSD. Included within this is

the overall responsibility for the operation of Joint Worldwide Intelligence Communications System (JWICS), a strategic secure, high capacity telecommunications network serving the IC with voice, data, and video services. DIA establishes defense-wide intelligence priorities for attaining interoperability between tactical, theater, and national intelligence related systems and between intelligence related systems and tactical, theater, and national elements of the DODIN. The DIA exercises operational management of JWICS via the JWICS network operations center.

l. **Other DOD Agencies.** Similar to other DOD component responsibilities, DOD agencies are responsible for ensuring that their information systems environment is developed and maintained in a manner that is consistent with and reflective of the DODIN architecture and that agency-specific programs are planned, resourced, acquired, and implemented IAW the DOD IM support plan and defense resource priorities. Those DOD agencies which are also part of the IC are also subject to the policies and guidance of the IC CIO. DOD Cyber Crime Center's responsibilities include:

(1) Provides digital and multimedia forensics, cyber investigative training; research, development, test and evaluation; and cyberspace analysis to DODIN defense, LE, IC, CI, and counterterrorism agencies;

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

(3) Serves as the operational focal point for the DIB Cybersecurity and Information Assurance Program's information sharing activities performed to protect unclassified DOD information that transits or resides on unclassified DIB information systems and networks.

m. **Department of Homeland Security**

(1) DHS has the responsibility to secure cyberspace, at the national level, by protecting non-DOD USG networks against cyberspace intrusions and attacks. The DOD ensures secure operation of the DOD portion of cyberspace and depends on other USG departments and agencies to secure the portions of cyberspace under their authority.

(2) Within DHS, the National Cyber Security Division (NCSD) is tasked to protect the USG network systems from cyberspace threats. NCSD partners with government, industry, and academia, as well as the international community, to make cybersecurity a national priority and to reinforce that cybersecurity is a shared responsibility.

(3) The National Security Presidential Directive 54/Homeland Security Presidential Directive 23, issued on 2 January 2008, established the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI formalizes a series of continuous efforts to further safeguard Federal systems from cyberspace threats. Under the CNCI, DHS has the lead in a number of areas, to include:

(a) Establish a frontline defense to reduce current vulnerabilities and prevent intrusions.

(b) Defend against the full spectrum of threats by using intelligence and strengthening supply chain security.

4. Legal Considerations

a. DOD must conduct CO consistent with US domestic law, applicable international law, and relevant USG and DOD policies. The legal framework applicable to CO depends on the nature of the activities to be conducted, such as offensive or defensive military operations; DSCA; service provider actions; LE and CI activities; intelligence operations; and defense of the homeland. Before conducting CO, commanders, planners, and operators must understand the relevant legal framework in order to comply with laws and policies, the application of which may be challenging given the ubiquitous nature of cyberspace and the often geographic orientation of domestic and international law. National Guard forces in Title 32, USC, status and state active duty status are not subject to the Posse Comitatus Act (PCA), and therefore may provide support without regard to the PCA. It is essential that commanders, planners, and operators consult with legal counsel during planning and execution of CO.

b. **Application of the Law of War.** It is DOD policy that members of DOD comply with the law of war during all armed conflicts, however such conflicts are characterized, and in all other military operations. The law of war is defined as that part of international law that regulates the conduct of armed hostilities. It encompasses all international law for the conduct of 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, unnecessary suffering, proportionality, and distinction (discrimination), which will apply to CO.

For more information on the law of war, see JP 1-04, Legal Support to Military Operations, *and CJCSI 5810.01D,* Implementation of the DOD Law of War Program.

c. **Lawful Military Attacks.** Military attacks will be directed only at military targets. Only a military target is a lawful object of direct attack. By their nature, location, purpose, or use, military targets are those objects whose total or partial destruction, capture, or neutralization offers a direct and concrete military advantage.

CHAPTER IV
PLANNING AND COORDINATION

> *"Alongside this nuclear danger is an entirely new kind of threat we have to be better prepared to confront – the threat of cyber[space] attacks. Cyber[space] has become a major concern as we face large numbers of attacks from non-state actors and large nations alike, and the prospect of a catastrophic disruption of critical infrastructure that would cripple our nation. The potential to paralyze this country from a cyber[space] attack is very real."*
>
> **Secretary of Defense Leon Panetta, October 2011**

1. Joint Operation Planning Process and Cyberspace Operations

a. Commanders integrate cyberspace capabilities at all levels and in all military operations. Plans should address how to effectively integrate cyberspace capabilities, counter an adversary's use of cyberspace, secure mission critical networks, operate in a degraded environment, efficiently use limited cyberspace assets, and consolidate operational requirements for cyberspace capabilities. The JFC will typically provide initial planning guidance which may specify time constraints, outline initial coordination requirements, authorize movement of key capabilities within the JFC's authority, and direct other actions as necessary. If requested by the JFC, CDRUSSTRATCOM may direct CDRUSCYBERCOM to provide assistance in integrating cyberspace forces, capabilities, and considerations into the JFC's plans and orders.

b. JP 5-0, *Joint Operation Planning,* states "Joint operation planning process (JOPP) provides a proven process to organize the work of the commander, staff, subordinate commanders, and other partners, to develop plans that will appropriately address the problem to be solved. It focuses on defining the military mission and development and synchronization of detailed plans to accomplish that mission." CO capability considerations and options are integrated into JOPP, just like all other joint capabilities and functions.

For more information on the JOPP, see JP 5-0, Joint Operation Planning.

2. Cyberspace Operations Planning Considerations

a. CO planners are presented the same considerations and challenges that are present in planning for other joint capabilities and functions, as well as some unique considerations. Targeting, deconfliction, commander's intent, political/military assessment, and collateral effects considerations all play into the calculations of the CO planner's efforts. In a similar fashion, all of the principles of joint operations, such as maneuver and surprise, are germane to CO. However, second and higher order effects in and through cyberspace can be more difficult to predict, necessitating more branches and sequels in plans. Further, while many elements of cyberspace can be mapped geographically in the physical domains, a full understanding of an adversary's posture and capabilities in cyberspace involves understanding the underlying network infrastructure, a clear understanding of what friendly forces or capabilities might be targeted and how, and an understanding of applicable domestic, foreign, and international laws and policy. Adversaries in cyberspace may be nation states, groups, or individuals, and the parts of cyberspace they control are not necessarily either within the geographic borders associated with the actor's nationality, or proportional to the actor's geopolitical influence. A criminal element, a politically motivated group, or even an individual may have a greater presence and capability in cyberspace than many nations do today. Regardless of what operational phase may be underway, it is always important to determine what authorities are required to execute CO. Cyberspace planners must account for the lead time to acquire the authorities needed to implement the desired cyberspace capabilities. This does not change the JFC's planning fundamentals, but does emphasize the importance of coordination with interagency partners, who may have authorities that are different from DOD. Despite the additional considerations and challenges of integrating CO in JFC planning, planners can use many elements of the traditional processes to implement the JFC's intent and guidance.

b. **Cyberspace-Related Intelligence Requirements (IRs).** During mission analysis, the joint force staff identifies significant gaps in what is known about the adversary and other relevant aspects of the OE and formulates IRs. IRs are general or specific subjects upon which there is a need for the collection of information or the production of intelligence. Based on the command's IRs, the intelligence 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 may include: network infrastructures, personnel status and readiness of adversaries' equipment, and unique cyberspace signature identifiers such as software/firmware versions, configuration files, etc.

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

(1) **Requests for Information (RFIs).** Cyberspace planners can submit an RFI to generate intelligence collection efforts in support of CO support to JOPP. RFIs respond to customer requirements, ranging from dissemination of existing products through the integration or tailoring of on hand information to scheduling original production. The intelligence office translating the customer's requirement and the primary intelligence producer determine how best to meet the customer's needs. The information must be timely, accurate, and in a usable format.

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

(2) **Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) Architecture.** The DOD's global connectivity has enabled joint force collection managers to levy tasking against all-source intelligence assets and resources, and submit tasking, collection, and production requirements directly to the appropriate CCDR. Further, collection databases can be leveraged via reachback to retrieve current and historical products. However, much of the TCPED may occur outside the theater because the sheer volume of requirements for first and second phase exploitation may quickly overwhelm in-theater assets.

c. **Targeting.** The purpose of targeting is to integrate and synchronize fires (the use of available weapon systems 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. The overall joint targeting cycle and target development process are described in JP 3-60, *Joint Targeting.* However, three aspects of CO should be included in the JFC's targeting processes: recognizing that cyberspace capabilities are a viable option for engaging designated joint targets; understanding that a CO option may be preferable in some cases; and first, second, and third order effects on joint targets may involve or affect elements of the DODIN. Additionally, there are some characteristics unique to cyberspace targets and cyberspace capabilities that are described below.

For additional information on joint targeting, see JP 3-60, Joint Targeting.

(1) **Characteristics of Targets in Cyberspace.** Every target has distinct intrinsic or acquired characteristics. These characteristics form the basis for target detection, location, identification, target value within the adversary target system, and classification for future surveillance, analysis, strike, and assessment. As discussed in Chapter I, "Introduction," cyberspace can be viewed as consisting of three layers: physical network, logical network, and cyber-persona. The challenge in targeting is to identify, coordinate, and deconflict multiple activities occurring across multiple layers.

(a) The *physical network* layer is the medium where the data travels. It includes wired (land and submarine cable) and wireless (radio, radio-relay, cellular, satellite) transmission means. It is the first point of reference for determining jurisdiction and application of authorities. It is also the primary layer for geospatial intelligence, which can also contribute useful targeting data in cyberspace.

(b) The *logical network layer* constitutes an abstraction of the physical network layer, depicting how nodes in the physical dimension of the information environment logically relate to one another to form entities in cyberspace. The logical network layer is the first point where the connection to the physical dimension of the information environment is lost.

(c) The *cyber-persona layer*, an individual's or groups' online identity(ies), holds important implications for joint forces in terms of positive target identification and affiliation, and activity attribution. Because cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form, significant intelligence collection and analysis capabilities are required for the joint forces to gain sufficient insight and SA of a cyber-persona to enable effective targeting and creation of the JFC's desired effects.

(2) **Characteristics of Cyberspace Capabilities.** Cyberspace capabilities must operate and create effects within the complex and ever-changing systems in cyberspace; however, they are each developed with certain environmental assumptions and expectations about the operating conditions that will be found in the target environment. The extent to which the expected environmental conditions of a cyberspace target cannot be confirmed

through intelligence sources represents an increased level of risk associated with using the capability. Cyberspace capabilities that have the fewest environmental dependencies and/or allow the operator to reconfigure the capability on-the-fly are preferred. Department of Defense Instruction (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.

(3) **Cascading and Collateral Effects.** Overlaps between military, civil, government, private, and corporate activities on shared networks in cyberspace make the evaluation of probable cascading and collateral effects particularly important when planning for CO. Due to policy concerns, an EXORD or applicable ROE may limit CO to only those operations that result in no or low levels of collateral effects. A collateral effects analysis to meet policy limits is separate and apart from the proportionality analysis required by the law of war. Even if a proposed CO is permissible after a collateral effects analysis, the proposed CO must also be permissible under a law of war proportionality analysis.

For more information see JP 3-60, Joint Targeting.

(4) **Target Nomination and Synchronization.** Component commanders, national agencies, supporting commands and/or the JFC staff submit target development nominations to the JFC targeting staff for development and inclusion on the JFC's joint target list (JTL). Once identified on the JTL, targets can be selected for engagement by organic assets (if within a component commander's assigned area of operations) or nominated for action by other joint force components and other organizations, usually via a coordinating body (joint fires element [JFE] of the operations directorate of joint staff) or working group (joint targeting working group [JTWG]). The JFE normally holds a JTWG for prioritization of the nominated targets through a draft joint integrated prioritized target list (JIPTL) and establishment of the "cut line." The "cut line" simply reflects an estimate of resources available to take action against targets in priority order and does not guarantee that a specific target will be attacked. The joint targeting coordination board (JTCB) provides a senior-level forum in which all components can articulate strategies and priorities for future operations to ensure that they are synchronized and integrated. Although most targeting issues are worked out at the JTWG, the JTCB normally conducts final coordination of the JIPTL and submits it for JFC approval. The JFE also maintains the restricted target list and no-strike list. The no-strike list contains objects or entities that are not legal targets, while, the restricted target list is constrained by the JFC for other reasons characterized as protected from the effects of military operations under international law and/or the rules of engagement.

For additional details on vetting, validation, and JTWGs, refer to JP 3-60, Joint Targeting, *and CJCSI 3370.01,* Target Development Standards.

(5) **Time-Sensitive Targeting**

(a) A time-sensitive target (TST) is a target of such high priority to friendly forces that the JFC designates it as requiring immediate response because it poses (or will soon pose) a danger to friendly forces, or it is a highly lucrative, fleeting target. TSTs are normally executed dynamically; however, to be successful, they require considerable deliberate planning and preparation within the joint targeting cycle. TSTs that are engaged through CO require detailed joint, cross-CCMD, interagency, and likely multinational planning and coordination of OPE, engagement, assessment, and intelligence efforts.

(b) The actual prosecution of a TST through cyberspace requires that cyberspace planners and operators coordinate with the supported commander early in the planning phase to ensure access to the target is available when the fleeting opportunity arises. In addition, JFCs should establish procedures to quickly promulgate execution orders for CO-engaged TSTs, which due to their unique cyberspace interagency deconfliction/coordination requirements may involve coordinating pre-approval for specific actions conducted under specific circumstances. Likewise, successful prosecution of TSTs requires a well-organized and well-rehearsed process for sharing sensor data and targeting information, identifying suitable strike assets, obtaining mission approval, and rapidly deconflicting weapon employment. The key for success is performing as much coordination and decision making as possible in advance.

For more information on attacking TSTs, see JP 3-60, Joint Targeting.

d. Target nomination processes remain unchanged when addressing CO and should be leveraged appropriately by planners. Development of target folders must include characteristics of the target as it relates to cyberspace. Development of this data is imperative to understand and characterize the cyberspace element and its relevancy. Also, this data allows the planner to develop and match an appropriate effect to be created against a particular target through cyberspace fires.

e. **DOD Information Network Operations.** The US military's reliance on cyberspace is well understood by our adversaries. DODIN operations underlie nearly every aspect of the JFC's operations, throughout the OE, however, it is often overlooked as a planning consideration. JFC planning to ensure DODIN resiliency in the face of cyberspace threats is essential. Besides physical protection of key cyberspace infrastructure, the JFC's primary defense-in-depth in cyberspace is DODIN operations which includes IA, configuration control and secure architectures, intrusion detection, bandwidth management/spectrum management, data encryption, and operating and maintaining the associated hardware (routers, receivers, switches, etc.). The GCC's JCCs must coordinate and deconflict these activities with USSTRATCOM via the USCYBERCOM CSE, where their effects transcend the AOR.

(1) **Situational Awareness.** Cyberspace SA 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. DODIN operations activities are the foundation of cyberspace SA, therefore, DODIN operations are fundamental to the commander's SA of the OE. A commander continually assesses the OE through a combination of staff element and other reporting; personal observation; intelligence, to include threat I&W; and representations of various activities occurring in the JOA through a COP. Sustainment of these communication channels, data feeds, and user interfaces is one of the key functions of DODIN operations. Accurate and comprehensive SA is critical for rapid decision making in

a constantly changing OE and engaging an elusive adaptive adversary. SA of adversary CO relies heavily on SIGINT, but contributions can come from all sources of intelligence. SA of friendly cyberspace is provided today by the Services and agencies operating their portions of the DODIN, DISA, through the theater NETOPS centers, to the CCMD theater/global NETOPS control centers, USCYBERCOM Joint Operations Center, Joint Functional Component Command for Space's Joint Space Operations Center, and their Service/agency leadership. They coordinate with each other as required to ensure operational effectiveness.

(2) **Sustainment, Remediation, and Recovery.** JFC mission-essential tasks to support DODIN operations include:

(a) Monitor and protect network capabilities in support of joint operations.

(b) Prioritize network assets for defense and recovery of JFC cyberspace capabilities (e.g., critical systems for priority restoral, alternative paths, backups).

(c) Assess operational impact of network disruptions and identify alternatives.

(d) Respond to network outages/intrusions/attacks.

(e) Dynamically reallocate network traffic to meet bandwidth and data priority requirements and mitigate attacks or other deleterious events.

3. Command and Control of Cyberspace Operations

a. Clearly established command relationships are crucial for ensuring timely and effective employment of forces. As authorized by CDRUSSTRATCOM, CDRUSCYBERCOM manages day-to-day global CO. Typically, CO require coordination between theater and global operations, creating a dynamic C2 environment. CO are integrated and synchronized by the supported commander into their CONOPS, detailed plans and orders, and specific joint offensive and defensive operations. The GCC is generally the supported commander for CO with first order effects with their AOR. Similarly, CDRUSSTRATCOM/CDRUSCYBERCOM is generally the supported commander at the global or transregional (across AOR boundaries) level. C2 of DODIN operations and DCO may require pre-determined and preauthorized actions based on meeting particular conditions and triggers, executed either manually or automatically if the nature of the threat requires instantaneous response. The JFC and planners should understand these command relationships, how they are derived and employed, and when necessary, how to deconflict them without compromising other operations. Forces conducting CO may simultaneously support multiple users. This requires extensive coordination, planning, and early integration of requirements and capabilities. Supported and supporting commanders coordinate, as appropriate, the deployment and employment of forces conducting CO required to accomplish the assigned mission. Some CO forces may be geographically separated from a particular supported theater of operations. Such cases require all involved commanders to take extra measures to ensure the supported commander is continuously aware of the remote supporting forces' operational status.

b. Forces providing global CO capabilities may need to support multiple CCMDs nearly simultaneously. Reachback to these capabilities allows faster adaptation to rapidly changing needs. At the same time, GCCs must be able to effectively conduct theater CO in order to operate and defend tactical and constructed networks. They must also be able to synchronize cyberspace activities related to accomplishing their operational objectives. In order to do that, some CO capabilities supporting synchronization may need to be forward deployed. However, CCMDs should retain knowledge and expertise required to support effective reachback within the CCMD, typically through the CCMD's JCC.

c. The Transitional Cyberspace Operations Command and Control (C2) Concepts of Operations (CONOPS) provides an interim framework (see Figure IV-1) to standardize cyberspace C2 mechanics and allow a more studied approach to achieve an enduring C2 architecture that defines global, regional, and functional cyberspace operational lanes; enables unity of effort; and allows CCMDs to use current authorities to conduct timely operations. The C2 CONOPS stresses the need for partnership among all DOD organizations conducting operations across the three cyberspace LOOs of: DODIN operations, DCO, and OCO.

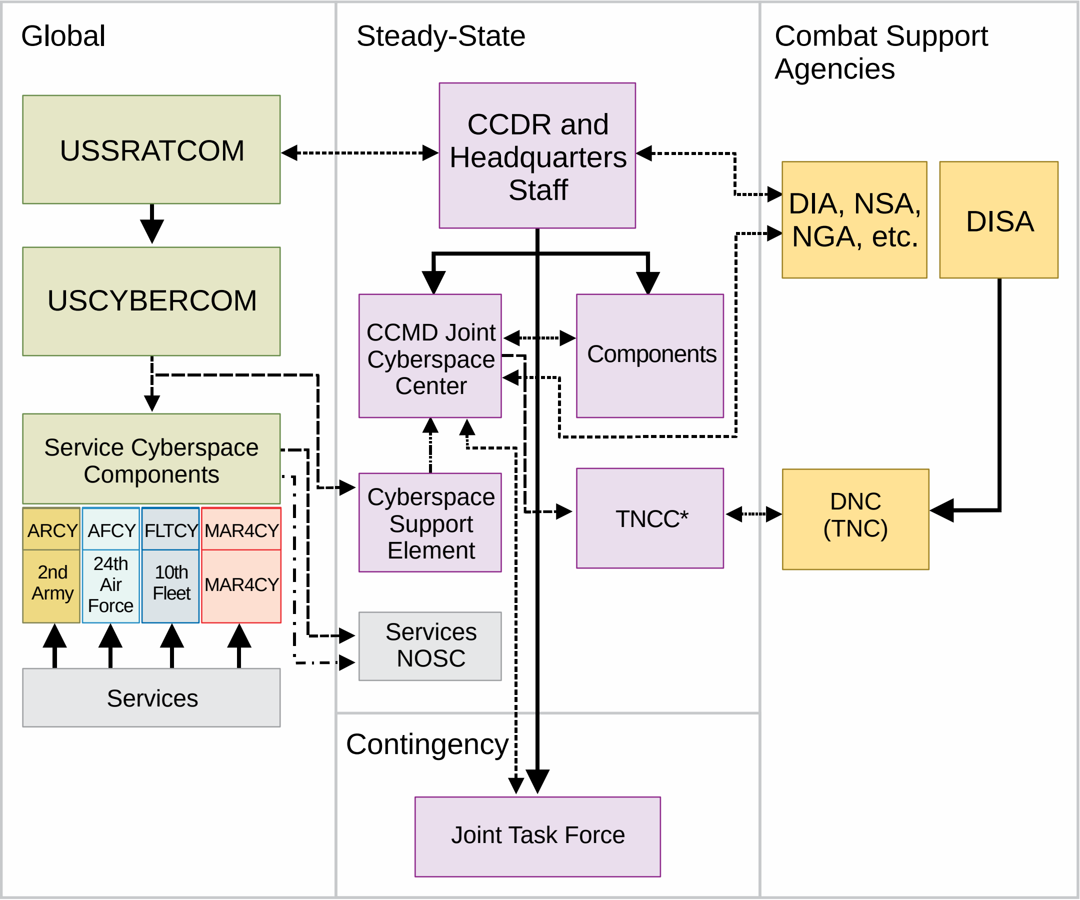
(1) CCDRs should size and structure the JCC to best support mission and CCMD requirements. CCMDs, through their JCC, supported by the CSE coordinate CO requirements and capabilities throughout their planning, operations, intelligence, targeting, and readiness processes in order to integrate and synchronize CO with all other military operations. Additionally, in partnership with USSTRATCOM, the JCC engages and coordinates regionally with interagency and multinational partners (as necessary). The JCC will:

(a) Combine inputs from USCYBERCOM with information about CCMD tactical and/or constructed networks to provide a regional/functional SA/COP tailored to CCMD requirements.

(b) Facilitate, 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 or DOD information networks. As early as possible in the planning process, provide USCYBERCOM with sufficient information about CCDR planned CO to enable deconfliction with USG CO.

(2) CSEs are organized to meet individual CCMD requirements and facilitate and coordinate all three cyberspace LOOs. The dual function of the CSE, as a forward element of USCYBERCOM, provides direct support to CCMDs and enables USCYBERCOM to support centralized, global CO. CSEs provide reachback for support from USCYBERCOM and its Service components, bridging theater/tactical and global/national cyberspace forces and operations.

Cyberspace Command and Control Organizational Construct



*Representational of JCC's relationship with DISA's sub-element.

Legend

ADCON	administrative control
AFCY	Air Forces Cyber Command
ARCY	Army Cyber Command
CCDR	combatant commander
CCMD	combatant command
COCOM	combatant command (command authority)
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNC	DISA network center
FLTCY	Fleet Cyber Command
JCC	joint cyberspace center
MAR4CY	Marine Corps Forces Cyberspace Command
NGA	National Geospatial-Intelligence Agency
NOSC	network operations and security center
TNCC	theater network coordination center
NSA	National Security Agency
OPCON	operational control
TACON	tactical control
TNC	theater network center
USCYBERCOM	United States Cyberspace Command
USSTRATCOM	United States Strategic Command

◄━━━━► COCOM
◄- - - - -► OPCON
◄·········► TACON
◄-·-·-·-► ADCON
◄·········► supporting
◄··-··-··► direct support

Figure IV-1. Cyberspace Command and Control Organizational Construct

d. For a subordinate force, the specific cyberspace element to support the force will be determined by the establishing CCDR and the JFC in coordination with USCYBERCOM.

e. Operations ENDURING FREEDOM, ALLIED FORCE, and UNIFIED PROTECTOR highlight that the US military will likely enter into conflict as part of a joint or multinational force. Planning for the specific C2 elements desired by the JFC will depend on the type and scale of the operation, the cyberspace presence or sophistication of the adversary, and the types of cyberspace targets identified. Regardless of what elements are established, the overlaps between global and theater missions in cyberspace, and the constraints and restraints on personnel conducting CO necessitate close coordination between the CCDR, CDRUSSTRATCOM, and other allied and interagency partners for the effective synchronization of CO.

4. Synchronization of Cyberspace Operations

The pace of CO requires significant pre-operational collaboration, as well as constant vigilance upon initiation, to ensure that activities in cyberspace and throughout the OE are coordinated and deconflicted in advance. One key to this is maintaining cyberspace SA and assessing the potential impacts to the joint force of any planned CO, including security posture, changes in configuration, or observed I&W of adversary activity. Planners and operators must also understand how operations within the OE may impact the JFC's CO efforts, and vice versa. Fire support coordination measures are a method that the joint force plans and uses in the air, land, and maritime domains which facilitate the rapid engagement of targets and simultaneously provide safeguards for friendly forces. Deconfliction and coordination efforts in or through cyberspace should include similar measures:

a. Deconfliction of the JFC's intended OCO, their activities, and the techniques planned to create these effects with other commands and agencies that may have equities in the same area of cyberspace is required. From a technical and operational perspective, deconfliction requires detailed analysis of each of the capabilities whose interoperability is being considered, as well as that of the target environment, to ensure the desired effects are achieved without unintended consequences. Additionally, the timelines required for analysis and coordination should be considered and included in the plan.

b. Planners should maintain awareness of the EMS and its impact on mobile devices and wireless networks, including cellular, wireless local area network, Global Positioning System, and other commercial and military uses of the EMS. CO and EA, to include offensive space control, must be deconflicted. Uncoordinated EA may significantly impact OCO utilizing the EMS. Depending upon power levels, the terrain in which they are used, and the nature of the system being targeted, unintended effects of EA can also occur outside of a local commander's AOR just as second order effects of CO may occur outside the AOR.

c. Minimizing vulnerabilities to the joint force caused by cyberspace applications. Coordinated joint force operations benefit from the use of various applications, including Web sites used for public affairs and strategic communication. Forward deployed forces also use the Internet, mobile phones, and instant messaging for logistics, morale purposes, and to communicate with friends and families. These DOD classified and unclassified networks are targeted by myriad actors, from foreign nations to malicious insiders. The JFC must work with DISA, the Services, and USSTRATCOM/USCYBERCOM as well as assigned forces to limit the threat to US and partner nations' networks. Several areas of concern exist for the JFC:

(1) Insider threats are one of the most significant threats to the joint force. Because insiders have a trusted relationship with access to the DODIN, any malicious activity can be much more far reaching than external entities attempting to gain access. 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 must consider risk mitigation measures for this threat, such as reinforcing training of the joint force to be alert for suspicious insider activity.

(2) Internet-based capabilities, including e-mail, social networking, and Web sites are used for both official and unofficial purposes and pose security risks that are not fully understood. The security risks of Internet-based capabilities are often obscured and mitigation of these risks is limited, due to the nongovernmental ownership of the majority of the supporting information systems or sites. These IA and OPSEC concerns, combined with bandwidth requirements of Internet applications, create an imperative for the JFC to be aware of and actively manage the impact of Internet-based capabilities.

(3) Cross-domain solutions between systems classified at different levels complicate cryptographic and other security support considerations, and should be included in planning consideration. These 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 coerce end-users into poor security practices. Likewise, emergent tasking for information sharing can exert pressure on network managers to build ad hoc networks over existing commercial infrastructure, or connect non-DOD US and partner networks without adequate security controls. USSTRATCOM and USCYBERCOM will work with JFCs to develop appropriate technical solutions and detailed security policies to address these needs. Planners should include requirements for early coordination to ensure that appropriate security features are included that meet the JFCs needs.

(4) CO also need to be deconflicted and synchronized with STO. Information related to STO and its contribution to CO can be obtained from the STO planners at CCMD or Service component headquarters.

5. Assessment of Cyberspace Operations

a. Assessment is a process that measures progress of the joint force toward mission accomplishment. The focus is on measuring progress toward the end state and delivering relevant reliable feedback into the planning process to adjust operations during execution. Assessment involves deliberately comparing forecasted outcomes with actual events to determine the overall effectiveness of force employment. More specifically, assessment helps the commander determine progress toward attaining the desired end state, achieving objectives, or performing tasks. Commanders continuously assess the OE and the progress of operations and compare them to their initial vision and intent. Based on their assessment, commanders adjust operations to ensure objectives are met and the military end state is achieved. Appendix D, "Assessment," of JP 5-0, *Joint Operation Planning*, describes the assessment process in detail. Additional assessment process information can be found in Appendix F, "The Assessment Process," of JP 3-60, *Joint Targeting.*

For more information on BDA and munitions effectiveness assessment, see JP 3-60, Joint Targeting*, and Defense Intelligence Agency Publication DI-2820-4-03,* Battle Damage Assessment (BDA) Quick Guide.

(1) *Measures of Effectiveness (MOEs).* MOEs are used to assess changes in system behavior, capability, or the OE. They measure the attainment of an end state, achievement of an objective, or creation of an effect. When expressed quantitatively, MOEs generally reflect a trend or show progress toward a measurable threshold. While MOEs may be harder to derive than measures of performance (MOPs) for a discrete task, they are nonetheless essential to effective assessment.

(2) *MOPs*. 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.

For more information on assessment, see JP 5-0, Joint Operation Planning, *and JP 3-60,* Joint Targeting. *Each publication describes the assessment process in detail and includes an appendix on the subject.*

b. **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, objectives and desired effects are developed by the JFC's staff and are used to develop tasks to subordinates. Subordinate staffs use the assigned tasks to develop tactical-level objectives, tasks, subordinate targeting objectives and effects, and plan tactical actions and MOPs/MOEs for those actions. Tactical actions typically must 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 will be used to conduct an operational level assessment which in turn supports the strategic level assessment (as required).

(2) Operational MOPs/MOEs avoid tactical information overload by providing commanders a shorthand method of tracking tactical actions and maintaining SA. MOPs and MOEs must be clearly definable and measurable, should be selected to support and enhance the commander's decision process, and guide future actions toward achieving objectives and end states.

(3) CO are a recent addition in the development of operational level MOPs/MOEs. In some cases, activities in cyberspace alone will have operational level effects; for example, the use of a cyberspace attack to bring down or corrupt the adversary

headquarters network could very well reverberate through the entire JOA. A CO option may be preferable in some cases.

(4) Assessments in cyberspace may be unique in that the normal assessment cell will not typically have the capabilities or expertise to assess CO; CO will typically involve multiple commands, such as the supported JFC, CDRUSCYBERCOM, and possibly other functional supporting JFCs. Additionally, with CO typically being conducted as part of a larger operation, assessment of CO will need to be conducted in the context of supporting the overarching JFC objectives. Therefore, CO assessments will require close coordination within each staff and across multiple commands. Coordination and federation of the assessment efforts will often require arrangements that need to be in place prior to execution.

c. **Navigation Warfare Considerations in CO Planning.** CO produces NAVWAR effects by assuring friendly access and/or denying enemy access to positioning, navigation, and timing information transmitted by global navigation satellite system (GNSS) or other radio navigation aid signals. Creation of global and theater NAVWAR effects is attained through the coordinated employment of CO, EW, and space operations.

6. Interorganizational Considerations

a. JFCs begin to coordinate and, when appropriate, integrate their activities with other agencies before and during joint operation planning. Integrating the interagency community effectively is vital to successful military operations, especially during theater shaping, stability, and transition to civil authority phases of an operation. Just as JFCs and their staffs must consider how the capabilities of other USG and nongovernmental organizations (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. Through JS and USCYBERCOM, JFCs should coordinate with interagency representatives during planning to 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, must ensure any interagency support required outside the AOR is fully coordinated 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. At the operational level, commanders should consider and integrate interagency capabilities into their estimates, plans, and operations that interagency partners can realistically commit to the effort.

c. Military leaders must work with the other members of the national security team to promote unified action. A number of factors can complicate the coordination process, including the agencies’ different and sometimes conflicting policies, legal authorities, roles and responsibilities, procedures, and decision-making processes. The JFC must ensure that interagency planners clearly understand military capabilities, requirements, operational limitations, liaison, and legal considerations. Additionally, planners should understand the nature of this relationship and the types of support interagency partners can provide. In the absence of a formal command structure, JFCs may be 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 can 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, 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 assigned to the CCDR's staff. The JIACG establishes regular, timely, and collaborative working relationships between civilian and military operational planners providing a CCDR with the capability to collaborate at the operational level with USG civilian agencies and departments. JIACG members participate in contingency, crisis action, and security cooperation planning. Additionally, they provide a collaborative conduit back to their parent organizations to help synchronize joint operations with the efforts of nonmilitary organizations.

e. **Planning and Coordination with Other Agencies.** A supported commander is responsible for developing interagency coordination requirements and mechanisms for each OPLAN. The JFC should supply the interagency partners with the capabilities that military planners have determined to be required and the shared understanding of the situation and common activities required to achieve the objective. This enables interagency planners to more rigorously plan their efforts in concert with the military, to suggest other activities or partners that could contribute to the operation, and to better determine any support requirements.

7. Multinational Considerations

a. Collective security is a strategic goal of the US, and joint operation planning will frequently be accomplished within the context of operation 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 must accommodate and complement such protocols and plans. JFCs must also anticipate and incorporate planning factors such as domestic and international laws, regulations, and operational limitations on the use of various weapons and tactics.

b. When working within a multinational task force, each country and Service can expect to be tasked by the commander with the mission(s) most suited to their particular capabilities. CO planning, coordination, and execution items that must be considered when a multinational force campaign or OPLAN is developed include:

(1) National agendas for each country of the multinational force may differ significantly from those of the US, creating potential difficulties in determining the CO objectives.

(2) Differing national standards and laws pertaining to sovereignty in cyberspace may affect willingness or the legality of their participation in certain CO. These differences may be reflected in policies or capabilities that are either narrower or broader than those of the US.

(3) In a US-led multinational force, countries without established CO doctrine may need to be advised of the benefits of CO and assisted in integrating CO into the planning process.

(4) Nations in a multinational force will often require approval of the CO portion of plans and orders from higher authority, which may significantly impede CO implementation. Additionally, this national-level approval requirement increases potential constraints and restraints upon the participating national forces, and further lengthens the time required to gain national approval for their participation. Commanders and planners should be particularly sensitive to national agendas and anticipate the additional time required for approval through this parallel national command structure.

(5) Security restrictions may prevent full disclosure of individual CO plans and orders with multinational partners; this may severely hamper cyberspace synchronization efforts. Therefore, the JFC's staff should obtain approval for information sharing among partners, and then issue specific guidance on the release of classified US material to the multinational force 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 for appropriate information sharing across the force.

(6) There will often be IT hardware and software incompatibilities that 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 DCO efforts.

(7) To effectively conduct multinational operations, multinational partners require appropriate access to systems, services, and information. The US joint force strives to provide necessary and appropriate access and support at the lowest appropriate security classification level. Commanders involved in multinational operations can enable this shared access by engaging proper authorities early in the process to determine appropriate access levels, necessary services, and satisfactory means for expediting the process for foreign disclosure of appropriate intelligence information.

c. **Integration.** In support of each multinational force, a hierarchy of bilateral or multilateral bodies is established to define objectives, develop strategies, and to coordinate strategic guidance for planning and executing multinational operations. The same is true for CO. Through dual involvement in national and multinational security processes, US national leaders integrate national and theater strategic CO planning with that of the multinational force whenever possible. Within the multinational structure, US participants ensure that objectives and strategy complement US interests and are compatible with US capabilities. Within the US national structure, US participants ensure that international commitments are reflected in national military strategy and are adequately addressed in strategic guidance for joint operation planning. Planning with intergovernmental organizations and NGOs is often necessary, particularly if CO supports foreign humanitarian assistance, peace operations, and other stability operations. Incorporating NGOs and their capabilities into the planning process requires the JFC and staff to balance NGOs' information requirements with OPSEC. 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 permissive environments.

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

For more information on multinational operations, see JP 3-16, Multinational Operations; *for more information on joint planning, see JP 5-0,* Joint Operation Planning.

Intentionally Blank

APPENDIX A
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. Director of Central Intelligence Directive 7/3, *Information Operations and Intelligence Community Related Activities.*

e. Goldwater-Nichols Department of Defense Reorganization Act of 1986.

f. Executive Order 12333, US Intelligence Activities.

g. Transitional Cyberspace Operations Command and Control (C2) Concept of Operations (CONOPS).

2. Strategy and Policy Documents

a. *Department of Defense Strategy for Operating in Cyberspace.*

b. *International Strategy for Cyberspace* (May 2011).

c. *Unified Command Plan.*

d. The National Military Strategy for Cyberspace Operations (NMS-CO).

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

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

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

h. *National Infrastructure Protection Plan.*

i. *Defense Strategic Guidance.*

3. Office of the Secretary of Defense Guidance

Secretary of Defense Memorandum, *Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations.*

4. Department of Defense

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

b. DODD 5205.15E, *DOD Forensic Enterprise.*

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

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

e. DODD 8500.01E, *Information Assurance (IA).*

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

g. DODI 8410.02, *NETOPS for the Global Information Grid (GIG).*

h. DODI O-3600.02, *Information Operations* (*IO) Security Classification Guidance.*

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

j. DODI O-8530.2, *Support to Computer Network Defense*.

k. DODD O-8530.1, *Computer Network Defense.*

5. Chairman of the Joint Chiefs of Staff

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

b. CJCSM 3122.08A, *IJSTO Supplement to Joint Operation Planning and Execution System, Volume II.*

c. CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces.*

d. CJCSI 3210.01B, *Joint Information Operations Policy*.

e. CJCSI 3370.01, *Target Development Standards.*

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

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

h. CJCSM 6510.01A, *Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program).*

6. Joint Publications

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

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

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

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

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

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

g. JP 3-07, *Stability Operations.*

h. JP3-08, *Interorganizational Coordination During Joint Operations.*

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

j. JP 3-13.1 *Electronic Warfare Operations.*

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

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

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

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

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

p. JP 3-28, *Civil Support.*

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

r. JP 5-0, *Joint Operation Planning.*

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

7. Service Publications

a. Air Force Doctrine Document 3-12, *Cyberspace Operations.*

b. United States Army Training and Doctrine Command Pamphlet 525-7-X, *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028.*

c. Naval Warfare Publication 3-63, Volume I, *Computer Network Operations.*

d. Field Manual (FM) 3-36, *Electronic Warfare in Operations*.

e. FM 3-09.32/MCWP 3-16.6A/NTTP 3-09.2/AFTTP 3-2.6, *Multi-Service Tactics, Techniques, and Procedures for the Joint Application of Firepower*.

8. Supporting Documents

a. CDRUSSTRATCOM CONPLAN, *Cyberspace Operations.*

b. CDRUSSTRATCOM *Operational Concept for Cyberspace.*

c. CDRUSSTRATCOM *Joint Concept of Operations for Global Information Grid NETOPS.*

d. USSTRATCOM: *US Cyber Command Implementation Plan*.

e. *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.

f. Director of Central Intelligence Directive (DCID) 7/3, *Information Operations and Intelligence Community Related Activities.*

APPENDIX B
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Joint Staff operational plans and interoperability directorate of a joint staff (J-7), Deputy Director, Joint and Coalition Warfighting, ATTN: Joint Doctrine Support Division, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and Joint Staff doctrine sponsor for this publication is the Joint Staff Director of Operations (J-3).

3. Redaction

This publication is a redacted version of JP 3-12, *Cyberspace Operations*, 5 February 2013, which is available on the classified Joint Electronic Library system.

4. Change Recommendations

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

To: JOINT STAFF WASHINGTON DC//J-3 DDGO/J-7-JEDD//

b. Routine changes should be submitted electronically to the Deputy Director, Joint and Coalition Warfighting Center, Joint Doctrine Support Division and info the lead agent and the Director for Joint Force Development, J-7/JEDD.

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

5. Distribution of Publications

Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified JPs must be IAW DOD Manual 5200.01, Vol. III, *DOD Information Security Program: Protection of Classified Information.*

6. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS at https://jdeis.js.mil (NIPRNET) and https://jdeis.js.smil.mil (SIPRNET).

b. Only approved JPs and joint test publications are releasable outside the CCMDs, Services, and Joint Staff. Release of any classified JP to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Defense Foreign Liaison/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, JS 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 CCMDs and Services.

GLOSSARY
PART I—ABBREVIATIONS AND ACRONYMS

AOR	area of responsibility
BDA	battle damage assessment
C2	command and control
CCDR	combatant commander
CCMD	combatant command
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CI	counterintelligence
CI/KR	critical infrastructure/key resources
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CNCI	Comprehensive National Cybersecurity Initiative
CNE	computer network exploitation
CO	cyberspace operations
CONOPS	concept of operations
CONPLAN	concept plan
COP	common operational picture
CSE	cyberspace support element
DCI	defense critical infrastructure
DCO	defensive cyberspace operations
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 networks
DSCA	defense support of civil authorities
EA	electronic attack
EMS	electromagnetic spectrum
EW	electronic warfare
EXORD	execute order
GCC	geographic combatant commander
GNSS	global navigation satellite system

I&W	indications and warning
IA	information assurance
IAW	in accordance with
IC	intelligence community
ICT	information and communications technology
IGL	intelligence gain/loss
IM	information management
IO	information operations
IP	internet protocol
IR	intelligence requirement
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
J-3	operations directorate of a joint staff
J-7	operational plans and interoperability directorate of a joint staff
JCC	joint cyberspace center
JFC	joint force commander
JFE	joint fires element
JIACG	joint interagency coordination group
JIPTL	joint integrated prioritized target list
JOA	joint operations area
JOPP	joint operation planning process
JP	joint publication
JS	the Joint Staff
JTCB	joint targeting coordination board
JTL	joint target list
JTWG	joint targeting working group
JWICS	Joint Worldwide Intelligence Communications System
LE	law enforcement
LOO	line of operation
MILDEC	military deception
MISO	military information support operations
MOE	measure of effectiveness
MOP	measure of performance
NAVWAR	navigation warfare
NCSD	National Cyber Security Division (DHS)
NGO	nongovernmental organization
NIPRNET	Nonsecure Internet Protocol Router Network
NMS-CO	National Military Strategy for Cyberspace Operations
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service

OCO	offensive cyberspace operations
OE	operational environment
OPE	operational preparation of the environment
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSD	Office of the Secretary of Defense
PCA	Posse Comitatus Act
PPD	Presidential policy directive
RFI	request for information
SA	situational awareness
SATCOM	satellite communications
SecDef	Secretary of Defense
SIGINT	signals intelligence
STO	special technical operations
TCPED	tasking, collection, processing, exploitation, and dissemination
TST	time-sensitive target
URL	uniform resource locater
USC	United States Code
USCYBERCOM	United States Cyber Command
USD(P)	Under Secretary of Defense for Policy
USG	United States Government
USSOCOM	United States Special Operations Command
USSTRATCOM	United States Strategic Command

PART II—TERMS AND DEFINITIONS

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

computer intrusion detection. None. (Approved for removal from JP 1-02.)

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

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

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 by an adversary. (Approved for inclusion in JP 1-02.)

defensive cyberspace operation response action. Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems. Also called **DCO-RA.** (Approved for inclusion in JP 1-02.)

defensive cyberspace operations. Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called **DCO.** (Approved for inclusion in JP 1-02.)

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

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

information assurance. Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. Also called **IA.** (Approved for incorporation into JP 1-02.)

offensive cyberspace operations. Cyberspace operations intended to project power by the application of force in or through cyberspace. Also called **OCO.** (Approved for inclusion in JP 1-02.)

JOINT

CHIEFS OF STAFF