Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

December 8, 2016

Defense Primer: Cyberspace Operations

Overview

The Department of Defense (DOD) has defined cyberspace as a 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. The DOD Information Network (DODIN) is a global infrastructure carrying DOD, national security, and related intelligence community information and intelligence.

Cyberspace operations are composed of the military, intelligence, and ordinary business operations of the DOD in and through cyberspace. Military cyberspace operations use cyberspace capabilities to create effects that support operations across the physical domains and cyberspace. Cyberspace operations differ from information operations (IO), which are specifically concerned with the use of information-related capabilities, such as military information support operations or military deception, during military operations to affect the decision making of adversaries while protecting our own. IO may use cyberspace as a medium, but it may also employ capabilities from the physical domains.

Cyberspace operations are categorized into the following:

- **Offensive Cyberspace Operations**, intended to project power by the application of force in and through cyberspace. These operations are authorized like operations in the physical domains.
- **Defensive Cyberspace Operations**, to defend DOD or other friendly cyberspace. These are both passive and active defense operations and are conducted inside and outside of DODIN.
- **DODIN Operations**, to design, build, configure, secure, operate, maintain, and sustain DOD communications systems and networks across the entire DODIN.

Cyber Strategy

In 2012, President Obama directed DOD to organize and plan to defend the nation against cyberattacks of significant consequence, in concert with other U.S. government agencies. The resulting DOD Cyber Strategy focuses on three primary cyber missions:

1. Defend DOD networks, systems, and information.
2. Defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence.
3. Provide cyber support to military operational and contingency plans.

Guided by this strategy document, DOD began to build a Cyber Mission Force (CMF) in 2012 to carry out DOD's cyber missions.

Cyber Mission Force

The Cyber Mission Force consists of 133 teams that are organized to meet DOD's three cyber missions. Specifically, Cyber Mission Force teams support these mission sets though their respective assignments:

- **Cyber National Mission Force** teams defend the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them.
- **Cyber Combat Mission Force** teams conduct military cyber operations in support of combatant commands.
- **Cyber Protection Force** teams defend the DOD information networks, protect priority missions, and prepare cyber forces for combat.
- **Cyber Support Teams** provide analytic and planning support to National Mission and Combat Mission teams.

Cyber Mission Force teams reached initial operating capability in October 2016. Currently comprising around 5,000 individuals, the cyber mission force is expected to grow to 6,200 by the end of 2018. Organizationally, the Cyber Mission Force is an entity of the United States Cyber Command.

United States Cyber Command

In response to the growing cyber threat, in 2009 the Secretary of Defense directed the establishment of a new military command devoted to cyber activities. USCYBERCOM is a sub-unified command, under the U.S. Strategic Command, whose stated mission is to "direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." Previously existing components, such as the Joint Task Force for Global Network Operations (JTF-GNO) and the Joint Functional Component Command for Network Warfare (JFCC-NW), were absorbed by USCYBERCOM and reorganized to provide centralized planning for cyberspace operations.

USCYBERCOM is commanded by a four-star general, who is also the director of the National Security Agency and chief of the Central Security Service. The commander manages day-to-day global cyberspace operations and leads defense and protection of DODIN. Each of the military services provides support to USECYBERCOM.

Military Service Components

Army Cyber Command: 2nd Army (ARCY)

Air Forces Cyber Command: 24th Air Force (AFCY)

Navy Fleet Cyber Command: 10th Fleet (FLTCY)

Marine Corps Forces Cyberspace Command: MAR4CY

Other Defense Components

Other entities within the DOD are tasked with a supporting or collaborative role in cyberspace operations.

National Security Agency

The National Security Agency (NSA) works closely with USCYBERCOM. NSA's two primary missions are information assurance for national security systems and signals intelligence. USCYBERCOM is co-located with the NSA at Fort Meade, MD.

Defense Information Systems Agency

The mission of the Defense Information Systems Agency (DISA) is to provide and ensure command and control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters across the full spectrum of military operations. The Director of DISA is responsible for the remediation of critical DODIN infrastructure issues.

Federal Role

The Department of Homeland Security (DHS) is the lead federal department for critical infrastructure protection and nonmilitary federal cybersecurity. According to the Cybersecurity National Action Plan, DHS is the lead federal agency for coordinating asset response activities. DOD is responsible for supporting the DHS coordination of efforts to protect the Defense Industrial Base (DIB) and the DODIN portion of the DIB. Together, the two are charged with defending the U.S. homeland and U.S. national interests against cyberattacks of significant consequence. The military cyber assets may be deployed in the event of a major cyberattack on U.S. critical infrastructure only when directed to do so.

Authorities

Title 10 of the *United States Code* is the authority under which the military organizes, trains, and equips its forces for national defense. Section 954 of the National Defense Authorization Act for Fiscal Year 2012 affirms that "the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and the War Powers Resolution."

Under Title 50, a "covert action" is subject to a presidential finding and Intelligence Committee notification requirements. 50 U.S.C. 3093 allows the President to authorize the conduct of a covert action if he determines such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the U.S. national security, which determination shall be set forth in a finding that shall be in writing, unless immediate action is required. The question of whether Title 10 or Title 50 applies to offensive cyberspace operations has been of particular interest to Congress with respect to its oversight duties, as they are subject to different reporting requirements. Title 10 *U.S. Code* Section 484 requires the Secretary of Defense to provide to the House and Senate Armed Services Committees quarterly briefings on all offensive and significant defensive military operations in cyberspace carried out by the Department of Defense during the immediately preceding quarter. Title 50 *U.S. Code* Section 3093 requires the Director of National Intelligence and all agencies involved in a covert action to keep the congressional intelligence committees fully and currently informed, and to furnish any information or material concerning covert actions (including the legal basis under which the covert action is being or was conducted).

Law of Armed Conflict in Cyberspace

Members of DOD must comply with the law of armed conflict or 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 United States or its individual citizens, including treaties and international agreements to which the United States is a party, and applicable customary international law. DOD policy states that the fundamental principles of the law of war will apply to cyberspace operations. These principles include military necessity, preventing or avoiding unnecessary suffering, proportionality, and distinction (discrimination).

Relevant Statute

Title 10, U.S. Code, *Armed Forces*, Section 111: Man, train, and equip US forces for military operations in cyberspace.

Title 50, U.S. Code, *War and National Defense*, Section 3093: Secure US interests by conducting military and foreign intelligence operations in cyberspace.

CRS Products

CRS Report R43848, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by Catherine A. Theohary

CRS Report R43955, *Cyberwarfare and Cyberterrorism: In Brief*, by Catherine A. Theohary and John W. Rollins

Other Resources

DOD. Joint Publication 3-13, *Cyberspace Operations*, February 5, 2013.

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

Catherine A. Theohary, ctheohary@crs.loc.gov, 7-0844

IF10537