Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 9, 2022

Defense Primer: Cyberspace Operations

Overview

The Department of Defense (DOD) defines 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 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 September 2018, the White House released a national cyber strategy consisting of four pillars: (1) protecting the American people, homeland, and way of life by safeguarding networks systems, functions and data; (2) promoting prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserving peace and security by strengthening the ability of the United States, its partners, and allies to deter and punish those who use cyber maliciously; and (4) advancing influence to extend the key tenets of an open, interoperable, reliable, and secure internet.

Following these pillars, DOD released its own cyber strategy outlining five lines of effort: (1) build a more lethal force; (2) compete and deter in cyberspace; (3) strengthen alliances and attract new partnerships; (4) reform the department; and (5) cultivate talent.

Three operational concepts identified in the DOD Cyber Strategy are to conduct cyberspace operations *to collect intelligence* and *prepare military cyber capabilities* to be used in the event of crisis or conflict, and *to defend forward* to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. Defending forward may involve a more aggressive active defense, meaning activities designed to disrupt an adversary's network when hostile activity is suspected.

Cyber Mission Force

DOD began to build a Cyber Mission Force (CMF) in 2012 to carry out DOD's cyber missions. The CMF 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 Teams** defend the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them.
- **Cyber Combat Mission Teams** conduct military cyber operations in support of combatant commands.
- **Cyber Protection 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.

CMF teams reached full operational capacity at over 6,200 individuals in May 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's stated mission is to "to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners." Elevated to a unified combatant command in May 2018, 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 USCYBERCOM.

Military Service Components

- **Army Cyber Command:** 2nd Army (ARCYBER)
- **Air Forces Cyber Command:** 24th Air Force (AFCYBER)
- **Navy Fleet Cyber Command:** 10th Fleet (FLTCYBER)
- **Marine Corps Forces Cyberspace Command:** MARFORCYBER)

Some services may reorganize their Cyber Commands into Information Warfare Commands or similarly named commands to emphasize the role of information.

Other Defense Components

Other entities within the DOD and the IC 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. 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. 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

Section 954 of the National Defense Authorization Act (NDAA) for FY2012 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." Section 1632 of the FY2019 NDAA affirms that DOD may conduct operations in cyberspace, including clandestine operations, short of hostilities or in areas in which hostilities are not occurring; it also states that a clandestine military activity or operation in cyberspace shall be considered a traditional military activity (TMA). Section 1642 of the FY2019 NDAA provides authority for DOD "to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter" in response to "an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes."

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. TMAs are excepted from this requirement. The FY2018 NDAA required notification of the use of cyber weapons and quarterly cyber operations briefings to the congressional Armed Services Committees.

The Obama Administration's classified Presidential Policy Directive 20 governed U.S. cyber operations policy, but it did not grant new authorities. According to the former officials, the document required interagency approval for significant cyber operations. In September 2018, the White House acknowledged replacing it with new guidance, National Security Presidential Memorandum 13, which is said to offer more authority to the commander of USCYBERCOM.

Law of Armed Conflict in Cyberspace

The law of war regulates the conduct of armed hostilities. It encompasses all international law binding on the United States, 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.

Relevant Statutes

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

Other Resources

DOD. Joint Publication 3-12, *Cyberspace Operations*, February 5, 2013.

DOD. *The Department of Defense Cyber Strategy,* September 2018.

Catherine A. Theohary, Specialist in National Security Policy, Cyber and Information Operations

IF10537

Disclaimer