

Updated November 29, 2024

Defense Primer: Cyberspace Operations

Overview

The Department of Defense (DOD) defines cyberspace as a global domain within the information environment (IE) consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Joint Publication (JP) 3-12, Joint Cyberspace Operations describes cyberspace operations as the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. 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 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 March 2023, the White House released a national cybersecurity strategy consisting of five pillars: (1) defend critical infrastructure; (2) disrupt and dismantle threat actors; (3) shape market forces to drive security and resilience; (4) invest in a resilient future; and (5) forge international partnerships to pursue shared goals.

In 2022, DOD issued a new, classified Cyber Strategy, superseding the unclassified 2018 DOD Cyber Strategy. The unclassified summary of the 2022 Strategy (released in 2023) maintains the previous strategy's emphasis on operations to defend forward, meaning to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. Defending forward may involve an aggressive active defense, meaning activities designed to disrupt an adversary's network when hostile activity is suspected. Four complementary lines of

effort are highlighted: to defend the nation; prepare to fight and win the nation's wars; protect the domain with allies and partners; and build enduring advantages in cyberspace.

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 through their respective assignments:

- **Cyber National Mission Teams** defend the nation by observing 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 (NSA) 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's Cyber Mission Force.

Military Service Components

United States Army: Army Cyber Command
United States Navy: Fleet Cyber Command/Tenth Fleet
United States Air Force: 16th Air Force/Air Forces Cyber
United States Marine Corps: Marine Corps Forces
Cyberspace Command

Other components include the Cyber National Mission Force (CNMF) and Joint Force Headquarters-DOD Information Networks (JFHQ-DODIN). The CNMF was elevated to a sub-unified combatant command in December 2022. Also in 2022, Congress granted USCYBERCOM enhanced budget authority to manage the planning, budgeting, and execution of resources for the US Cyber Force.

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 NSA works closely with USCYBERCOM, particularly given the dual-hatted nature of the Director. 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. The JFHQ-DODIN oversees the day-to-day operation of DOD's networks and actively defends the DODIN. The JFHQ-DODIN commander is dual-hatted as the director of DISA.

Assistant Secretary of Defense for Cyber Policy

Title 10 U.S.C. 138 established an Assistant Secretary of Defense for Cyber Policy (ASD-CP) in the Office of the Secretary of Defense to oversee DOD cyber policy and supervise budget review of cyber activities. The ASD-CP also serves as the Principal Cyber Advisor.

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 2012 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, classified guidance, National Security Presidential Memorandum 13, which reportedly offers 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 10, *U.S. Code, Armed Forces*, Section 394: Authorities concerning military cyber operations.

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

Other Resources

DOD. Joint Publication 3-12, *Cyberspace Operations*, December 2022.

DOD. *2023 Summary of the Cyber Strategy of the Department of Defense*, September 2023.

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

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.