Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 23, 2025

Defense Primer: U.S. Cyber Command (USCYBERCOM)

U.S. Cyber Command (commonly referred to as CYBERCOM), is the Department of Defense (DOD)—which is "using a secondary Department of War designation" under Executive Order 14347 dated September 5, 2025—functional unified combatant command (CCMD) responsible for cyberspace operations. The command defends DOD information systems, supports military commanders with cyberspace operations, and defends the United States from cyberattacks. In addition to defending against increasing adversarial attempts to compromise military, intelligence, and defense industrial base networks and critical infrastructure, CYBERCOM is focused on countering a wide array of malicious cyberspace activities.

Background

The origins of CYBERCOM can be traced to the late 1990s, when DOD efforts focused on network centric warfare and strengthening U.S. computer network operations—the precursor to cyberspace operations—through various task forces. The department later established a Joint Task Force for Global Network Operations (JTF-GNO) for defensive cyberspace operations and a Joint Force Component Command for Network Warfare (JFCC-NW) for offensive operations. Both task forces operated under U.S. Strategic Command (STRATCOM). Air Force officials also recognized the importance of cyberspace operations, declaring cyberspace an official Air Force domain in 2005 and initiating work to develop a new cyber command. In 2009, the Air Force established Air Forces Cyber and 16th Air Force as cyber-focused organizations.

On June 23, 2009, Robert Gates, then-Secretary of Defense (SECDEF), directed the creation of CYBERCOM, establishing the organization as a subordinate (or *sub*-) unified command under STRATCOM. Both the JTF-GNO and JFCC-NW were absorbed into the new command, with their missions moving from CNO to cyberspace operations. Initially, CYBERCOM received assistance from the National Security Agency (NSA), including personnel, equipment, and resources to perform its mission. The command reached full operational capability in 2010. In 2016, under Section 923 of the National Defense Authorization Act for Fiscal Year 2017 (NDAA; P.L. 114-328), Congress authorized establishing CYBERCOM as a unified CCMD. In 2017, the first Trump Administration directed that CYBERCOM "be elevated to the status of a Unified Combatant Command." Led by a four-star general or admiral, CYBERCOM is headquartered at Fort George G. Meade in Maryland. The commander is *dual-hatted* (i.e., simultaneously oversees two distinct organizations) and also serves as the Director of the National Security Agency (DIRNSA).

Mission and Organization

According to CYBERCOM, its mission is to "direct, synchronize, and coordinate cyberspace planning and operations—to defend and advance national interests—in collaboration with domestic and international partners." The command performs four assigned missions:

- Defend U.S. critical infrastructure and democratic processes from malicious cyberspace actors;
- Defend DOD Information Networks (DODIN);
- Integrate options and capabilities in CCMD campaigns and plans; and
- Increase DOD cyber effectiveness through collaboration with allies and partners.

Components.

CYBERCOM is organized into four service components that provide forces to the command: Army Cyber Command, the Navy's U.S. Fleet Cyber Command, Marine Forces Cyberspace Command, and Air Forces Cyber/16th Air Force. The commanders of these service components are dual-hatted as Joint Force Headquarters Cyber (JFHQ-C) commanders. CYBERCOM also has two subordinate unified commands that conduct operations on a continuing basis for the command: the Cyber National Mission Forces (CNMF) and DOD Cyber Defense Command (formerly JFHQ-DODIN).

The Cyber Mission Force (CMF), CYBERCOM's operational arm, comprises several cyber mission forces: The CMF consists of the Cyber National Mission Force, the Cyber Protection Force, and the Cyber Combat Mission Force, each with their own associated mission teams. These teams are controlled through the four subordinate service JFHQs and the two subordinate unified commands. Coast Guard Cyber Command, part of the Department of Homeland Security, has a direct support relationship to CYBERCOM. Congress has been exploring the idea of creating a separate cyber military service under CYBERCOM through the Cyberspace Solarium Commission (CSC), created by Congress in the National Defense Authorization Act for Fiscal Year 2019 (NDAA; P.L. 115-232).

Expanded Authorities

In view of CYBERCOM's specialized missions that require uniquely trained personnel and equipment, Congress has in 10 U.S.C. §167b provided the command with expanded authorities related to budget, acquisitions, and personnel management processes—authorities that are, in general, broader than those provided to certain other CCMDs and similar to those of the military departments. In 2018, the Trump administration delegated additional authorities to the SECDEF for certain military cyberspace operations, according to DOD.

Budget

DOD requests funding for CYBERCOM in budget justification documents associated with multiple Defense-Wide accounts: Operations and Maintenance (O&M); Procurement; and Research, Development, Test, and

Evaluation (RDT&E). The Department of the Army serves as the *Combatant Command Support Agent* for CYBERCOM, providing the command logistical and administrative support. Congress in Section 1507 of P.L. 117-81 assigned certain budget responsibilities to the CYBERCOM commander. Since FY2024, DOD has requested headquarters funding as part of a line item for the command within the O&M, Defense-Wide account (rather than in the Army's O&M account). In FY2025, Congress provided CYBERCOM $1.6 billion for O&M, $109.7 million for procurement, and $1.0 billion for RDT&E.

CYBERCOM Strategic Concerns

In his 2025 posture statement to the Senate Armed Services Committee (SASC), Acting Commander of CYBERCOM, Army Lieutenant General William Hartman, described some areas of strategic concern for CYBERCOM as:

- China's "persistent access to U.S. critical infrastructure systems pre-position for attack in a contingency or crisis scenario."
- Russia's integration of sophisticated military and intelligence cyber forces to achieve its strategic objectives, cyber actors to "subvert Ukraine and divide Western allies," and toleration of cyber-crime activities that "often serve state purposes against foreign targets."
- Creating U.S. operational and strategic advantages through the growing use of artificial intelligence while also "denying similar advantages to adversaries seeking to exploit our systems and data."

Potential Issues for Congress

Nomination of Next CYBERCOM Commander

On April 4, 2025, DOD announced that Air Force General Timothy Haugh was no longer serving as commander of CYBERCOM or DIRNSA. Lieutenant General Hartman assumed the role of acting commander of CYBERCOM. A new, permanent commander has been nominated for consideration. The Senate confirms individuals appointed to the grade of 4-star general or admiral and assigns them to CYBERCOM commander under 10 U.S.C. §601. In anticipation of hearings to confirm Army Lt. Gen. Joshua M. Rudd, Congress may consider:

- Developing questions for a potential nominee;
- The operational background of a potential nominee;
- The current cyber threat landscape facing U.S. national security interests; and
- The dual-hatted roles and status of the CYBERCOM commander and DIRNSA positions.

CYBERCOM Commander Dual-Hatted Status as Director of the National Security Agency

In 2022, the SECDEF and Director of National Intelligence (DNI) sponsored a study of the dual-hatted CYBERCOM commander/DIRNSA leadership arrangement that, according to Haugh, concluded "protecting our national security would be more costly and less decisive if NSA and USCYBERCOM were led by two different leaders, and that the dual-hat arrangement produces better outcomes for the nation." According to Haugh, the SECDEF, the Director of National Intelligence (DNI), and the Chairman of the Joint Chiefs of Staff "subsequently determined to maintain the arrangement," and DOD has "focused on ensuring an enduring and sustainable dual-hat arrangement."

In 2022, Congress increased its oversight of the relationship between CYBERCOM and NSA, in Section 1556 of P.L. 117-263, by directing the SECDEF to provide the congressional defense committees with an annual briefing on the command relationship and operations of CYBERCOM and NSA.

Congress could consider whether or not to direct an independent study conducted outside of the auspices of DOD/DNI on the effectiveness and potential efficiencies presented by the leadership and operations of CYBERCOM and NSA, co-located at Fort Meade. Congress could also consider the role of civilian leadership and oversight of NSA.

Modernization Efforts

In his April 9, 2025, testimony to the SASC Subcommittee on Cybersecurity, Lieutenant General Hartman outlined several initiatives central to the modernization of CYBERCOM and maintenance of a credible cyber deterrent. Congress may choose to consider:

- Continued oversight of the implementation of *CYBERCOM 2.0* and assessment of any policy changes that might be required to finalize the initiative;
- An independent evaluation regarding the potential establishment of a United States Cyber Force;
- Mechanisms and funding options that support the development and integration of artificial intelligence in defense-related cyberspace operations;
- Options focused on improving talent management across the spectrum of DOD cyberspace operations;
- Whether to expand the scope and funding provided to CYBERCOM for the purpose of supporting cooperative research agreements with education and industry;
- Mechanisms and funding to improve the integration of reserve component personnel into operations focused on securing critical infrastructure; and
- Options to increase interagency cooperation and integration with CYBERCOM.

Operational Authority

Title 10 of the U.S.C. provides the foundational authorities for conducting military cyberspace operations. Additional authorities are governed by the classified National Security Presidential Memorandum-13 (NSPM-13), *United States Cyber Operations Policy*, first promulgated in 2018 during the Trump Administration, according to DOD, and reportedly replacing an Obama Administration cyber operations directive. A Joint Staff official reportedly described the policy as hastening interagency coordination by delegating to the SECDEF "certain cyberspace authorities to do cyber effects operations for a particular mission." In March 2025, the SECDEF reportedly ordered CYBERCOM to pause offensive cyber operations conducted against Russia for one day. DOD reportedly denied the issuance of such an order. Congress may wish to clarify whether or not such an order was issued and to what extent it affects the provisions of NSPM-13.

Robert Switzer, a former National Defense Fellow with CRS, contributed to this product.

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

Disclaimer