Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Analysis of a Potential Cyber Military Service

August 19, 2026

Introduction

Congress has long deliberated the idea of creating a separate cyber military service to match the cyberspace domain, tasking various organizations to study the idea. This topic is also of interest to the current Congress, particularly with the publication of a report by the Commission on Cyber Force Generation and the revised CYBERCOM 2.0 Force Generation Model implementation plan. The question of whether a separate cyber service is necessary goes hand-in-hand with the perennial question of whether to preserve the dual-hatted arrangement of Cyber Command's (CYBERCOM's) commander as Director of the National Security Agency, which has been raised in Congress since CYBERCOM's inception in 2010. This In Focus provides background information on CYBERCOM and the multiservice Cyber Mission Force, including the dual-hatted arrangement; the work of the Cyber Force Generation Commission; and analysis of maintaining the status quo versus creating a new service.

Cyberspace as a Domain

The Department of Defense (DOD)—which is "using a secondary Department of War designation" under Executive Order 14347 dated September 5, 2025—declared cyberspace an operational domain in 2009. In 2010, the Quadrennial Defense Review referred to cyberspace as being "as relevant a domain … as the naturally occurring domains of land, sea, air, and space." A formal DOD cyber strategy naming the new domain was published in 2011. Subsequent doctrine 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.

Establishment of CYBERCOM

The origins of CYBERCOM can be traced to the 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 the 24th Air Force, which later merged with the 25th Air Force to become the 16th Air Force (Air Forces Cyber).

On June 23, 2009, the then Secretary of Defense (SECDEF) Robert Gates directed the creation of CYBERCOM, establishing the organization as a subordinate (or *sub-)* unified command under STRATCOM. Both JTF-GNO and JFCC-NW were absorbed into the new command. Initially, CYBERCOM received assistance from the National Security Agency (NSA), including personnel, equipment, and resources to perform its mission. The command reached initial operating 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 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, also serving as the director of NSA (DIRNSA).

Cyber Mission Force

DOD began to build a Cyber Mission Force (CMF) in 2012 to carry out DOD's three cyber missions. Specifically, CMF teams support these mission sets though 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 reached full operational capacity with 133 teams and around 6,200 individuals in 2018. Up to 14 additional teams were authorized in 2022. Organizationally, CMF is an entity of CYBERCOM, with each service branch providing its own cyber forces. These forces are organized through Army Cyber Command, Fleet Cyber Command/Tenth Fleet, 16th Air Force/Air Forces Cyber, and Marine Corps Forces Cyberspace Command.

Analysis of a Cyber Military Service

Since the advent of CYBERCOM and the concept of cyberspace as a warfighting domain, some defense officials in tandem with congressional offices and committees have analyzed arguments for and against creating a separate, independent cyber military service. Some observers argue that the potential benefits of such a construct could include the following:

- Specialization and Focus. A dedicated branch could treat cyberspace as its primary mission rather than being subordinate to traditional warfare domains.
- Recruiting and Retention. CMF comprises four different service branches, each with varying standards and promotion metrics. A stand-alone service could implement flexible pay, direct commissions, and career paths designed specifically for cyber warfighting experts.

- Command and Control. Currently, CYBERCOM coordinates with the cyber forces of multiple services. An independent force could centralize the acquisition of cyber-specific technologies and unify force generation under one command structure.

Other observers argue that the potential disadvantages could include the following:

- Cost and Timing. Standing up a new military service is a costly and time-consuming endeavor. Some studies estimate a cyber service could cost up to $11 billion to stand up and $20 billion annually to operate and up to 18 months to reach initial operational capacity.
- Domain Disconnects. Cyberspace is multidomain, as it exists within the land, sea, and air domains. Separating cyber operators into their own branch could result in manning mismatches or delays when, for example, infantry divisions or naval fleets need immediate cyber support.
- Disruption of Readiness. Some former CYBERCOM officials argue that CMF is already agile and adaptive and that creating a new service could be highly disruptive at a time when readiness and rapid response capabilities are essential.
- Stovepiping. Some analysts note concern for further stovepiping of cyber from other information-related capabilities, such as psychological operations and electronic warfare. These capabilities, once the purview of services' information operations commands, often became separate endeavors with the creation of the services' cyber commands.

Commission on Cyber Force Generation

The Center for Strategic & International Studies (CSIS), in partnership with the Cyberspace Solarium 2.0 project at the Foundation for Defense of Democracies (FDD), launched the Commission on Cyber Force Generation on August 4, 2025, "to provide recommendations on how to organize a new military service that would ensure and defend the United States' strategic superiority and security in the cyber domain." On June 3, 2026, the commission published a report that found, among other things, that the current structure of CMF is "insufficient" to meet the increased challenge of cyber threats facing the nation. The report noted growing interest in creating a single military service for cyberspace as an operating domain, stating that

> [m]any observers contend that the challenge of generating military capability and capacity necessary to deter, compete, fight, and win in the cyber domain can be directly attributed to the lack of a single organization responsible and accountable for force generation in cyberspace—or organizing, training and equipping the military forces operating in this domain.

The commission recommends a military service with approximately 20,000 active-duty uniformed personnel, 3,500-5,000 National Guard personnel, and a civilian workforce of 6,000 to start. It recommends employing only commissioned and warrant officers for uniformed personnel and, instead of a reserve component, it recommends establishing a Cyber National Guard to be "leveraged by both state and federal authorities." According to the commission's report, the initial budget for standing up a "Cyber Force" would be an estimated $10 billion-$11 billion. The FY2027 defense budget request overview allocates $7.7 billion to cyberspace operations, with $4.1 billion designated to CYBERCOM and the remaining $3.6 billion for other defense entities, including NSA. The report offers two paths to achieving a Cyber Force: alignment within the Department of the Army or establishment of its own military department. The report notes the latter path as requiring "significant time and resources."

Considerations for Congress

Congress may consider the following questions when deliberating whether to establish a new cyber service.

Cyber Military Service Leadership

There are statutory caps to the number of general and flag officers (10 U.S.C. §525(a) and 10 U.S.C. §526) in the military services. Would a new cyber military service require changing these caps for a four-star commander and additional general officers, or would these positions be filled by existing general officers? In terms of civilian leadership, would a civilian Secretary counterpart, similar to Service Secretaries, be established?

Joint Chiefs of Staff Membership

Would a cyber military service commander become a member of the Joint Chiefs of Staff (JCS)? If so, how might it influence current JCS procedures and operations?

Cyber Military Service and the Unified Command Plan

The Unified Command Plan (UCP) is a classified executive branch document prepared by the JCS Chairman and approved by the President that establishes the missions, responsibilities, and geographic areas of responsibility for combatant commands. Would the creation of a cyber military service impact the current UCP and conform with the provisions of 10 U.S.C. §161, which cover the establishment of combatant commands and congressional reporting requirements?

Catherine A. Theohary, Specialist in National Security Policy, Cyber and Information Operations
Andrew Feickert, Specialist in Military Ground Forces

IF13291

Disclaimer