JUNE 2026

CSIS Commission on U.S. Cyber Force Generation

Summary Report

CO-CHAIRS

Joshua Stiefel

Ed Cardon

CO-DIRECTORS

Lauryn Williams

Taylar Rajic

Matthew Pearl

LEAD AUTHOR

Erica D. Lonergan

A Report of the CSIS Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JUNE 2026

CSIS Commission on U. S. Cyber Force Generation

Summary Report

CO-CHAIRS

Joshua Stiefel

Ed Cardon

CO-DIRECTORS

Lauryn Williams

Taylar Rajic

Matthew Pearl

LEAD AUTHOR

Erica D. Lonergan

A Report of the CSIS Strategic Technologies Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Cover: Lidiia/Adobe Stock

Contents

Acknowledgements

The following group of leading experts in cybersecurity and force generation contributed to the development of this report:

Commissioners

Perri Adams, Fellow at the Dartmouth Institute for Security and Technology Studies

Rye Barcott, Co-Founder and CEO of With Honor

George Barnes, President and Partner of Red Cell Partners' Cyber Practice

LTG (Retired) Maria B. Barrett, Former Commanding General of the Network Enterprise Technology Command and Commanding General, U.S. Army Cyber Command

LTG Ed Cardon, USA (Ret.), Founding Partner and Co-CEO of Touchstone Futures

VADM (Retired) Craig Clapperton, CEO of Clapperton Consulting Corporation

ADM (Retired) Michael Gilday, CEO of Crossover Solutions National Security USA

Lt. Gen. (Retired) Jerry Glavy, President of Glavy Outcomes Group

Maj. Gen. (Retired) Ryan Heritage, Senior Associate (non-resident) for the Strategic Technologies Program at CSIS

CAPT (Retired) Mike Herlands, Owner of Audvan LLC

Rob Lee, CEO and Co-Founder of Dragos

Rob T. Lee, Chief AI Officer and Chief of Research at the SANS Institute

Joseph Lin, Co-Founder and CEO of Twenty

Dr. Erica D. Lonergan, Assistant Professor at the School of International and Public Affairs, Columbia University

LCDR (Retired) Tyson Meaders, Director of Cyber at Anduril Industries

RADM (Retired) Mark Montgomery, Senior Director of the Center on Cyber and Technology Innovation and Senior Fellow at the Foundation for Defense of Democracies

COL (Retired) Chris Reid, U.S. Public Sector Chief of Staff at Elastic

Ted Schlein, Chairman and Founding General Partner, Ballistic Ventures

LtGen (Retired) Robert Skinner, Director at the Defense Information Systems Agency

Joshua Stiefel, Vice President for Government Relations at Second Front

Dr. Michael Sulmeyer, Professor of the Practice at Georgetown School of Foreign Service

LtGen (Retired) Chris Weggeman, Managing Director of Cyber & Strategic Risk

Senior Advisers

Chris Cleary, Vice President of the Global Cyber Practice at ManTech

Emily Harding, Vice-President of the Defense and Security Department and Director of the Intelligence, National Security, and Technology Program at CSIS

Kurt Sanger, Counsel at Buchanan Ingersoll & Rooney PC

Ari Schwartz, Managing Director of Cybersecurity Services at Venable

Reviewer

Dr. Nikita Shah, Senior Fellow with the Intelligence, National Security, and Technology Program at CSIS

The CSIS Commission on U.S. Cyber Force Generation also wishes to express its deepest gratitude to the individuals, both in and out of uniform, who courageously offered their perspectives, views, and choice words to this report. The nation is indebted to these warfighters trying daily to hold the country's adversaries at risk and keep us safe in cyberspace.

Acronyms

ACIC	Army Counterintelligence Command
ADCON	Administrative control
AFOSI	Air Force Office of Special Investigations
AOR	Area of responsibility
C2	Command and control
CCF	Chief of the Cyber Force
CFCC	Cyber Force Component Command
CID	Criminal Investigative Division
CYBERCOM	United States Cyber Command
DC3	Defense Cyber Crime Center
DCO	Defensive cyber operations
DOD	Department of Defense
DODD	Department of Defense Directive
DODIN	Department of Defense Information Networks
EBC	Enhanced budget control
EUCOM	United States European Command
GAO	Government Accountability Office
GMI	General military intelligence (foundational intelligence)
HUMINT	Human intelligence
IMD	Integrated Mission Delta
IMINT	Imagery intelligence
JAG	Judge Advocate General
MASINT	Measurement and signature intelligence

MCIO	Military Criminal Investigative Organization
MDCO	Military Department Counterintelligence Organization
MILPERS	Military Personnel
NCIS	Naval Criminal Investigative Service
NCWDG	Navy Cyber Warfare Development Group
NDAA	National Defense Authorization Act
NOAA	National Oceanic and Atmospheric Administration
NORTHCOM	United States Northern Command
NSA	National Security Agency
O&M	Operations and Maintenance
OCO	Offensive cyber operations
PME	Professional military education
R&D	Research and development
RCO	Rapid Capabilities Office
RDT&E	Research, Development, Test, and Evaluation
S&TI	Scientific and technical intelligence
SIGINT	Signals intelligence
SOCOM	United States Special Operations Command
SPACECOM	United States Space Command
STRATCOM	United States Strategic Command
USFK	United States Forces Korea
USPHS	United States Public Health Service

Key Terms

Term	Definition
Cyber Force	A proposed independent military service focused on generating cyber forces (manning, training, and equipping) for joint operations in cyberspace
Force generation	Military service responsibilities to organize, train, equip, sustain, and provide ready forces (often described as "man, train, and equip")
Force employment	Combatant command responsibility to employ assigned forces to execute operations and campaigns
Cyberspace operations	Military operations conducted in and through cyberspace to achieve objectives; refers to offensive, defensive, and DODIN operations
Offensive cyber operations (OCO)	Actions intended to project power in and through cyberspace, including cyber exploitation and cyberattacks to create effects against adversary systems
Defensive cyber operations (DCO)	Actions conducted in response to imminent or active threats to preserve the ability to use cyberspace capabilities and defend mission-relevant networks and data
DODIN operations	Operations to secure, configure, operate, extend, maintain, and sustain DOD information networks to preserve confidentiality, availability, and integrity

Executive Summary

The United States faces an unprecedented range of cyber threats from nation-state and criminal cyber actors amid fast-moving technology developments, including AI-enabled cyber offensive and defensive applications. The first pillar of the Trump administration's Cyber Strategy for America declares the United States "will deploy the full suite of government offensive and defensive cyber operations" against its adversaries.[1] These adversaries include nations like the People's Republic of China and Russia, which are targeting the U.S. and allied critical infrastructure that underpins all elements of national and economic security, and are using AI to rapidly advance the scale and scope of attacks and develop new attack vectors. Meanwhile, U.S. frontier AI developers are producing ever-more-advanced models capable of finding and exploiting vulnerabilities, as well as strengthening cyber defenses. Adversaries are working to leverage these same AI capabilities and will continue to exploit network vulnerabilities unless the United States can better defend itself in the cyber domain against persistent threats.

Across the Department of Defense (DOD), there is a consensus and recognition that the existing design of the military's cyber forces is insufficient. Many 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. This dilemma is unique to the cyber domain, as there are already dedicated military services for each of the other four recognized warfighting domains—land, sea, air, and space. A recent attempt to address this force generation gap—the U.S. Cyber Command (CYBERCOM) 2.0 initiative announced by the Pentagon in November 2025—intends to give CYBERCOM some additional "service-like"

authorities by standing up three new organizations for personnel assignments, training, and rapid capability development. Additionally, Congress has directed the National Academies of Sciences, Engineering, and Medicine to conduct a study looking at the feasibility of standing up an independent military service dedicated to the cyber warfighting domain.

The CSIS Commission on U.S. Cyber Force Generation

Looking beyond incremental reforms, the core premise motivating the CSIS Commission on U.S. Cyber Force Generation is that America's current cyber force generation model faces important challenges. It is also at odds with how the U.S. military has organized itself for warfighting dating to 1986 and the defense organization reforms of the Goldwater-Nichols Act. If there is a decision to create a Cyber Force, there will significant challenges in implementing the decision given current force generation repsonsibilites are shared between the Services and CYBERCOM.

In response, the Center for Strategic and International Studies (CSIS), in partnership with the Cyber Solarium Commission 2.0 (CSC 2.0) project at the Foundation for Defense of Democracies, launched this commission to articulate a vision, mission, and implementation plan for a new U.S. Cyber Force—an independent military service dedicated to the cyber warfighting domain—rather than to reprise existing debates about whether such a force should be established. This report does not focus on the decision to create a Cyber Force—it instead presents options for how to best implement the a future decision to establish a Cyber Force.

Over the course of 10 months, the commission convened leading experts across the military, government, academia, and the private sector to examine how the United States can best build a dedicated Cyber Force to establish and acquire the most cutting-edge offensive and defensive capabilities, ensure the recruitment and retention of top cyber talent, and elevate cyberspace to a core warfighting domain on par with air, land, sea, and space. Commissioners engaged extensively on Capitol Hill and with current and former DOD officials regularly while developing recommendations in this report. Working from the starting assumption that the decision to establish a Cyber Force has been made, the commission discussed how such a force could be structured, resourced, and trained to respond to the evolving cyber threat environment.

Recognizing the complexity of establishing a Cyber Force, the commission focused on the core operational, organizational, and force-generation questions required to stand one up effectively. This report thus provides a comprehensive plan with options for implementation on day one following a presidential decision.

Goals of a Cyber Force and Its Relationship to CYBERCOM

The commission was designed to focus on how a notional Cyber Force could enhance both offensive and defensive cyber capabilities, ensure the recruitment and retention of top cyber talent through multiple accession pathways, and elevate cyberspace to a core military domain on par with air, land, maritime, and space. Critically, the commission was not tasked with determining if a Cyber

Force is desirable, but instead helping the DOD and Congress understand how such a force could be stood up and implemented on a relevant timeline following a presidential decision.

The commission's recommendations center on the elements required to stand up a new United States Cyber Force, a new military service with a narrowly defined, cyber-specific mission. Its central obligation would be to organize, train, and equip forces to conduct offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO). Critically, this ensures that internal security-related efforts, formally known as Department of Defense Information Networks (DODIN) Operations, are retained by the Army, Navy, Marine Corps, Air Force, and Space Force.

If established, the Cyber Force would assume most of the "service-like" responsibilities currently held by CYBERCOM, mirroring the relationship between the existing services and the combatant commands established by Goldwater-Nichols. It would be established as an independent branch of the U.S. Armed Forces within the DOD, with force generation responsibilities comparable to the existing military services. In standing up a Cyber Force, priority would be given to minimizing disruptions to current and ongoing cyber operations being carried out by the existing services, requiring the force be stood up at a meaningful speed to meet the evolving threat environment.

Estimated Size and Cost of a Cyber Force

The commission recommends establishing a Cyber Force with an end strength of 20,000 active-duty uniformed personnel, an additional 3,500–5,000 National Guard personnel, and a civilian complement of 6,000 personnel, or about 30 percent relative to the uniformed force size. Among uniformed personnel, the commission recommended the Cyber Force consist of commissioned officers and warrant officers, but without an enlisted cadre—following the U.S. Public Health Service precedent. Several considerations informed this estimate, including the size and composition of the existing forces aligned to cyber operations across CYBERCOM and the services today; historical assessments performed by Space Force, the Government Accountability Office (GAO), and federally funded R&D centers; and commissioners' own experiences and expertise. The commission recommended against standing up a Cyber Force Reserve, preferring solely a National Guard construct able to operate under both federal and state authorities. Such a model would enable the Cyber Force to best leverage part-time talent and support recovery efforts related to cyberattacks on critical infrastructure.

Building on current DOD funding levels, the commission estimates around $10–$11 billion would be the initial budget requirement to stand up the Cyber Force.

Cyber Force's Institutional Alignment Within the DOD

The commission considered two viable options for institutional alignment. The first option is alignment within the Department of the Army. This would allow the Cyber Force to fit within the existing DOD bureaucracy, which could then be leveraged for speed and efficiency. A key trade-off of this option is the risk that the Cyber Force would be considered lower priority than the much larger Army organization.

A second option is aligning the Cyber Force in its own military department, a new Department of the Cyber Force. This option would ensure maximum prioritization of cyber issues across the Pentagon, amid a shifting threat environment and force generation challenges. The key trade-off is that standing up an entirely new Pentagon bureaucracy would require significant time and resources and thus take significantly longer to implement.

How Long Would a Cyber Force Take to Stand Up

The commission estimated that, regardless of institutional alignment, reaching initial operating capacity (IOC) would take between 12 and 18 months and proceed through several sequential phases: setting conditions; fielding the IOC; iterative growth over several years; and institutional refinement. This approach emphasizes maintaining force quality over establishing force mass, and experimentation with novel approaches over rigid design features.

A notional U.S. Cyber Force would assume the force generation—or man, train, and equip—responsibilities laid out in Table 1.

Following a presidential decision or legislative action to establish a new Title 10 service, this force generation model would address longstanding structural challenges and build the Cyber Force the United States needs for this critical domain of warfare.

Table 1: Force Generation Functions of a Cyber Force

Function	Key Responsibilities and Activities
Man (Organize)	■ **Recruitment:** Attract highly specialized technical talent, selecting for quality. ■ **Personnel Management:** Administer pay, morale, welfare, and medical support. ■ **Personnel Transition:** Realign personnel from existing services into the new Cyber Force (prioritizing adaptability and rapid experimentation). ■ **Force Composition:** Manage a ~30,000-person force (20,000 active-duty commissioned and warrant officers, 3,500–5,000 National Guard, and 5,000–6,000 civilians and contractors). ■ **Career Pathways:** Establish dual-track (technical and managerial) advancement models for mission-, technical-, and capability-focused leaders.
Train	■ **Force Preparation:** Train and certify offensive and defensive cyber operators. ■ **Culture and Doctrine:** Develop cyber concepts, doctrine, tactics, techniques, and procedures. ■ **Education:** Deliver professional military education (PME) and specialized cyber leadership training. ■ **Readiness:** Assume the role of joint force trainer, providing standardized training for cyber forces. ■ **Cyber Force Generation and Training Command:** Generate, sustain, and certify ready cyber forces for operational employment.
Equip	■ **Infrastructure:** Operate facilities, systems, and supporting infrastructure. ■ **Budgetary Control:** Manage dedicated cyber funding (with an initial budget of approximately $10–$11 billion). ■ **Intelligence Support:** Provide foundational all-source cyber intelligence capabilities.

Source: CSIS Commission on U.S. Cyber Force Generation.

Introduction

Starting from a directive to create a Cyber Force, the report makes two core assumptions. The commission assumed the Cyber Force will be established as an independent branch of the Armed Forces, within the DOD, with force generation responsibilities comparable to the other military services (Army, Navy, Air Force, Marine Corps, and Space Force). The commission further assumed that implementation of the Cyber Force must occur at a meaningful speed while still balancing the need to minimize undue operational impact in the short term.

Today, U.S. Cyber Command (CYBERCOM), as one of the DOD's 11 unified combatant commands, is statutorily responsible for force employment in and through the cyber domain. However, while the U.S. military has defined cyberspace as a domain of warfare since 2004, there is not a single entity with the primary responsibility for generating forces in that domain. Instead, responsibilities are split across the five existing services, together with some "service-like" authorities that CYBERCOM retains. The cyber domain is thus the only domain of warfare that lacks a dedicated organizational unit for force generation.

The fact that the current approach is failing to keep pace with the threat is generally accepted. In February 2025, a former CYBERCOM commander, General Paul Nakasone, acknowledged the United States had fallen behind its adversaries in cyberspace.[2] Last fall, a former deputy national security advisor at the White House went even further, publishing an article titled "China is Winning the Cyberwar."[3] In short, the U.S. military lacks the focus, resourcing, manpower, and platforms to accomplish its missions in cyberspace.

The current and longstanding issues with the nation's ability to accomplish its desired missions in the cyber domain all stem from a single, fundamental problem: The U.S. military is not structured to generate, train and equip the necessary number of personnel with cyber mastery and expertise. Testifying before Congress in April 2026, Assistant Secretary Katie Sutton, the DOD's senior-most civilian cyber leader, stated that the department faces "significant challenges . . . recruiting the right people with the right aptitude and skill sets, retaining our most skilled and experienced operators in the face of lucrative industry opportunities, and providing the specialized, agile training needed to win against our nation's adversaries."[4]

No service within the Department of Defense has primacy for cyber force generation—none of the services prioritizes cyber force generation.

There is a dangerous gap between the centrality of cyberspace for modern warfighting and the U.S. military's persistent inability to generate the capabilities necessary to deter, compete, fight, and win in the cyber domain. No service within the DOD has primacy for cyber force generation—none of the services prioritize cyber force generation. In turn, across five different services, there are inconsistent approaches to recruiting, initial training, education, career progression pathways, and compensation. This has resulted in a disjointed and inefficient effort that provides ineffective and inconsistent results. An independent Cyber Force will naturally prioritize creating a cohesive and unified approach to the recruitment, training, promotion, and retention of qualified personnel whose skills correspond to the requirements of warfighting in cyberspace.

Such an approach will also be in line with historical precedent, following in the footsteps of the establishment of the Air Force in 1947 and the Space Force in 2019. The creation of both services reflected a recognition that the air and space domains play unique roles in warfighting and demand a single service focused on generating capabilities aligned to those unique domains. So, too, is cyberspace a distinct operational domain with unique force generation requirements, and consequently, as its own service, the Cyber Force can optimize organizing, training, and equipping for that domain. The current force generation model has repeatedly failed to produce and sustain the density of talent, the robust cadre of leadership, and the most cutting-edge capabilities that are necessary for the United States to generate forces for warfighting in the cyber domain. The body of this report offers a detailed path forward for how to build the Cyber Force the nation needs for this critical domain of warfare.

1

Structure, Roles, and Mission

Methodology and Recommended Functions

To envision how a future Cyber Force could best be organized, the CSIS Commission on U.S. Cyber Force Generation over the course of 10 months engaged in structured discussions, interviewed personnel ranging from senior leaders to current operators, conducted tabletop exercises, and reached out to industry and subject matter experts. A common theme that emerged from this process was the criticality of defining specific functions the Cyber Force will perform to accurately design the force generation service.

Commissioners started with a comprehensive examination of Department of Defense Directive (DODD) 5100.01, the Pentagon's foundational document for establishing the functions of the Department of Defense and its major components, supporting the core mission areas of the Armed Forces, which include broad DOD military operations and activities required to achieve the strategic objectives of the National Security Strategy, National Defense Strategy, and National Military Strategy.[5] A critical first step following the decision to establish a Cyber Force will be to update DODD 5100.01. The commission engaged in extensive deliberations and generated multiple drafts of possible revisions to DODD 5100.01. Detailed below is the notional text regarding the Cyber Force's core functions—which includes force generating capabilities for defensive cyber operations (DCO) and offensive cyber operations (OCO). Critically, the commission's proposed revision of DODD 5100.01 establishes that the Cyber Force's senior uniformed officer (referred to as chief of the Cyber Force) serves as a coequal member of the Joint Chiefs of Staff as principal military adviser for all U.S. Cyber Force functions, as well as the most senior officer of this new service.

This proposed revision of DODD 5100.01 serves as the commissioners' anchor point throughout the entire effort and is as follows:

In addition to the common military service functions listed in paragraphs 2.a. through 2.n. of this enclosure, the Cyber Force shall develop concepts, doctrine, tactics, techniques, and procedures, and organize, train, equip, and provide forces with strategic, expeditionary, and campaign qualities to perform the following specific functions:

1. Conduct prompt and sustained cyberspace control operations across all geographies in order to control, contest, seize, occupy, and defend cyberspace areas.
2. Conduct cyber defense to support joint campaigns and assist in achieving cyberspace superiority.
3. Interdict enemy land, sea, space, air power, and cyber communications through operations within, from, or traversing cyberspace.
4. Provide support for cyberspace operations to enhance joint campaigns, in coordination with the other military services, combatant commands, and U.S. government departments and agencies.
5. Conduct authorized civil works programs, to include projects for improvement of cybersecurity in the United States, its territories, and its possessions, and conduct other civil activities prescribed by law.
6. Conduct reconnaissance, surveillance, and target acquisition.
7. Conduct expeditionary cyberspace operations other than those that are organic to the individual military services.
8. Remain fluent in foreign technologies used in cyber infrastructure, information systems, and weapon system technologies.
9. Excel at integrating existing commercial and open-source solutions into existing capabilities or as alternatives to bespoke capability development.
10. Provide timely and relevant response options to respond to, and disrupt, ongoing or recurring cyberattacks against critical infrastructure and key resources.
11. Enable freedom of maneuver in cyberspace.
12. Provide effects from or within cyberspace in support of joint campaigns.
13. Conduct cyberspace operations in support of deterrence, to include providing and maintaining hard-target surety and capabilities.
14. Provide the commander in chief with the full range of crisis response and escalation management options via the cyber domain.
15. Generate capabilities for foundational, all-source intelligence related to the cyber domain.
16. As required and permitted by law, provide defensive cyber support to state and local governments.

Man, Train, and Equip Responsibilities

In this report, the CSIS Commission on U.S. Cyber Force Generation has designed a concept for building a Cyber Force that is laser-focused on force generation (known as "man, train, and equip" or "organize, train, and equip" responsibilities). To mirror the functions of the existing services, the Cyber Force will serve as the single institution primarily responsible for manning, training, and equipping technically and operationally proficient OCO and DCO forces. To perform this role, the Cyber Force will also have the responsibility of recruiting, supplying, equipping (including R&D), servicing, mobilizing, demobilizing, administering (including morale and welfare), and maintaining personnel, as well as of constructing, outfitting, and repairing military equipment, buildings, structures, and utilities.[6]

The commission's task over 10 months was to provide a vision and plan for how a Cyber Force could be established to remedy the military's perennial shortfalls in force generation for cyber-capable forces. At the core of the matter, commissioners sought to resolve the present paradox affecting CYBERCOM—a combatant command responsible for force employment and increasingly gaining ownership over force generation, but still dependent on the military services for personnel, administration, recruitment, and policy. While many will point to U.S. Special Operations Command (SOCOM) as a combatant command also charged with force generation responsibilities, the special operations community in fact retains the institutional separation of the force generation functions from the force employment functions, with geographic combatant commands maintaining responsibility for the operational control over special operations forces in their area of responsibility (AOR).

In the absence of a dedicated service for cyberspace, CYBERCOM is expected to perform the functions of both a combatant command and a military service, putting force generation and force employment under one leader, the same arrangement that Congress sought to prevent through the 1986 defense organization reforms under the Goldwater-Nichols Act.[7]

To date, Congress and the White House have supported empowering CYBERCOM to a point. In 2017, CYBERCOM was designated as the joint force trainer and joint force provider to standardize training for cyber forces.[8] In the FY 2022 National Defense Authorization Act (NDAA), Congress granted CYBERCOM enhanced budgetary control, enabling it to directly control some resources for equipping the cyber mission force. Additionally, as a result of a congressional mandate, CYBERCOM has developed and launched its "CYBERCOM 2.0" initiative, approved by the secretary of defense in November 2025, to further control responsibilities normally performed by the military services through the establishment of three new staff organizations to control personnel assignments, training, and rapid capability development. Together, these efforts give CYBERCOM greater "service-like" authorities by managing aspects of the organize, train, and equip functions performed by the military services.

Paradoxically, as CYBERCOM gains greater control over force generation, force employment demands are increasing. The current trend is incrementally recreating the pre-1986 conditions that

led to congressional intervention via the Goldwater-Nichols Act and the legislative separation of force generation from force employment under a single leader.

Unsurprisingly, in the decade since CYBERCOM has been assigned joint force trainer and joint force provider functions, balancing force employment and force generation has proven an increasingly challenging task. The cyber mission set has expanded and its pace of operations increased, but the demands of force generation have not kept pace.

If established, the Cyber Force will organize, train, and equip forces for the cyber domain. Therefore, it will assume most of the "service-like" responsibilities currently held by CYBERCOM, mirroring the relationship between the existing services and the combatant commands. Comparable to the roles of the existing services for their respective domains, the Cyber Force must be deliberately structured to master the requisite disciplines and skills for cyber warfare, advance joint warfighting concepts, and integrate cyber effects as directed across the whole of government. Additionally, the Cyber Force will require similar enablement functions to the existing military services, such as acquisition, budgeting, intelligence, research, legal, and legislative support.

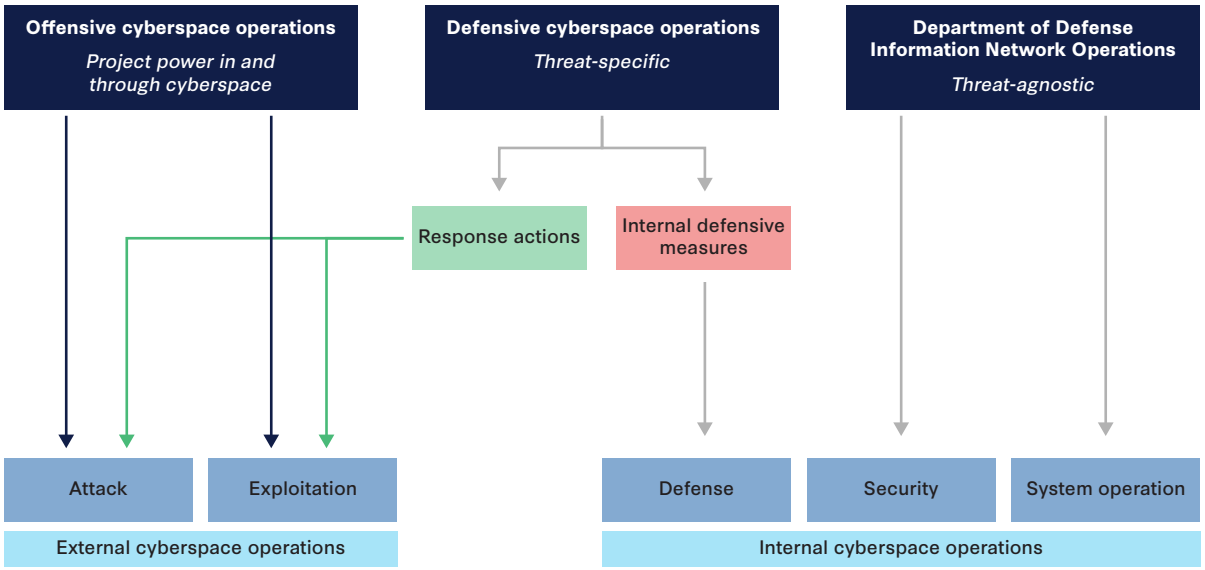
Service Parameters and Responsibilities

Each military service today relies on information technology (IT) and performs activities in cyberspace that are an extension of their core domain-specific warfighting responsibilities (whether that is on land for the Army, in the air for the Air Force, at sea for the Navy, or in space for the Space Force). For example, in September 2025, an audit by the GAO found that the DOD and the Coast Guard had established almost 440 organizations with more than 70,000 military, civilian, and contractor personnel conducting offensive, defensive, and internal security operations in and through cyberspace.[9] They identified 26 separate non-operational organizations, offices, and headquarters involved in budgetary support to cyberspace operations, with 10 separate entities within the Army alone.[10] The GAO also found that there are more than two dozen DOD components presently responsible for the command and control (C2) of cyberspace operations, creating additional complications and complexity.[11]

The commission strongly disfavored a Cyber Force that absorbs all current efforts and responsibilities leveraging networked technologies. Specifically, the Cyber Force should not be expected to replicate the work performed by these more than 400 pre-existing organizations. However, the commission agreed that establishing a Cyber Force will result in a net efficiency by addressing critical redundancies and returning billets to the other services.

The commission judged that the most optimal course will be for the Cyber Force to focus on activities specifically related to generating capabilities for OCO and DCO. Critically, this ensures that efforts related to internal security, formally known as Department of Defense Information Networks (DODIN) Operations, are retained by the Army, Navy, Marine Corps, Air Force, and Space Force for their respective segments of the DODIN.

Figure 1: Cyberspace Operations Missions and Actions



Source: Joseph W. Kirschbaum et al., *DOD Cyberspace Operations: About 500 Organizations Have Roles, with Some Potential Overlap*, GAO-25-107121 (Washington, DC: GAO, September 2025), https://www.gao.gov/assets/gao-25-107121.pdf.

In scoping the Cyber Force, the commissioners discussed how historical precedent should inform the division of roles and responsibilities for cyber-relevant force generation between the Cyber Force and the existing services. For example, when the Air Force was created in 1947, the existing services defined the aviation capabilities they will need to retain due to their relevance to core missions. The Army, Navy, and Marine Corps still maintain a tremendous inventory of both fixed- and rotary-wing aircraft, with each service possessing more aircraft than most nations' air forces. However, the Air Force remains ultimately responsible for generating capabilities for the air domain, whereas the other services' aircraft operate in support of objectives for their respective warfighting domains.

Recent U.S. military operations, such as Operation Midnight Hammer in June 2025, which targeted Iranian nuclear program sites, have demonstrated this delineation of unique roles and responsibilities. In this case, sites were struck by B-2 bombers leveraging unique advanced precision munitions, protected by F-35 and F-22 fighter aircraft, all supported by multiple aerial tanker aircraft.[12] Despite the robust capabilities of the other services' aircraft, only the Air Force could have generated the forces needed to perform this operation.

Drawing this analogy forward to a Cyber Force, each of the existing military services has already built and independently operates their own networks, communications, and unique applications. A tactical commander must be able to securely operate their own technological footprint to be effective on the modern battlefield. The Cyber Force will not seek to gain control of these service-specific functions from the existing services. In fact, after the establishment of a Cyber Force, the Army, Navy, Air Force, Marine Corps, and Space Force will still need to retain personnel and capabilities related to technology management, use, and security for service-specific functions, applications, networks, installations, and weapons systems. Examples include the Navy destroyer's

hull, mechanical, and electrical systems or the mission planning systems within the Air Operations Center for U.S. Air Forces in Europe.

Consequently, absorbing and attempting to unify the numerous DOD networks and environments under the direct control of the Cyber Force was considered by the commission—and dismissed in short order. Any such alternative will be infeasible or impractical due to likely detrimental operational effects. In particular, it will overburden the Cyber Force from the outset to such an extent that it will detract from its core missions.

Size of the Cyber Force

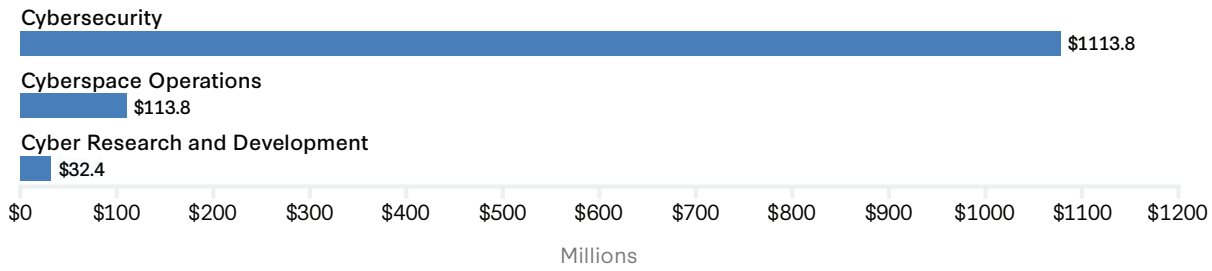
The appropriate size of the new service is a key consideration to inform the design of the Cyber Force. Based on congressional requirements, as well as the DOD's own design and planning processes, any service's size is measured in terms of total uniformed personnel. To be successful, the commission believes that Cyber Force requires a combined force of approximately 30,000 personnel, with an active-duty end strength of 20,000, a part-time component organized through a National Guard construct of 3,500–5,000 personnel, and approximately 5,000–6,000 civilians and contractors. As envisioned, the Cyber Force will be the second-smallest uniformed service, next to the U.S. Space Force (10,400 end strength for FY 2026).[13] Several considerations informed this estimate, including the size and composition of the existing forces aligned to cyber operations across CYBERCOM and the services today; historical assessments performed by Space Force, the GAO, and federally funded R&D centers; and the commissioners' own experiences and expertise. The commission arrived at this number after engaging in an analysis of existing cyber-aligned forces across the 440 organizations conducting offensive, defensive, and internal security operations in and through cyberspace across the DOD and Coast Guard, as well as the need for a net efficiency that consolidates redundant missions while focusing strictly on core OCO and DCO.[14] This size is intended to be large enough to provide the institutional tail and support functions required for service independence while remaining small enough to prioritize technical density and quality over mass, effectively providing a realistic shot at meeting mission requirements that the current smaller, fragmented pick-up team model cannot.

The commissioners also addressed the numerous, distinct cyber missions and organizations across the defense enterprise. The commission does not take the position that the Cyber Force should be responsible for generating capabilities across all of those missions. Therefore, the assessment in this report focused on the size of forces needed for the Cyber Force to accomplish core missions—specifically, generating capabilities for OCO and DCO—rather than for meeting all of the DOD's cybersecurity requirements.

Budgeting for Cyber Force

Approximating an appropriate budget will be an essential task for a new cyber service. At congressional direction, the DOD has been required to consolidate the total budget aligned to cyberspace operations, as distinct from cybersecurity investments, from FY 2017 onward.[15] The total budget, referred to as the Cyberspace Activities Budget, includes three categories: Cybersecurity, Cyber Operations, and Cyber Research & Development. An illustrative example for FY 2026 is depicted below.[16]

Figure 2: FY 2027 Cyber Activities Budget Request



Source: DOD Comptroller, *DOD Information Technology & Cyberspace Activities Budget Overview* (Washington, DC: DOD, August 2025), https://www.cape.osd.mil/content/SNAPIT/files/FY26/TAB%20A_FY26PB%20ITCA%20Budget%20Overview--Final.pdf.

Prior to 2024, this consolidated budget was divided between the Army, Navy, Air Force, and Marine Corps. As a result of a congressional requirement, however, CYBERCOM has since assumed responsibility for a significant portion of the budget from the services—approximately $2.9 billion out of the total $5.4 billion as of FY 2026.[17] This allocation, referred to as enhanced budget control (EBC), enables CYBERCOM to directly manage the resources aligned to the operations it conducts. While EBC includes funds for Operations & Maintenance (O&M), Procurement, and Research, Development, Test & Evaluation (RDT&E), it critically does not cover military pay and allowances (MILPERS), nor does it fund the facility support provided by the services. In the latest budget request, the DOD has requested $4.1 billion to CYBERCOM under EBC for FY 2027.

BUDGETARY PROJECTIONS

To inform its projections, the commission utilized DOD budget data from FY 2020 to today. Additionally, the commission spoke with subject matter experts on federal budgetary policy and process. Factoring in the president's FY 2027 budget request of $7.7 billion, the commission estimates that the Cyber Force will require an initial budget of roughly $10–$11 billion, covering all appropriations categories of O&M, Procurement, RDT&E, and MILPERS. Much of this funding will come through the reallocation of existing budgetary allocations rather than new and additional funding.

With a recommended size of 20,000 active-duty personnel, the commission estimates that requisite MILPERS funding (e.g., pay, bonus, and Tricare) for the Cyber Force will be approximately $2.541 billion, based on current MILPERS figures across the Army, Marine Corps, Navy, Air Force, and Space Force. For the proposed 5,000 personnel organized within the Cyber National Guard, the commission estimates an additional $216.6 million. This yields a total cost of approximately $2.758 billion for Cyber Force military personnel.

TIMELINE FOR BUDGET REALLOCATION

In estimating a timeline associated with budget reallocation, the commissioners reviewed the president's proposed budget for FY 2021, submitted to Congress in February 2020, only two months after the Space Force had officially been established in the FY 2020 NDAA.[18] Within two months, the Pentagon's financial management was able to revise the budget request to reflect and mechanically accommodate the newest branch of the armed forces. The example of the Space Force provides a

fair barometer for the Cyber Force. With nearly a decade of institutional experience in managing the Cyberspace Activities Budget as a unified portfolio between them, the commission believed that realigning defined elements from current accounts into a new Cyber Force account could occur in quick succession.

2

Implementation Plan

Timeline for Personnel Realignment

The initial implementation of the Cyber Force will be pivotal. The organizational complexity of integrating personnel across five disparate services, combined with an operating environment that continues to evolve, results in a variety of unknown and unknowable interrelated factors.

The history of the services' cyber roles and organizations demonstrates that early decisions and structures create institutional inertia and can limit the capacity for nascent organizations to rapidly adapt and evolve to meet personnel and operational demands in the future. The initial implementation period must therefore create the conditions for long-term DOD success in the cyber domain while minimizing any disruptive impact on ongoing operations. It will also be imperative for the implementation process to prioritize quality over quantity with respect to personnel. This must be a guiding principle that informs the build of the Cyber Force.

The primary philosophy for the Cyber Force's personnel transition should be adaptability and rapid experimentation. Some design decisions can be accurately planned in detail prior to implementation; others will inevitably rely on assumptions that prove incorrect or are derailed by completely unforeseen factors. Therefore, any implementation plan will need to contain sufficient flexibility to adapt and adjust as conditions, missions, and priorities change or emerge. That said, it is possible to build the initial core cadre of the Cyber Force in a relatively short period of time. Success on this front will result in operational units presented within 12–18 months, working alongside the existing cyber mission forces, which remain engaged through their respective services.

The Cyber Force should not simply "lift and shift" the existing workforce into the new service.

To accomplish this goal, the implementation plan must leverage the existing talent within the active-duty and reserve cyber mission force while creating a clear demarcation point for personnel to allow new models, modes of thinking, and organizational cultures to emerge. The Cyber Force should not simply "lift and shift" the existing workforce into the new service. While migrating existing operational cyber mission force units may be less disruptive in some regards, this approach will risk replicating existing challenges and threaten the long-term success of the Cyber Force's mission. Instead, the commissioners propose a phased and iterative approach that prioritizes force generation, the purpose motivating the creation of the Cyber Force, while mitigating against short-term disruptions to the cyber operational demands of today's joint force.

The Cyber Force should adopt the core principle of "probe, sense, adapt" within its planning to encourage institutional creativity and adaptability. As a result, this report's proposals are intentionally more descriptive rather than prescriptive the further out it projects into the transition. This enables the rapid and iterative testing of new ideas at the scale of acceptable loss to find the most effective methods for cyber force generation.

For example, the Cyber Force could adopt a competitive evolutionary approach to the design of cyber units. Within this approach, the Cyber Force will not commit to a single unit structure, which may be slow to perfect and will reduce future flexibility. Instead, the Cyber Force could adopt an agile approach that enables its workforce to rapidly adopt different unit structures and adapt from what it learns, using experiences to inform future decisions.

This design approach trades predictability for adaptability. While this is not typical within the existing services, it will enable the Cyber Force to meet the operational demands of the joint force while creatively overcoming its unique challenges within the boundaries of established law and DOD policy. Further, this approach reinforces the institutional culture of adaptability and innovation that is essential for success in the cyber domain.

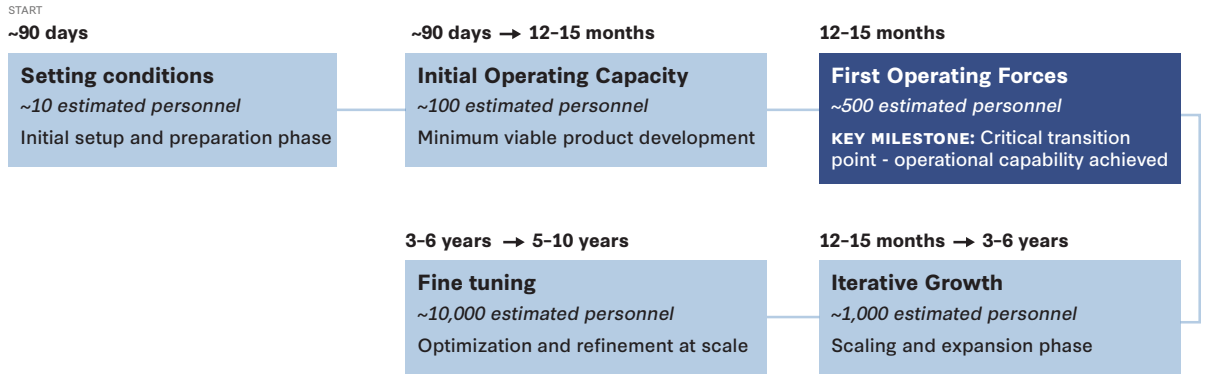
CONCEPT

Implementing and growing the Cyber Force should occur in four major phases: setting conditions, building the initial operating capacity, iterative growth, and ongoing fine-tuning. Within each phase, there will be milestones, feedback mechanisms, and iterative processes. The sequencing and details of these will vary as new information is learned and preconditions are met. An important measurable milestone is the point at which the Cyber Force presents its first operational unit to the joint force, requiring a critical mass of personnel and institutional capacity.

That said, while this milestone is crucial to meeting short-term operational demand, it cannot alone guarantee the enduring success of the service. Instead, a more significant (if difficult to measure) marker of success will be whether the institutional conditions of the Cyber Force are appropriately set. These more abstract indicators—the Cyber Force's organizational culture as shaped by its first leaders, the attributes it selects for, personnel and resource allocation, and other early and

recurring decisions—are critical for the Cyber Force to succeed in addressing DOD workforce demands from the start. Without a deliberate emphasis on these qualitative institutional conditions, the Cyber Force risks replicating existing force generation problems while incurring the up-front costs of starting a new service—an organizational worst-case scenario.

Figure 3: Timeline to Building the Initial Operating Capacity



Source: CSIS Commission on U.S. Cyber Force Generation.

PHASE 1: SETTING CONDITIONS

The first phase of the Cyber Force personnel transition begins with the decision to create a new cyber force generation organization and ends once conditions are set to begin implementation. This includes the capacity to initiate creation of the first operational units and begin an accessions and training pipeline. Success in this phase is based on selecting the right initial leaders and planning team, developing an effective model to assess personnel for the service, establishing a coordinated plan for the transition of selected personnel, and ultimately setting the right organizational culture. This phase should be accomplished within 90–120 days of the creation of the Cyber Force.

In this view, within two weeks of the decision to create a service, the DOD will create an initial planning group that will include a select team of military personnel and outside experts. They will be responsible for assessing the conditions and existing assumptions shaping Cyber Force implementation. The initial planning group will then identify the immediate next steps and form working groups focused on specific tasks and topics. This will include identifying and consulting with necessary subject matter experts beyond the expertise of the initial planning group, along with the identification and onboarding of more personnel to complete specific tasks.

In this phase, the Cyber Force planning staff will rely on borrowed resources and administrative support while securing longer-term resources. Particular care must be taken in selecting the core planners and minimizing the number of people implicitly picked for a service without a deliberative process. Given the diverse nature of the military's current construct for cyber operations, consideration should be given to the selection of planners with operational experience from across existing services, mission types, and grades to represent the total cyber mission workforce.

Within the first 45 days, more permanent task groups will form. While there is a range of approaches the initial planning group could adopt, several critical topic areas warrant dedicated effort. These include two teams: an assessment team that will focus on creating assessment criteria, selecting additional personnel, and building formal processes; and an administrative team focusing on necessary support functions for the service as a whole, including pay, funding, facilities, and contracts. The guiding principle for the assessment team is a ruthless focus on quality over quantity. It should be evaluated for its capacity to select highly qualified candidates, regardless of the rate of selection. This means the transition assessment should be biased toward false negatives or selecting fewer individuals in the initial rounds of selection. In practical terms, the existing senior cyber work role standards could be used as the baseline expectation for the Cyber Force.

As the Cyber Force builds the capacity for accessions, a unique assessment should be created to select for the strongest potential candidates with feedback mechanisms from the operational force. Both the transition and accessions assessments will continue to evolve to ensure the quality of Cyber Force personnel. Eventually, the personnel selection process may be integrated into Cyber Force recruiting and training functions.

Additional key focus areas for the planning teams should include training and education, operations, and capabilities. These focus areas may start as ad hoc working groups, eventually transitioning into formal teams or dedicated organizations as the Cyber Force develops. The personnel assigned to these teams will continue to evolve over time to align necessary expertise. Initial planning personnel may move between teams within the Cyber Force or return to their parent services as tasks are accomplished. The primary goals for these teams will include the following:

- The goal of the **training and education teams** will be to plan for initial training and education of Cyber Force candidates. This includes reviewing operational work roles, common lexicon, and foundational knowledge, as well as developing concepts and metrics for initial and advanced training and educational requirements. These efforts will set conditions for the eventual enduring training and education models.
- The goal of the **operations teams** will be to plan and set conditions for the presentation of forces to operational commands. This includes the development of concepts of employment, processes to develop unit structures, and requirements for personnel and equipment (e.g., hardware and software).
- The goal of the **capabilities teams** will be the development, acquisition, and management of the hardware and software solutions required by the Cyber Force. The initial focus will be on supporting the other two areas while determining the processes and structures required for longer-term solutions. Planning efforts must address the division of responsibilities between CYBERCOM and the new service.

Throughout the "setting conditions" phase, total personnel numbers will incrementally increase. Personnel may participate in multiple teams and move to more dedicated or permanent positions as the teams mature. There will also be turnover as detailed personnel return to their parent organizations, subject matter experts are no longer needed, and permanent personnel are assigned or hired.

This phase can start under the direction of a carefully selected temporary transitional leader. However, it is imperative that, by the end of this phase, a senior leader in the Cyber Force is selected. At a minimum, this person will be the leader of the force-generating organization. In the longer term, they may become the inaugural Cyber Force chief.

Selecting the first senior leader will be a critical step in creating the Cyber Force's culture. This leader's task will be uniquely challenging, even when compared to previous inaugural service leaders. Unlike the Air Force and Space Force, which drew predominantly from a single service, the Cyber Force senior leader must integrate personnel from every military service and reflect the distinct culture and mission of the organization. The Cyber Force initial planning group should consider a range of hiring practices, including those from the industry, and should consider leaders with a broad range of operational and institutional cyber leadership from across the active-duty, reserve, joint, and interagency community.

PHASE 2: FIELDING THE INITIAL OPERATING CAPACITY

The second phase of Cyber Force implementation is fielding the initial operating capacity. This phase begins when the initial Cyber Force implementation team has consolidated the necessary resources to begin transitioning personnel into the Cyber Force and ends when the first Cyber Force operation units are presented to the operational force. Success in this phase is based on validating the personnel transition process, integrating selected personnel into the initial concepts for force presentation, and beginning to ingrain the new Cyber Force culture and vision into its personnel while minimizing disruption to the existing operational cyber mission forces. This phase should be accomplished within 12–15 months from the creation of the Cyber Force.

Phase 2 is focused on creating the first training and operational units from selected personnel. The first Cyber Force units should not be built to the exact model of the existing teams. Instead, the Cyber Force should assess the appropriate minimal unit size and the quantity and mix of skills needed for identified operational missions, without excessive dependencies to their internal construct. Additionally, the units should be presented with dedicated intermediate staff sufficient to manage their operational integration challenges. For OCO, the Cyber Force may consider generating forces of similar scale and capability to the Cyber National Mission Force Joint Task Force or the Task Groups used by other headquarters. For DCO, the Cyber Force may consider a minimum scale comparable to between one and two Cyber Protection Teams of 40–80 personnel, with an additional 5–15 staff assigned to manage operational planning and integration. These estimates should be informed by, and continue to mature and evolve with, concepts of employment for Cyber Force personnel.

In staffing initial civilian personnel for the Cyber Force, efforts should be made to leverage the U.S. Tech Force, "an elite corps of engineers to build the next generation of government technology," which will be placed at major departments and agencies, including the DOD. This initiative offers an opportunity to enable unique skills from the commercial sector to be deployed for national cybersecurity missions.[19]

> The primary focus for initial Cyber Force implementation stages should be the presentation of OCO and DCO capabilities to the combatant commands. However, the Cyber Force will also need to eventually provide organic capability development at echelon and may decide to provide more specialized capabilities such as red teams, initial access teams, or other dedicated expertise to accomplish a given mission requirement. These more specialized functions could be presented as discrete capabilities provided by new units, or they may be added to larger units as those units grow and internally organize.

Fielding the first operational Cyber Force units requires attaining a critical mass of personnel with a representative composition of skills from the existing cyber mission force. These personnel may be selected from existing formations, drawn from reserve forces, or directly assessed from outside military service. The timing of personnel transfers should be deliberate to nest with implementation plans and provide predictability to the services. Highly qualified candidates may be selected but not transition immediately, based on factors that could include their assessed skills, the status of the implementation timeline, and the needs of the existing cyber formations.

The planning team should evaluate a range of concepts for the transition of personnel. Regardless of the specific details, Cyber Force planners should develop a concept that is adaptable and scalable and that moves with purpose toward establishing a high standard for all Cyber Force units. Finally, and perhaps most crucially, the selected transition plan must be developed to receive personnel from a wide range of sources and integrate them into the Cyber Force's organizational culture.

The transition and integration program is decisive for ensuring that the Cyber Force does not replicate existing problems. Instead, the program must communicate the shared vision and language upon which the service will build new paradigms optimized to the unique demands of cyberspace. The goal of the transition and integration program is to serve as a shared cultural demarcation between members' prior services and the Cyber Force. Its primary purpose is to build the shared culture of technical excellence, adaptability, and innovation necessary for the Cyber Force and the joint force to succeed in the cyber domain. The transition program may also include training to prepare candidates for specific roles or provide a common technical baseline. Cyber Force planners should thus explore a wide range of concepts and acknowledge that their program will invariably evolve over time.

One potential transition concept will be structured around future unit composition. In this concept, the Cyber Force will assess a wide range of individuals while developing the initial unit compositions. Once the necessary personnel have been identified to meet the projected unit composition, those individuals will transfer into the Cyber Force, complete an integration program to build the culture and unit cohesion, complete their collective training and certification, and then be presented to the operational commands. This process will then be refined and repeated throughout the subsequent phases of Cyber Force implementation. This concept is one of many that the Cyber Force planners could evaluate. It is meant as an example and not as prescriptive guidance.

Regardless of the adopted transition concept, the fielding of new Cyber Force units will be integrated into existing cyber mission force allocation plans and will allow an equivalent number of teams (currently provided by existing services) to be deactivated. Some of those personnel will be selected to transition into the Cyber Force and then integrated and assigned to constitute future units. Other personnel will be redistributed to other teams within their parent service, with the potential of a future transition to the Cyber Force. The goal is to rapidly integrate and field operational units from the existing cyber workforces of the services while limiting the negative impact to ongoing operations to the maximum extent possible.

The number of teams presented to CYBERCOM by the existing services has grown over the years, and the allocation of these forces has changed, both in routine fashions and in response to crises. Despite attempts at standardized teams, the cyber mission force is already composed of disparate units varying in composition, task organization, and capability. In the short term, Cyber Force units will be one more set of units for CYBERCOM and its subordinate operational headquarters to array against its requirements. As the Cyber Force matures and grows, it will likely present the majority of forces and intermediate headquarters to CYBERCOM. However, the other services may continue to invest in specific service-retained cyber capabilities that will continue within the existing force employment model.

In addition to developing the first operational units and the integration program, the Cyber Force must prioritize the development of training for critical work roles or those with long training pipelines, such as operators and exploitation analysts. As these training pipelines can take 12 months or longer, identifying and qualifying newly assigned personnel in these work roles requires starting early. Personnel in these work roles are often tasked to support other organizations. Therefore, the Cyber Force should consider presenting them as individual augmentees to the National Security Agency (NSA) and CYBERCOM organizations until such time that a critical mass of personnel in the Cyber Force is reached to constitute units. This approach has the additional benefits of addressing one of the major training challenges immediately, relieving a persistent burden from the existing services, and ensuring a high initial technical baseline for the Cyber Force. It should be noted that the Cyber Force does not need to use the current training model, provided that its training standards are accepted by the operational stakeholders. In other words, the Cyber Force could have a longer pipeline or higher standards, or it could even provide training for personnel to move interchangeably between NSA and CYBERCOM.

Developers are another work role with a long training period that should persist in the Cyber Force. Thus, beginning training early is essential. On the defensive side, there are no equivalent pipelines for the Tier-1 work roles of analytic support officer and data engineer. However, the Cyber Force should evaluate its priorities in training personnel that can accomplish these functions, and it should assess whether that training should be distinct from or overlap with any other training. The Cyber Force should also consider integrating training and educational requirements to reduce the downtime before an individual is mission capable without sacrificing quality or rigor. Similarly, training should include opportunities for individuals to demonstrate their competency at required skills to minimize training that is rudimentary or redundant. Such analysis is outside the scope of this report but is essential if a service is going to mature new methods of operations rather than merely adopt those that evolved over time based on factors that may be irrelevant or obsolete.

Throughout the fielding phase, the planning teams will continue to refine and develop concepts and prepare resources for the further growth of the Cyber Force. For example, the planning teams will continually refine the initial assessment process to select additional personnel. The goal is to mature into more permanent programs to bring in personnel for both civilian and uniformed positions from within and outside the military. Similarly, the training, education, and integration programs will need to be continually evaluated and refined, adding capacity and meeting a broader set of requirements.

In all cases, the Cyber Force should seek to develop models grounded in the fundamental attributes of the cyber domain and its forces rather than defaulting to the models of the existing services. While large industrial models of force generation may make sense for some of the existing services, tailored and integrated approaches will likely be preferable for a cyber service. For instance, if an operational headquarters is the only user of a program of record, it may be appropriate for management of the program to reside inside those headquarters rather than in an organizational equivalent to the Army's Materiel Command.

PHASE 3: ITERATIVE REFINEMENT AND GROWTH

The third phase of the Cyber Force implementation is iterative refinement and growth. This phase begins when the first Cyber Force units are presented for employment with the joint force and ends when the Cyber Force is the primary source of cyber personnel for the joint community. Success in this phase is based on scaling the personnel transition process while maintaining quality, refining concepts for force presentation tailored to different joint requirements, and beginning organic recruitment and accessions at scale. This phase should be accomplished within three to four years from the creation of the Cyber Force.

The Cyber Force must grow its presented force from the first defensive and offensive capabilities to the point where it provides the preponderance of cyber combat power and is able to meet the obligations specified in the revised Title 10 and joint concept documents. This growth must prioritize quality, never losing sight of its goal of providing a cyber force that is more effective and optimized for the unique demands of cyberspace. The "race to FOC"—or full operational capacity—is

imperative and should avoid historical problems found during the initial build of the cyber mission force. Speed during the transition is imperative, and unnecessary delays stemming from "decision by committee" may result in self-inflicted institutional harm.

Throughout the growth phase, the Cyber Force must continue to increase both capability and capacity. It will expand its core capacity for OCO and DCO while developing and fostering critical supporting functions, such as capability development, reverse engineering, red teaming, strategy and doctrine, dedicated legal expertise, threat intelligence, and vulnerability research. These supporting capabilities may start as independently presented forces but should gradually integrate organically at echelon within larger cyber units.

A key milestone will be the creation of the first O6 or O7 operational command (equivalent to the group/brigade/wing level for the other services). This operational command will be comparable in size and scope with the present institutional construct for one of the six service components under CYBERCOM, combining the capacity for operational planning and units of action. This unit will organically provide most operational support and can be presented as a Cyber Force Component Command, detailed later in the report.

On the longer term, however, Cyber Force growth should not simply be a matter of replicating the initial fielded units. First, there will be lessons learned and the operational context will evolve. Second, any growth could include new functions and capabilities. Third, the right mix of forces to build higher-level formations will vary by mission, be that informed by the supported command or by the adversary. As such, one cyber group may have different requirements for capability development than another. Like a Marine Air-Ground Task Force or a joint force commander, there will be a set of core functions for which the combat power may be tailored temporarily or enduringly. However, for the Cyber Force, this tailoring may occur at lower echelons than traditionally seen across the joint force. Finally, alternate unit structures should be developed and evaluated to provide opportunities for comparative lessons learned.

Throughout the growth phase, the work of the original planning teams will likely be formalized within the Cyber Force headquarters. These staff elements will continue to direct concept refinement and coordinate Cyber Force resources within the joint community. During this phase, the Cyber Force staff should evaluate and begin creating the necessary major commands in addition to the operational headquarters discussed previously. The appropriate scope and function of these headquarters will be informed by the progress of implementation to that point. However, they could include equivalents to the Army Transformation and Training Command or the services' recruiting commands. Within this phase, the Cyber Force staff should coordinate with the joint community to consolidate and optimize cyber education and training for the joint force.

For implementation purposes, the growth phase ends once the Cyber Force is the primary provider of cyber operational forces and headquarters to the joint force. The Cyber Force would present forces to the Joint Forces Headquarters–Cyber and Cyber National Mission Force. The growth phase of the Cyber Force implementation should seamlessly transition into its enduring force management process, which will govern future growth, reduction, and changes to structure.

PHASE 4: FINE-TUNING

During the growth phase, the Cyber Force will replace the majority of cyber forces presented by the other services. However, it may continue to rely on the existing services for specific functions or specialties. During the fine-tuning phase, however, the Cyber Force will coordinate with other services to identify the long-term plan for these functions and specialties. These plans may include committing to reliance on another service, such as for medical providers; using the training pipeline of another service, such as airborne or judge advocate general training; transitioning training to the Cyber Force; or hiring Cyber Force civilians with the appropriate skills. This last option will be the case for most administrative functions.

In addition to personnel aspects, the fine-tuning phase should encompass all supporting and service functions, including facilities, service contracts, basing considerations, programs of record, garrison services, and a host of other details to support the mission.

The Cyber Force should not seek growth for growth's sake. The benefits of vertical integration, scale, and control risk a loss in agility and focus. Additionally, the existing services inherently offer better economies of scale given their absolute sizes. For functions that are neither core nor operational and cannot be fulfilled by the Department of the Army (should the Cyber Force be established within it) or an existing service, the default solution should be civilians or contracted support. In all cases, the overriding considerations must be enabling mastery and operational adaptability within the cyber domain.

Force Composition

The commission envisions the Cyber Force as a relatively small military organization that meets the requirements of the operational force by focusing on quality and adaptable cyber domain expertise. In addition to an active-duty component, the commission recommends a part-time component, along with a complement of civilian personnel permanent forces that will be bolstered by strong relationships with industry, academia, and international partners. This should include the ability to rapidly integrate expertise from the proposed Cyber National Guard and outside the military to meet the evolving requirements of the domain and the mission.

To be successful, the commission recommends the Cyber Force total approximately 30,000 personnel—comprising an active-duty end strength of 20,000, a part-time component organized through a National Guard construct of 3,500–5,000, and around 5,000–6,000 civilian and contractor personnel.

To be successful, the commission recommends the Cyber Force total approximately 30,000 personnel—comprising an active-duty end strength of 20,000, a part-time component organized through a National Guard construct of 3,500–5,000, and around 5,000–6,000 civilian and

contractor personnel. The level and specific makeup of military and civilians providing augmented expertise will vary, but it should be built into the force structure from the start.

The Cyber Force should define its workforce by enduring mission functions rather than by temporary tradecraft. It will require personnel to conduct operations, provide operational support, and perform administrative functions. Occupational categories might include OCO, DCO, intelligence, capability development, and infrastructure. Individuals may specialize within occupational categories—focusing on specific functions such as on-net operations, threat intelligence, analytic development, and targeting, for instance—or generalize within or across categories to plan operations and lead cross-functional teams.

The Cyber Force will also need specialists from other fields with cyberspace familiarity for such purposes as operational law, budgeting, and acquisitions. Finally, the Cyber Force will need personnel to efficiently perform administrative tasks, such as maintaining facilities, managing payroll, and providing physical security. By grouping personnel into broad occupational categories within which they can specialize or generalize, the Cyber Force will preserve distinct competencies, support future changes in how cyber missions are conducted, and create a professional identity strong enough to anchor training, career development, and long-term readiness.

Uniformed Personnel Model

BACKGROUND

As organized today, the services have leveraged force structure models built to reflect their respective priorities, whether that be littoral combat for the Marine Corps or complex ground maneuvers for the Army. While this is appropriate for their core missions, the services have applied these same models to cyberspace, irrespective of whether they are applicable to the domain. In the case of the Army, Navy, Marine Corps, and Air Force, cyber components reflect their service constructs.[20] Regardless of service, any location participating in cyber operations today will be principally enlisted personnel, managed and overseen by a smaller number of commissioned officers, with few warrant officers. For each service, officers are expected to provide leadership, warrant officers will contribute technical expertise, and the enlisted personnel will perform hands-on work.

However, these legacy constructs do not directly translate when applied to cyberspace. For example, the Navy, Marine Corps, and Air Force have all judged aviation to be sufficiently complex and technical that all pilot positions are reserved exclusively for commissioned officers, while the Army expands that to include warrant officers. Many of the more technical and complex work roles within the cyber ecosystem (e.g., developer, operator, and exploitation analyst) are inconsistently filled across the services (see Table 2). Officers often serve as frontline managers, though they may not possess the commensurate technical know-how.[21]

Across the services, the same cyber operational work roles are performed by individuals of different ranks and with different benefits, frequently resulting in two individuals from two separate services performing the same functions but being paid at vastly different rates. In 2022, a GAO audit found a complex overlap of military career fields aligned to the CYBERCOM work roles.[22]

Table 2: U.S. Cyber Command Work Roles

		U.S. Cyber Command Work Roles		
		Developer	*Operator*	*Exploitation Analyst*
Service Career Fields	Army	Cyber Capability Development Officer/Technician (17D/170D)	Cyber Warfare Officer/Technician/Specialist (17A/170A/17C)	
	Navy	Cyber Warfare Engineer (1840)	Cyber Warrant Officer (7840)	
			Cryptologic Warfare Officer (1810)	
			Information Profressional Officer (1820)	
		Cryptologic Technician Networks (CTN)		
	Marine Corps		Cyber Defensive Operator (enlisted) (1721)	
			Cyber Operations Chief (enlisted) (1799)	
	Air Force	Computer Systems Programming (3D0X4)		Network Intelligence Analyst (1N4)
		Cyber Warfare Operations (1B4)		
		Cyberspace Effects Operations Officer (17S)		

Source: Brenda S. Farrell et al., *Government Accountability Office, Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking*, GAO-23-105423 (Washington, DC: GAO, December 2022), https://www.gao.gov/assets/d23105423.pdf.

The CYBERCOM 2.0 effort acknowledges this issue and suggests institutional ways to remedy it.[23] While the effort is a necessary and positive step for improving cyber force employment, uncertainty over the effort's resourcing and implementation prospects provided an opportunity for the commission to consider a wider range of lasting reforms that a Cyber Force could institutionalize.

CONSIDERATIONS

In extensive discussions, the commission considered three possible models for uniformed force composition. Each currently exists within the U.S. government, with two in use by uniformed services not considered part of the armed forces: the United States Public Health Service (USPHS, within the Department of Health & Human Services) and the Commissioned Officers Corps of the National Oceanic and Atmospheric Administration (NOAA Corps, within the Department of Commerce). Importantly, commissioners agreed that regardless of determination on uniformed force composition, a Cyber Force must be augmented by both civilian and contract personnel.

The commission examined the following options for uniformed force composition:

1. Military service comprised of commissioned officers, warrant officers, and enlisted personnel (present Armed Forces model)
2. Military service comprised of commissioned officers and warrant officers (USPHS model)[24]
3. Military service comprised exclusively of commissioned officers (NOAA Corps model)

The commission also examined the traditional "pyramid" design for retention, advancement, and promotion. This structure for personnel management drives the Armed Forces' up-or-out model, which provides little flexibility—not to mention insufficient structure for individuals to develop both the strong technical foundations and the operational knowledge required for operations in the cyber domain.

RECOMMENDATION AND ANALYSIS

The commission recommends that the Cyber Force adopt the USPHS precedent, building its force to consist of commissioned officers and warrant officers, but without an enlisted cadre. This recommendation is based on the uniquely specialized skill sets and attributes so valuable as to merit the rank and respect of a warrant officer, as well as the commensurate pay and compensation to match the individual's contributions.

Within the current ecosystem, enlisted personnel are performing a portion of operations, with the expectation that they will serve as both tactical leaders and technical advisers or subject matter experts. However, given their incredible intellect, skill, and attributes, combined with leadership by competence at the moment of need, these operators and analysts are more like commissioned officers. In addition, the enlisted pay scale cannot adequately compensate this community, even with pay incentives and special duty bonuses. Due to the technical nature and lengthy training pipelines for cyber experts, commissioners struggled to justify applying the enlisted pay scale to them, which is often half the compensation of a new warrant officer.[25] However, technical expertise is at the core of the warrant officer corps, making warrant officers an important element of the Cyber Force.

Table 3: Enlisted and Officer Personnel in Military Service Branches

Service Branch	Enlisted	Officers	Total	Ratio of Enlisted to Officers
Army	353,326	92,014	445,340	1.8 to 1
Navy	272,792	55,144	327,936	4.9 to 1
Marine Corps	151,755	21,341	173,096	7.1 to 1
Air Force	251,412	60,508	311,920	4.2 to 1
Space Force	4,872	4,574	9,446	1.1 to 1
Total DOD	1,034,157	233,581	1,267,738	4.4 to 1

Source: Defense Manpower Data Center, "Active Duty Military Personnel by Service by Rank/Grade (Updated Monthly)," U.S. Department of Defense, September 2024, https://dwp.dmdc.osd.mil/dwp/app/dod-data-reports/workforce-reports.

According to the DOD's most recent demographics report from 2024, there are 4.4 enlisted personnel for every officer on active duty. The Space Force has the lowest ratio of enlisted members to officers (1.1 enlisted personnel for every officer), while the Marine Corps has the highest (7.1 enlisted personnel for every officer).[26] Given the technical nature and extended training timelines

required, commissioners estimated that, were it to include an enlisted cadre, the Cyber Force's enlisted-to-officer ratio will more closely resemble that of the Space Force than the Marine Corps. Considering a legacy pay scale, the commissioners could not articulate valuable reasons to preserve enlisted rank structure when the same individuals could continue their service as warrant officers.

This approach also mirrors best practices found in the industry, where advancement can occur via a technical track or a managerial track. When overlaid with a military model, commissioners viewed parallels between expectations for warrant officers with industry expectations for technical leaders, and they compared the expectations for commissioned officers with those on the managerial trajectory.

Non-Uniformed Force Composition

The commission unequivocally emphasized the value of civilian and contract personnel to their uniformed counterparts. While the Cyber Force will be anchored to its military personnel, it will also benefit from a civilian and contractor workforce, just as no service exists today without civilians and contractors. Across the existing services, civilian personnel serve in critical work roles and positions, including as capability developers and on-net operators. Within the Cyber Force, they should continue doing so to allow additional paths for personnel to serve. These personnel should qualify for the future equivalent of the Cyber Excepted Service pay scales and for skill pay equivalent to the military personnel.

As noted earlier, the commission estimated that a civilian complement of 5,000–6,000 personnel, or up to 30 percent relative to the size of the uniformed force, was a useful barometer for related discussions around planning, programming, and budgeting.

Civilian expertise should be integrated as a permanent part of the workforce, especially in capability development, mission engineering, specialized analysis, research, testing, and training infrastructure. Contractors should support surge capacity, infrastructure, and other non-inherently governmental functions. However, core mission authorities, stewardship of long-term operational resources, and sensitive operational judgment should remain with government personnel.

Active, Guard, and Reserve Components

As with force composition, commissioners understood the opportunity to apply new frameworks to this dynamic issue set. Presently, the military services' active components are complemented by cyber units in their respective reserve components, the Army National Guard and the Air National Guard. However, both the DOD and Congress have signaled that the current model is insufficient to harness the talent resident in both the Reserve and National Guard components. Despite 16 separate legislative efforts by Congress from 2015 to 2026 to improve Guard and Reserve utilization, the military departments inadequately implemented these mandates due to competing priorities in other domains. Last year, then-Acting Commander Lt. Gen. William Hartman testified to the House Armed Services Committee that CYBERCOM was seeking new pathways to access expertise in the National Guard and Reserve, and that he was seeking additional ideas from Congress.[27]

Table 4: Reserve, National Guard, and Auxiliary Components of Military Services

Armed Forces	Reserve	National Guard	Auxiliary
Army	X	X	
Marine Corps	X		X
Navy	X		X (in times of war)
Air Force	X	X	X
Coast Guard	X		X
Space Force			

Source: CSIS Commission on U.S. Cyber Force Generation.

To complement Cyber Force's active component, the commission considered the following options:

1. Cyber Force Reserve
2. Cyber National Guard
3. Cyber Force Reserve *and* Cyber National Guard

The commission recommends establishing a Cyber National Guard, rather than Cyber Force Reserve. The commission does not recommend establishing both a Cyber National Guard and a standing Cyber Force Reserve.

Commissioners universally endorsed the need and value of a part-time component that could take the form of either a Reserve or National Guard component. However, the commission judged that a single organizational design for the part-time component was more economical and efficient than building both. In determining whether to recommend a Cyber National Guard or a Cyber Force Reserve, the commission considered the former to be a greater benefit than the latter, as a National Guard can be leveraged under both federal and state authorities, whereas a Reserve component can only be leveraged under federal control.

Commissioners also began exploring unique mission sets that could be assigned to a Cyber National Guard. One function which had particular applicability could be a specialization in operational technology (those technologies that support industrial and critical infrastructure around the country). With the ability to be leveraged by both state and federal authorities, a Cyber National Guard will be uniquely positioned to assist in recovery from cyberattacks against critical infrastructure owners and operators.

Cyber Workforce Roles and Specialties

The Cyber Force should organize its workforce around a small number of enduring specialty job families supported by stackable mission qualifications, rather than a large catalog of narrow job titles tied to current workflows. This approach will give the service a stable professional structure while preserving flexibility as tools, mission processes, and the relationship between analysis,

preparation, execution, and assessment continue to evolve. Roles should be defined by mission function and decision responsibility, not by temporary task boundaries or current platforms.

Offensive cyberspace operations should encompass mission preparation, mission execution, maneuver in and through target environments, access employment, effects delivery, and assessment of operational effects. Defensive cyberspace operations should include mission defense, incident response, hunt, and expeditionary defensive support to the joint force.

The core specialty job families should be OCO, DCO, operational preparation of the environment and access sustainment, intelligence and target analysis, and capability development with mission engineering. OCO should encompass mission preparation, mission execution, maneuver in and through target environments, access employment, effects delivery, and assessment of operational effects. DCO should include mission defense, incident response, hunt, and expeditionary defensive support to the joint force. Because the Cyber Force is intended to focus on OCO and DCO rather than on the broader DODIN enterprise, routine network administration and general enterprise IT should remain outside the core occupational model except where directly tied to operational mission systems.

Operational preparation of the environment and access sustainment should stand as a distinct specialty family, responsible for long-duration preparation of target environments, development and sustainment of placement and access, maintenance of approved operational infrastructure and identity resources, and other activities required to set conditions for later action. Intelligence and target analysis should include technical analysis, target systems analysis, network mapping, dependency analysis, and the human, organizational, and behavioral dimensions of target development that shape access planning, target interaction, and assessment. Capability development and mission engineering should include software development, tool engineering, exploit and access development and employment, test and evaluation, integration, sustainment, and continuous mission support.

Mission planning, targeting, assessment, and mission integration should be treated as cross-cutting qualifications employed across these specialty families rather than as isolated career silos. The same should be true of selected advanced qualification areas for specialized target environments and mission problem sets, including industrial control systems, telecommunications, cloud environments, space-related dependencies, and other high-demand operational areas.

This structure preserves important distinctions without creating unnecessary stovepipes. Operations, environment preparation, intelligence, and engineering are not the same function and should not be collapsed into a single specialty merely because they often support the same

mission. At the same time, personnel should be able to hold multiple qualifications across adjacent specialties as operational practice changes. The Cyber Force should therefore rely on broad specialty families with stackable mission qualifications instead of hard coding every task into a separate permanent role.

From a common foundation, personnel should move into primary specialty qualification, mission qualification, advanced certification, and recurring requalification. Within the officer- and warrant-based personnel model proposed above, both career tracks should allow members to remain technical and operational at senior grades. The service should support parallel paths for mission leadership, technical leadership, and capability leadership rather than forcing advancement through generic administrative roles. A notional career path should therefore move from common foundational preparation, to specialty qualification, to advanced mission certification, and then to senior mission or senior technical tracks.

Recruiting and Developing the Force

To cultivate the necessary expertise across the required workforce roles described above, the Cyber Force must begin by recruiting the right people and empowering them throughout their careers through education, training, and assignments, all while emphasizing promotion and retention.

The Cyber Force will need to have greater emphasis on permeability and lateral entry than the other services. This diverges from the general military model, where personnel enter service at the same ranks and higher ranks are managed through promotion and attrition. Additionally, the Cyber Force will foster a degree of specialization greater than what is generally attainable in those forces that have high turnover and that must be prepared to replace large amounts of combat losses. The key focus of Cyber Force recruitment efforts will be cyber domain expertise, primarily for those conducting operations but also, to a lesser extent, for those providing operational support.

UNIQUE RECRUITMENT REQUIREMENTS AND APPROACH

The Cyber Force should recruit for quality, mission relevance, and long-term adaptability. It should preserve access to narrowly valuable technical expertise while also identifying candidates who can grow into high-demand roles. While any service must possess generalists, a Cyber Force must prioritize building a force of specialists and future specialists whose technical excellence is consistently tied to operational purpose.

Because small numbers of highly capable personnel can generate outsized operational effects, the service should recruit for uncommon technical aptitude, judgment, discretion, adaptability, and demonstrable mission relevance.

The Cyber Force should adopt a recruitment model built on selectivity rather than scale. The objective should be to identify and attract individuals who can create disproportionate operational

value, not simply to fill authorizations. Mass does not equate to force in cyberspace. Because small numbers of highly capable personnel can generate outsized operational effects, the service should recruit for uncommon technical aptitude, judgment, discretion, adaptability, and demonstrable mission relevance.

Recruitment should therefore be designed to attract two populations at once. The first is candidates who already possess specific high-value technical skill sets relevant to Cyber Force missions. The second is candidates with the cognitive profile, discipline, and learning velocity to develop rapidly into demanding specialties. The service should keep the door open to highly specialized talent rather than treat breadth for its own sake as the preferred model.

The Cyber Force should avoid a stovepiped approach to recruitment that treats technical activity as an end in itself. However, this should not be mistaken for a preference for military generalists. The service should recruit specialists and develop specialists. The Cyber Force must also ensure that candidates understand that their technical expertise must be applied to operational purpose. The issue is not whether a recruit is narrowly skilled, but whether that skill can be translated into mission effect, effective teamwork, and disciplined service. Recruitment should therefore favor candidates who can connect technical excellence to military outcomes.

Familiarization with other warfighting domains should be treated as an important part of early professional formation, not as a threshold requirement that unnecessarily narrows the pool for junior officer and warrant officer entrants. Prior military experience, prior service in another domain, or preexisting operational fluency should be viewed as advantages where present, especially for direct commission or more senior entry, rather than as prerequisites for initial recruitment. The Cyber Force should recruit primarily for mission-relevant aptitude and skill, then build broader joint understanding through education, training, and operational exposure.

The service should also recruit against enduring mission needs rather than temporary technology fashions, given the rapid pace of technological advancements in cyberspace. External credentials, certifications, academic pedigrees, and commercial résumés should be treated as useful indicators. However, they should not serve as substitutes for direct assessment of aptitude, suitability, and potential for service. Recruitment should be supported by deliberate relationships with universities, technical communities, industry, and other public sector talent pools to reach both emerging and mature talent without outsourcing standards of selection.

The Cyber Force should not rely on a single accession path. It should access junior officers through dedicated pre-commissioning and officer candidate pathways; experienced civilians through direct commission; prior-service personnel through interservice transfer; and warrant officers through a distinct technical accession pathway, open to both prior-service and qualified civilian specialists. Because the Cyber Force will not maintain an enlisted force of its own, it cannot depend on a traditional internal feeder base for warrant officers. Its warrant accession model should therefore be designed from the outset to identify and appoint mature technical talent directly into warrant service where mission needs justify it.

SIMPLIFIED AND CONSOLIDATED ACCESSION PROCESS

The Cyber Force should streamline accession administratively and technically, whether for initial entry, direct commission entry, or rejoining active duty. Rather than force applicants through a slow sequence of disconnected approvals, the service should use a single case-managed pipeline that coordinates recruiting, technical screening, medical review, security processing, appointment actions, and training assignment. Applications should be accepted on a rolling basis, evaluated by standing selection panels, and processed through parallel administrative actions wherever possible. Priority applicants should be matched early to projected training seats and mission categories to reduce unnecessary delay between selection and entry on duty.

Constructive service credit should be available for experienced applicants whose prior military or civilian work demonstrably aligns to Cyber Force requirements. This authority should be used carefully, but it is necessary if the service intends to compete for mature technical talent and bring in experienced personnel at grades commensurate with their qualifications. The same accession framework should support both full-time and part-time entry, allowing the Cyber Force to draw talent from the civilian labor market without requiring every qualified applicant to enter through a traditional full-time career path.

The Cyber Force should treat accession as a specialized force generation system rather than an administrative intake process. A unified accession architecture with multiple entry paths, rigorous technical validation, streamlined processing, and built-in support for both full-time and part-time service will better align with the needs of a small, highly technical officer- and warrant-officer-based service.

The Cyber Force will also take responsibility for the deliberate longitudinal assessment and improvement of selection criteria over the duration of an individual's career. The Cyber Force will develop a structured data collection process that integrates the performance of selected candidates as they progress through their initial training, ongoing professional education, and mission performance to identify and refine key indicators of future performance in the cyber mission force. These insights will be used on a continuous basis to improve the ongoing assessment and selection process. This deliberate feedback system will also integrate with the retention processes and solicit ongoing feedback from both operational commands and individuals. As the cyber domain evolves, the Cyber Force will likewise adapt to ensure it is selecting the most talented and capable force possible.

Service Culture and Doctrine

Each of the military services is defined by a distinct organizational culture that reflects the demands of warfighting in its respective domain. It will thus be imperative for the Cyber Force to foster an organizational culture that reflects the unique aspects of warfighting in and through cyberspace.[28] Such values, identities, norms, and attributes will likely be different from those embraced by the other services. For example, cyberspace is a complex, global, interdependent, and interconnected IT environment. Operations in and through cyberspace are dynamic and rely on a constantly evolving technological ecosystem, as well as on the interaction of diverse actors, both state and

non-state. Civilian networks and infrastructure are frequently interdependent with military networks and infrastructure. Cyberspace is also a constructed domain, requiring daily maneuvers to contest adversary campaigns.

By necessity, an effective cyber service will need to include a cadre of skilled personnel and will need to build and acquire cutting-edge capabilities that together enable agile, dynamic, adaptive, and creative operations in the cyber domain. This translates into specific organizational structures and policies around the type of personnel recruited into the Cyber Force; pathways for promotion and career advancement; standards; and approaches to training and education that enable adaptability, flexibility, and continuous learning.

The traditional military generalist will be replaced by "cyber-minded" leaders who understand the technical nuances of the domain as intimately as an infantry officer understands a rifle, a pilot understands aircraft, or a submariner understands nuclear propulsion.

The organizational climate will also need to be uniquely attentive to the intense psychological demands of the virtual battlefield and the demands of continuous operations, providing specialized medical and mental health support that acknowledges the distinct stressors of cyberspace operations. In this environment, the traditional military generalist will be replaced by "cyber-minded" leaders who understand the technical nuances of the domain as intimately as an infantry officer understands a rifle, a pilot understands aircraft, or a submariner understands nuclear propulsion.

Additionally, the culture of the new service will need to reflect an operational tempo that is dynamic and unceasing, with cyber operations taking place throughout all phases of conflict. For other low-density or high-demand military capabilities—such as special operations forces—the military employs the Joint Operations Readiness Training System, an established cycle consisting of dedicated windows for training, alert time, pre-deployment, and deployment. To date, this has not been applied to cyberspace operations, with individuals "on target" for the entirety of a typically two- to three-year assignment cycle.[29]

Finally, the Cyber Force will require the authority and resourcing to serve as the joint force's primary doctrinal authority for cyberspace operations.

Unlike the rigorous approach used by the existing services to develop, test, and refine the development of doctrine, strategy, and policy, today's military cyber ecosystem lacks any capability to perform this critical work. The absence of standardized doctrine development—of the type currently practiced at the Army's Combined Arms Command, the Naval Aviation Warfighting

Development Center, the Air Force Warfare Center, or the Marine Corps Warfighting Laboratory—ensures that cyber operators are less effective and impactful than would otherwise be possible.

The Cyber Force will be responsible for developing, refining, and institutionalizing the concepts that govern the employment of cyber capabilities across competition and conflict, judged against the following objectives:

- Broadening and aligning the Joint Warfighting Concept with cyberspace as a maneuver domain, not merely a supporting function
- Developing and iterating operational concepts for persistent engagement, autonomous cyber operations, and large-scale cyber campaigns
- Institutionalizing campaign design in cyberspace—including phases, lines of effort, and operational objectives
- Advancing concepts for human-machine teaming, including agentic and autonomous cyber capabilities
- Serving as the central body for concept validation and doctrinal updates
- Establishing a common lexicon, taxonomy, and conceptual framework for cyberspace operations, and in so doing resolving longstanding ambiguity between cyber, information, and electromagnetic activities
- Defining cyberspace as a domain in which forces maneuver, gain positional advantage, and achieve operational effects independent of other domains

If successful, Cyber Force doctrine will move beyond enablement constructs and instead articulate the following:

- Ways to gain, maintain, and leverage cyberspace superiority to achieve strategic- and theater-level military objectives
- Processes for integrating lessons learned from real-world cyber operations, intelligence insights, and industry innovation
- Trajectories for developing, deploying, and managing emerging technologies, such as AI and quantum computing, as well as their potential impact on U.S. military operations and activities
- The means to conduct complex military campaigns in cyberspace below the threshold of armed conflict
- The integration of cyber operations with activities in the other warfighting domains as a coequal form of maneuver

Training and Education

Training and education are distinct but complementary functions. The Cyber Force should approach training and education as a unified and complementary system designed to produce

personnel who are both technically proficient cyber professionals and qualified members of the joint military community. The Cyber Force should treat both training and education as ongoing necessities for its personnel and invest in consistent validation and improvement of those professional development efforts.

A service that invests only in training produces personnel who are capable until circumstances shift. A service that invests only in education produces personnel who understand the problem but cannot act on it. This integrated professional development system for all Cyber Force personnel and members of the joint force community is critical to fielding an effective force capable of meeting the cyber requirements of operational commands and adapting to the emerging challenges and opportunities of the cyber domain. The organization, management, and continuous improvement of this professional development system will best be organized under a Force Generation and Training Command.

The Cyber Force will have to conduct a comprehensive evaluation of the existing distributed training and education approaches from the services and ongoing CYBERCOM 2.0 efforts. Similar to the phased personnel realignment discussed in an earlier section, the Cyber Force should pursue a phased transition of existing training and educational resources to minimize the disruption to the current cyber mission force. The primary objective for the Cyber Force must be implementing a professional development system designed to ensure that Cyber Force personnel have the knowledge, skills, and judgement required to meet the evolving demands of the cyber domain.

CYBER FORCE TRAINING

Cyber Force training should be designed for the unique nature of the cyber domain and the workforce strategy the Cyber Force adopts. The technology, tools, and tactics of the cyber domain are constantly evolving, making training material obsolete within months. Recognizing the extreme perishability of cyber skills, the Cyber Force must implement an immersive, continuous training and currency model. The Cyber Force must deliver tailored, responsive, and graduated training to ensure that personnel and units can rapidly integrate new tools and technologies within its established operational readiness model. To mirror the workforce strategy of prioritizing quality over quantity, Cyber Force training should establish a tiered progression toward mastery for both individuals and units. The Cyber Force must establish a baseline standard for training and currency that reflects the demands of the mission rather than the average proficiency of the current cyber workforce.

The objective of Cyber Force training is to provide personnel and units with the venues and instruction that reflect the standard demanded by nation-state competition in the cyber domain. To meet this objective, Cyber Force training must be adaptable enough to keep pace with the evolution of the cyber domain and rigorous enough to prepare personnel to compete and win against nation-state adversaries.

In this model, the Cyber Force should assume the role of joint force trainer. This will require close coordination and collaboration between the educational elements of the accessions process, initial and ongoing professional education, and ongoing training development.

CYBERCOM and operational commands will continue to provide crucial feedback to guide the development and rigor of individual and collective training. Additionally, the Cyber Force will need to integrate with existing partner training and certification requirements from the operational force. To accomplish this, the Cyber Force should review the existing individual and unit training requirements for opportunities to improve. In pursuing these objectives, Cyber Force training should aspire to be the venue of choice for high-quality and operationally relevant basic, intermediate, and advanced cyber training across the DOD and within cyber organizations across the federal government, while also serving as the premier integration hub for commercial partners.

Certification and currency requirements are a critical component of both individual- and unit-level training. The existing cyber mission force relies on job qualification records for individuals and certification events for organizations. While elements of both the job qualification records and unit certification process may be directed by partner organizations—particularly around OCO—the Cyber Force should conduct a holistic evaluation of the individual and unit certification process to increase the standard and integrate with professional military education (PME) and the operational readiness cycle to remove redundancies. Where possible, the Cyber Force should seek to validate the training readiness of both individuals and units through performance-based evaluations of their respective operational demands, as opposed to solely process-oriented evaluations.

Achieving this vision will require deliberate decisions about how the Cyber Force training system is designed, resourced, and sustained. Cyber Force training should be designed to be responsive to operational demands, with explicit mechanisms for continuous feedback from operational commands. Further, the Cyber Force training model must be deeply integrated with the operational readiness model discussed elsewhere. Cyber Force training should be designed for continuous technical upskilling, potentially on the order of every 12–18 months, to ensure that personnel and units have the necessary training available while rotated off-mission in the readiness cycle. The Cyber Force should evaluate available commercial training solutions where appropriate while also retaining the capacity to develop and deliver timely and rigorous training that can address highly specialized requirements in deep technical areas.

Finally, maintaining a sufficient number of qualified cyber instructors has proved a consistent challenge across the existing cyber training and education efforts within the services. The Cyber Force should develop a competitive system that selects qualified instructors from the operational force and enables them with experience in industry, academic, and external research organizations. Selection as an instructor should be competitive and beneficial to career progression to incentivize highly experienced and qualified members of the operational force to integrate their experience into Cyber Force training. This emphasis will reflect both the scarcity of qualified instructors and the asymmetric impact a small number of exceptional instructors can have on the personnel they develop.

Together, these design principles should produce a training system that is not only rigorous and adaptive but institutionally capable of improving itself as the domain evolves. It will ensure that training remains responsive to current mission requirements and that trainees benefit from the real-world experience of their instructors.

CYBER FORCE PROFESSIONAL MILITARY EDUCATION

The Cyber Force education program should be designed to develop the foundational knowledge, judgement, and analytical skills necessary to adapt to the evolving conditions of the cyber domain. Where Cyber Force training will develop proficiency in specific tools, platforms, and mission types, Cyber Force education will develop the broader intellectual foundation that allows personnel to overcome emerging challenges and succeed in novel situations beyond what training anticipated. Regardless of how rapidly the Cyber Force training program can adapt, there will remain a need for an educational program which instills ingenuity and creativity within Cyber Force personnel. Cyber Force education should span the full arc of a career, from the educational baseline established prior to accessions into the force through ongoing PME and advanced academic programs that develop the technical and strategic depth tailored to roles across the workforce.

Cyber Force education must be deliberately multidisciplinary in its design. Success in the cyber domain draws simultaneously on technical, legal, intelligence, and strategic competencies from a range of existing academic disciplines. While the specific educational balance should be tailored to the demands of career progression, every Cyber Force member should be equipped with a broad educational foundation upon which they can specialize.

The long-term aspiration for Cyber Force education is to produce officers and warrant officers who are among the most technically sophisticated in the joint force and the most intellectually prepared to operate at the intersection of technology, law, intelligence, and national security policy.

As such, Cyber Force education should not simply accept a narrow technical curriculum. Instead, it should develop an educational approach that produces personnel who can reason across the full breadth of the domain. The long-term aspiration for Cyber Force education is to produce officers and warrant officers who are among the most technically sophisticated in the joint force and the most intellectually prepared to operate at the intersection of technology, law, intelligence, and national security policy.

Cyber Force personnel must embrace a culture of lifelong learning to succeed in the constantly evolving cyber domain. At its foundation, the Cyber Force should deliberately evaluate and shape the educational baseline of its future officers and warrant officers. The development of this educational foundation should be informed by the operational force, the Cyber Force training program, external commissioning sources, and partners in academia. The Cyber Force could

join—or even assume a lead role in—the existing National Centers of Academic Excellence in Cybersecurity program run by the NSA's National Cryptologic School. Whether through the existing program or other means, the Cyber Force should seek to ensure that the curriculum at venues such as ROTC programs, Officer Candidate School, and existing service academies reflects the technical and analytical preparation the cyber mission force requires.

Education is a critical component of cyber readiness. In Section 1506 of the FY 2022 NDAA, Congress directed a report on overall workforce and education requirements for cyberspace and information warfare, including the necessity for a dedicated National Cyber Academy.

The creation of the Cyber Force introduces an opportunity to consider alternative models for both undergraduate accessions and advanced cyber education, including the creation of a dedicated service academy. This review should consider a wide variety of existing and novel domestic and international approaches to meet the educational and accessions demands of the Cyber Force. This will naturally include the extension of the four-year service academy, ROTC, and scholarship program models in use across the DOD. The Cyber Force should also consider novel educational models informed by the United Kingdom's Royal Military Academy Sandhurst or the Naval Postgraduate School. For example, the Cyber Force could create an academy that offers a one-year undergraduate program on the model of Sandhurst, alongside two-year advanced degree programs similar to the Naval Postgraduate School.

Regardless of the outcome of any decision, the subject of cyber education following the creation of the Cyber Force warrants deliberate consideration. The Cyber Force will be uniquely positioned to set the standard for cyber education. Like the existing service academies, the Cyber Force should leverage its concentration of experienced cyber personnel to connect concepts in the classroom to the operational reality of the cyber domain. Whether as an academy or a PME institution, the Cyber Force should seek to create an institution that shapes the professional identity of the Cyber Force and elevates the standard for cyber education across the joint force and the federal government.

Beyond initial accession requirements, the Cyber Force should establish a tailored PME program that reflects the professional culture of the service. This program will both respond to the baseline requirements of the joint force and prepare Cyber Force personnel for the unique demands of their operational environment. Cyber Force leaders will face challenges that are not purely technical, but involve the complex interplay of law, economics, cognitive effects, governance, and military operations.

Additionally, personnel in the existing cyber mission force often operate at echelons of command that are not reflected in the typical joint PME curriculum. The goal of the Cyber Force PME program must be to develop personnel over their careers who can contribute meaningfully to

operational, institutional, and policy decisions at successively higher levels of responsibility. As officers and warrant officers progress through their careers, for instance, PME should deepen in both technical rigor and strategic breadth. This could include the development of highly selective advanced schools equivalent to the Army's School of Advanced Military Studies or the Air Force's Weapons School.

A key element to the success of Cyber Force education should be programs for advanced academic education, including graduate programs, fellowships, and joint research opportunities. These programs should be managed throughout the duration of a Cyber Force career as both a deliberate force development investment and an opportunity to integrate emerging concepts from the academic community of interest. Cyber Force education programs should therefore maintain structured contact between operational units and academic institutions.

To facilitate this connection, the Cyber Force should also evaluate the utility of a core research institution with both dedicated and rotational personnel from the operational force that can facilitate collaboration between the force, academia, and existing federally funded research and development centers. Such an institution could serve to bridge the gap between operations, educational programs, doctrine and strategy development, and capability development efforts with external partners in industry and academia.

Finally, the Cyber Force should offer educational opportunities for leaders from across the joint and partner community. These Cyber Force–run courses will improve joint leaders' understanding of the cyber domain, as cyberspace is a critical enabler across the range of joint functions in addition to being an independent domain of operations. Senior leaders from across the joint force no longer have the luxury to outsource cyber expertise. They must understand how cyber acts as a structural modifier of every instrument of national power, not just in military operations.

The Cyber Force should thus develop and inform PME curricula at traditional staff and war colleges to prepare joint leaders' understanding of the role of cyberspace in competition, crisis, and conflict. Similarly, Cyber Force leaders require the same core education and attributes expected of any staff and war college graduate. The DOD must have leaders across the joint force that can translate cyber capabilities into strategic advantage, integrate cyber operations with joint and coalition campaigns, and manage escalation and stability in a persistent competition environment.

ADVANCEMENT AND PROMOTION

Advancement and promotion in the Cyber Force should preserve multiple equally valued models of senior service. The service should reject the assumption that there is only one valid pattern for senior advancement or that all high-performing personnel must converge toward the same type of senior leader. At a minimum, the Cyber Force should preserve a leadership-centered path focused on mission command, organizational leadership, and force integration that is grounded in technical competence; a technical-centered path focused on operations, capabilities, and mission engineering; and blended, flexible paths that combine operational breadth with sustained technical depth. Officers should be able to rise through any of these paths to the highest commissioned

grades. Warrant officers should have a respected and competitive advancement structure that preserves deep expertise, long-term mission continuity, and senior technical authority.

Within the applicable promotion framework, centralized boards should serve as the final confirming mechanism rather than the primary source of professional judgment. The principal basis for advancement should come from sustained observation by peers, mission leaders, technical supervisors, qualification authorities, and specialty development processes that can assess real performance over time. Promotion decisions should therefore rest on a richer record of demonstrated contribution than generic administrative performance alone, and that record should be broad enough to recognize different forms of excellence rather than forcing all personnel into one model of competitiveness.

The attributes prioritized for advancement should be sustained mission impact, technical credibility, sound judgment, adaptability, and the ability to lead and develop high-performing teams. The service should value officers and warrant officers who can solve difficult operational problems, contribute meaningfully to mission readiness, and maintain credibility in their specialties as the character of the mission evolves. It should be clear that remaining technical, even in a highly specialized area, is fully compatible with promotion. Deep specialization should not be treated as evidence of narrowness or lack of potential. At the same time, broader operational experience, cross-functional service, and increased organizational responsibility should also be recognized as valuable where they strengthen mission leadership and force integration. The objective is not to prefer specialists over broad operators, or broad operators over specialists, but to promote both according to standards appropriate to their form of contribution to the force.

Milestones should therefore be understood as belonging to multiple valid advancement patterns rather than a single universal ladder. Foundational and advanced qualification, recurring requalification, repeated successful operational or capability-development tours, validated leadership in missions or technical programs, instructor or evaluator duty, selected advanced education, and command experience may all be important milestones, but not every milestone should be required for every path. A technical-centered career may place greater weight on repeated high-end mission performance, capability contribution, instructor or evaluator service, advanced qualification, and long-term technical credibility. A leadership-centered career may place greater weight on increasingly complex operational integration, team and organizational leadership, command, and broader force responsibilities. Other careers may combine elements of both. Moving across specialties, serving in broader roles, and building wider institutional perspective should remain a valid path to promotion, but it should not be treated as a universal prerequisite for senior advancement. Likewise, remaining close to specialized mission work should remain fully promotable when that service continues to produce high-value contributions.

The Cyber Force should promote both operational leaders and technical specialists, and it should do so explicitly rather than rhetorically.

In short, promotion systems should compare members against standards appropriate to their competitive category, qualifications, and demonstrated service to mission readiness rather than force all talent into a single mold. The Cyber Force should promote both operational leaders and technical specialists, and it should do so explicitly rather than rhetorically. A force that allows only one pattern of advancement will gradually produce only one type of senior officer and one definition of merit. In a cyber service, this will in practice narrow judgment, weaken innovation, and erode the very expertise the force is meant to preserve.

3

Organizational Alignment within the Department of Defense

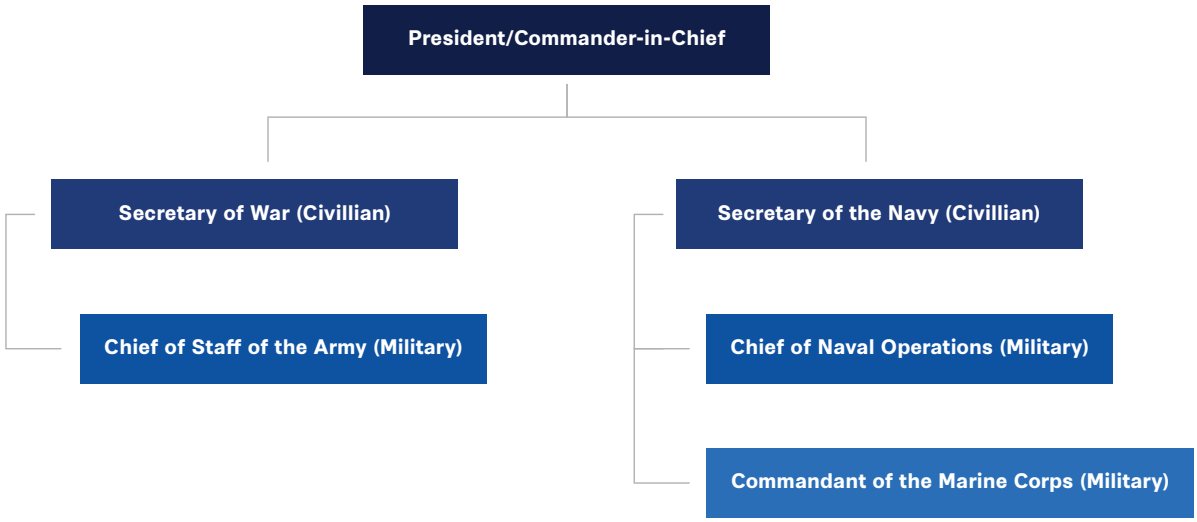
Placement of the Cyber Force within a Military Department

The institutional alignment of the Cyber Force—where to house a United States Cyber Force within the Department of Defense—was a matter of recurring debate. Commissioners held strong views in favor of two distinct options: aligning the new service under the Department of the Army or establishing a wholly new military department, a Department of the Cyber Force.[30]

Until the mid-twentieth century, the uniformed military services of the era (the Army, Navy, and Marine Corps) were managed and overseen by cabinet-level departments with a secretary of war responsible for the Army, while (since 1798) the secretary of the Navy held responsibility for the Navy and the Marine Corps.

Following the National Security Act of 1947, the Departments of War and the Navy were subsumed under the newly established Department of Defense, along with the new Department of the Air Force. Under the reformed structure, the secretary of defense was charged with coordination among the military departments and services and served as the single civilian officer representing the military within the president's cabinet.

Figure 4: U.S. Military Organization, Pre-1949



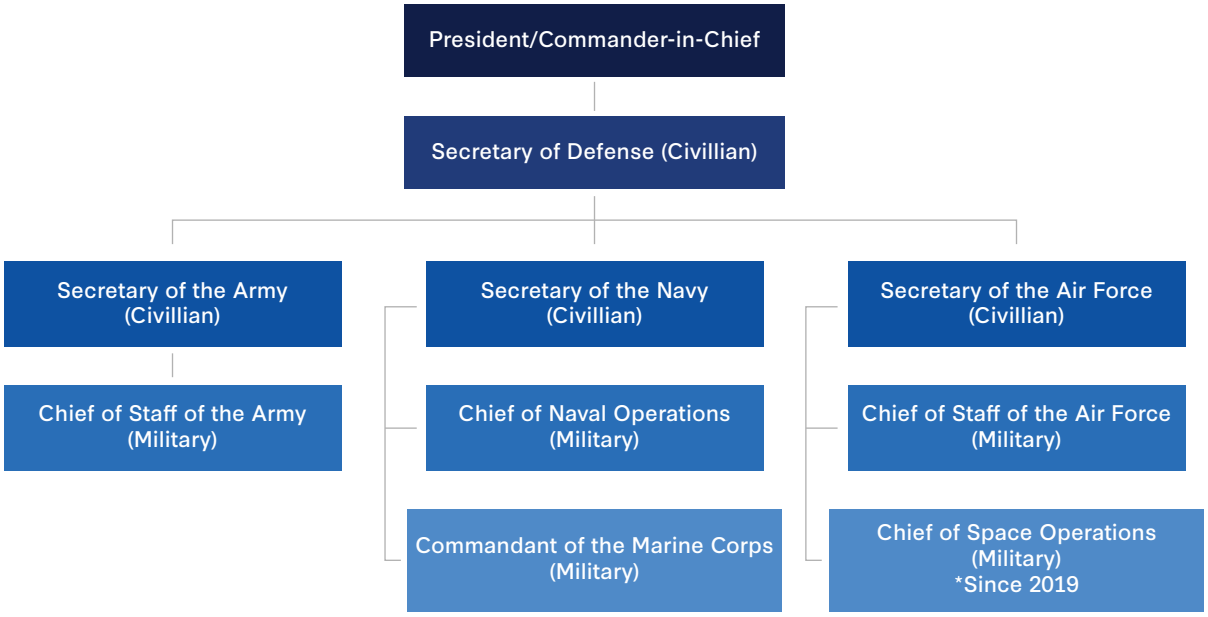
Source: CSIS Commission on U.S. Cyber Force Generation.

Currently, the term "military departments" refers specifically to the three executive departments within the DOD: the Department of the Army, the Department of the Navy, and the Department of the Air Force. These are administrative organizations led by civilian service secretaries who are appointed by the president and confirmed by the Senate. The military departments are not combatant units. Rather, they are the bureaucratic and institutional shells headquartered at the Pentagon that recruit, fund, train, and equip the military services. Under the post-1947 reorganization, the secretaries of the military departments were charged with the following for their respective services: recruiting; organizing; supplying; equipping (including research and development); training; servicing; mobilizing; demobilizing; administering (including the morale and welfare of personnel); maintaining; constructing, outfitting, and repairing military equipment; and, finally, constructing, maintaining, and repairing buildings, structures, and utilities and acquiring real property and interests in real property necessary to carry out the responsibilities specified in this section.[31]

The military departments conduct institutional missions, which include the long-term development of the force. The military departments are best viewed as the combined effort of both the civilian secretariat and the uniformed services, with the uniformed services representing actual combat capability and the secretariat performing administrative and oversight functions. Civilian-led secretariats oversee and manage the activities of the subordinated military services, as well as the services themselves. With a civilian statutorily in charge, the arrangement between the secretary, the secretariat, and the uniformed services reflects and enshrines civilian control over the military.

Since the Goldwater-Nichols Act of 1986, the uniformed services in their institutional capacities do not employ their own forces. Instead, that responsibility rests with the unified combatant commands, such as Central Command (CENTCOM) or Indo-Pacific Command (INDOPACOM), which then employ those forces for operational missions.

Figure 5: Department of Defense Organizational Design, Post-1949



Source: CSIS Commission on U.S. Cyber Force Generation.

Until the Space Force was established in December 2019, only the secretary of the Navy had responsibility for more than one uniformed service. Despite some early notions that the Space Force will eventually transition from the Department of the Air Force to a future "Department of the Space Force," there is no momentum or evidence of this occurring.[32] While larger than either the Departments of the Navy or Air Force, the Department of the Army is today the only military department responsible for only one uniformed military service.

Option 1: Alignment of the Cyber Force to an Existing Military Department

This model aligns the Cyber Force under the Department of the Army. The relationship between the Cyber Force and the secretary of the Army will be no different from the relationship between the Marine Corps and the secretary of the Navy or the Space Force and the secretary of the Air Force. The Department of the Army will be brought in line with its Navy and Air Force counterparts, henceforth responsible for the management of two dedicated branches of the armed forces.

ADVANTAGES

Proponents of aligning the Cyber Force under the Department of the Army generally considered this approach most expedient and efficient through administrative, economic, and political lenses. Under the existing model, each of the military departments, with the exception of the Department of the Army, oversees two services. By building under the Department of the Army, the Cyber Force can leverage an existing and mature civilian secretariat with developed processes and established facilities. In this way, a Cyber Force could stay focused on core warfighting responsibilities rather than developing an entirely new administrative structure.

Beyond expediency, the Army and Cyber Force are similarly focused on the individual as the central element in operational planning, particularly when compared to the platform-centric view of the Navy or Air Force, where combat capability is considered in terms of the numbers of capital ships or aircraft. For Army leaders, operational outcomes are tied to the number of soldiers that can be put on target, whereas counterparts in the Navy and Air Force consider the number and types of platforms necessary to hold an objective at risk. Given the lack of dependency on hardware, military operations in cyberspace share more in common with the Army perspective. This mindset of "people before platforms" affects innumerable aspects of military operations, including operational planning, training, budgetary forecasting, and intelligence support.

Proponents of organizing the Cyber Force under the Department of the Army see a scenario whereby the already sizable challenges of creating a new military service are partially offset by leveraging the Department of the Army's existing infrastructure for legal, financial, and logistical support. This arrangement will be significantly more cost-effective than standing up a dedicated military department solely to oversee the Cyber Force, which will require the creation of hundreds and potentially thousands more civilian and administrative billets than those required within the Department of the Army. A decision to establish the Cyber Force within the Department of the Army preserves the core objective of an independent uniformed service for the cyber domain while mitigating the risk of bureaucratic redundancy and bloat.

As just one example, under the leadership of the secretary of the Army, the United States Military Academy at West Point could serve as the entryway for future officers of the Army or the Cyber Force. This will mirror the United States Naval Academy, which trains future officers for the Navy and the Marine Corps, as well the United States Air Force Academy, which trains cadets for careers in the Air Force and Space Force. By institutionalizing the Cyber Force as a core component of the Department of the Army, future Cyber Force leaders could capitalize on common resources that are not specific to the Cyber Force, such as medical personnel and facilities. This is even more critical when considering the disproportionate investments by the Army over the last decade compared to the other services, to include a wholly new cyber-centric campus at Fort Gordon in Georgia. Moreover, when evaluating the real estate requirements for the new service, the Cyber Force could leverage unused and underutilized Army facilities and holdings, without having to negotiate either new land purchases or building construction.

Finally, advocates argue that authority over the Cyber Force empowers a secretary of the Army, granting them responsibility over warfare across two domains. Given the primacy of the sea in the physical realities of the Indo-Pacific AOR and the emphasis on that AOR for the past few years, the Army's share of the DOD's budget has slid significantly, representing only 17 percent of the proposed FY 2027 budget—down from 26 percent in FY 2020.[33] Stewardship over a new service that can reach across continents and create strategic-level effects without requiring capital-intensive weapons systems institutionally strengthens the Army secretary in bureaucratic and budgetary battles within the Pentagon.

DISADVANTAGES

Given the relative sizes of Army versus a future Cyber Force, some critics have highlighted the potential risk that any Army secretary will struggle to balance time, attention, and priorities between the two forces. Opponents have also alleged that a new Cyber Force will struggle for institutional prioritization compared to the Army as a service in larger, intradepartmental debates. The risk is that the Cyber Force, while an independent service, may struggle to achieve all of the aspirations of its creators because the civilian secretariat cannot adapt to meet the needs of both the Army and the Cyber Force.

Additionally, opponents note that the Department of the Army's civilian bureaucracy is presently comprised of a significant number of former Army service uniformed and civilian employees who may be too wedded to an institutional culture of exclusively servicing one branch of the armed forces.

Finally, when looking across the total force of active-duty, Army Reserve, and National Guard personnel, the combined strength of the Department of the Army dwarfs the other services, diminishing prospects that the civilian secretariat can change in a meaningful way to balance the demands of the Army and a Cyber Force.

Option 2: Alignment of the Cyber Force to a Newly Created Military Department

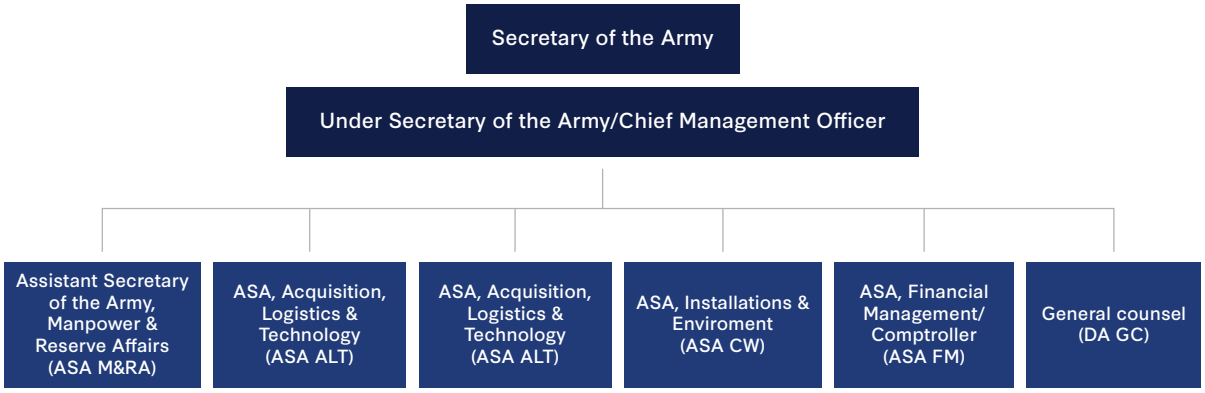
The commission also considered building out a newly established Department of the Cyber Force as the fourth military department within the Department of Defense. Proponents of this option note that operations in cyberspace are sufficiently unique from land operations to warrant placing them under a single civilian leader. In addition, they consider the size of the Army and its potential to overshadow a nascent service envisioned at 20,000 active-duty uniformed billets. Through this lens, the cultures of the Army and the Cyber Force are fundamentally dissonant, resulting in potential bureaucratic friction that could undermine the purpose of a dedicated service for the cyber domain.

Some commissioners pointed to the experience of the Army's cyber branch since its establishment in 2014, noting that despite some tangible advancements, the net result has been a "cyber culture poorly integrated within the Army's dominant culture."[34] Cyber operators are often pressured to "speak infantry" to justify their existence to maneuver commanders, a process that can lead to the "semantic rebranding" of cyber roles to fit traditional Army paradigms.[35] Even Army Cyber Command, created specifically to emphasize the importance of cyber operations over traditional signal, information operations, and intelligence roles in the Army, is now led by a respected three-star general officer who has important experience in the Army's signal corps but who never previously held a cyber-specific position. Proponents of a new military department argue that placing the Cyber Force under the Department of the Army could exacerbate these tensions, forcing digital warriors to conform to standards—such as physical fitness, grooming, and traditional PME—that are not tied to cyber-specific readiness and technical discipline standards.

ADVANTAGES

Proponents of this option assert that the Cyber Force will be far better positioned to achieve its designed purpose as a new, standalone military department. From this lens, the current challenges plaguing cyber force generation are too complex for a new Cyber Force to depend on the Army Secretariat to address, when that organization is "purpose-built" today to support force generation for land warfare.

Figure 6: Current Organization of the Department of the Army Secretariat



Source: CSIS Commission on U.S. Cyber Force Generation.

The Departments of the Navy and Air Force provide illustrative examples. Whereas the Department of the Navy has evolved over its history to balance its support of both the Navy and the Marine Corps, some perceive the Department of the Air Force as struggling to adjust to managing both the Air Force and Space Force since 2019. This is particularly noteworthy when considering that the total size of the Army (active duty, reserve, and National Guard) is nearly twice that of the Air Force and Space Force combined. Given the proposed size of the Cyber Force, at 20,000 personnel, some commissioners expressed a deep concern that, no matter its importance, the Army Secretariat would be incapable of balancing the needs of a new force with those of the nearly 1 million Army personnel. Alternatively, a Department of the Cyber Force, with its own secretary and civilian secretariat, will ensure that the uniformed component has the support and oversight it needs to perform at its full potential.

Proponents believe that only a dedicated military department can enable the Cyber Force to enact meaningful change that addresses existing challenges. To successfully compete in the Defense Department's byzantine but critical annual resource allocation process, it will be necessary to convince the DOD's non-cyber-focused leadership that cyber forces are worth resourcing. A small but dedicated team of civilian officials in a cyber military department could be more effective at that task than an Army Secretariat balancing requirements across two distinct domains of warfare.

DISADVANTAGES

While most commissioners agreed that establishing a dedicated military department for cyberspace could enable a level of institutional focus not possible with a Cyber Force housed under the Department of the Army, some argued that building both a uniformed service and a civilian-led

military department will be too laborious and too costly to implement in a reasonable timeframe. Moreover, critics asserted that there is not commensurate political appetite for this option at present, particularly while the DOD works to implement the CYBERCOM 2.0 reforms announced in late 2025. Practically, there are significant doubts about the scale of the challenges faced in building a new Cyber Force without leveraging a functional and mature parent organization to support the budgetary, real property, and administrative requirements of the new service.

Table 5: FY 2026 Budget Request by Military Department

Dept. of the Army	Dept. of the Navy	Dept. of the Air Force	Defense-Wide
$197.4 Billion	$292.2 Billion	$301.1 Billion	$170.9 Billion

Source: Department of War, *FY2026 Budget Request Overview Book* (Washington, DC: DOW, July 2025), https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/FY2026_Budget_Request_Overview_Book.pdf.

At even $20 billion, the Department of the Cyber Force will be structurally disadvantaged relative to the annual budget battles that occur across the military departments and services. Opponents of the dedicated military department have noted how this structural mismatch could persistently handicap a new Cyber Force.

4

Modern Capability Development

Operational Requirements for Capability Velocity

Modern capability development in the cyber domain is no longer defined by linear procurement cycles but by architectural and operational velocity. The primary outcome required of a Cyber Force by the joint force is the immediate availability of mission-relevant capabilities, especially the ability to conduct vulnerability research, develop exploits and persistent access tools, and provision infrastructure at a tempo that matches or exceeds that of the adversary.

Advances in technologies, especially advanced AI tools, have improved the speed of capability delivery. However, there are enduring institutional and structural hurdles. To achieve the required speed, the Cyber Force should explore both technical and non-technical solutions, such as a dynamic, pooled developer unit for talent allocation; the institutionalization of fused squadrons; the adoption of flexible software-centric appropriations; and integration with Cyber Force training and doctrinal efforts.

Organizational Design and Talent Allocation

To deliver these outcomes, the Cyber Force should organize its "man, train, and equip" functions to eliminate the bureaucratic silos between developers and operators.

THE POOLED DEVELOPER UNIT

One potential approach is for the Cyber Force to establish a centralized, pooled developer unit, commanded by a colonel (O-6). This unit will serve as the single administrative control (ADCON)

element and institutional home for all capability development work roles. Unlike legacy service models that assign technical personnel to specific operational units through rigid permanent change-of-station cycles, the Cyber Force will manage its developer talent as a dynamic pool of ready capability.

In this model, the force employer (e.g., CYBERCOM) will be responsible for identifying steady-state target prevalence and skill requirements—analogous to a geographic commander identifying the required ratio of maritime versus land-based assets for a specific theater. For example, if a campaign requires an increased density of mobile-platform specialists for a specific mission set, the Cyber Force ADCON Developer Unit will prioritize and allocate personnel from its ready pool to the operational task forces. This will allow the joint force to force-organize around specific outcomes, ensuring that task forces receive a tailored package of developers and agreements officers without the friction of multiyear personnel cycles. The service's role is to ensure personnel are manned, technically certified, and maintained at the peak of technical proficiency for deployment into combined operational teams.

CONTINUOUS TECHNICAL IMMERSION

The cornerstone of workforce development for this talent pool should be continued growth through immersion rather than rote schoolhouse pipelines. Stale skills are an operational liability. Therefore, the Cyber Force should explore options to institutionalize the following:

- **Assessment:** Before the Cyber Force can instill the skills necessary to operate effectively, it must determine what skills are needed—including by taking the best emergent skills in the private sector. Thus, the Cyber Force should undertake a systematic evaluation of such emergency skills in the private sector and determine which of those skills are applicable in the context of the Cyber Force.
- **Rotational Industry Exchange:** The Cyber Force can create opportunities for personnel to undertake rotational tours at leading global technology firms to stay current with state-of-the-art software engineering and AI. These tours will need to be governed by specific legal safe harbors for intellectual property and conflict of interest to encourage deep technical integration.
- **Technical Conference Engagement:** Another opportunity is for personnel to be encouraged to regularly attend and actively participate in the global security research community (e.g., DEF CON, Black Hat, and Usenix). This will allow service members to be integrated into the "white hat" community where new vulnerabilities are discovered daily.
- **Permeable Career Pathways:** Mirroring industry models, the Cyber Force should evaluate career pathways for upward mobility for individual contributors that do not mandate a transition into managerial or command roles, ensuring that its best technologists stay behind the keyboard as senior technical authorities.

FUSED UNITS OF ACTION: THE CYBER COMBINED ARMS SQUADRON

A related issue is collapsing the distance between those who build technology and those who employ it. One approach to do so is to establish a Cyber Combined Arms Squadron as a cross-discipline unit of action.

These squadrons could be fused warfighting formations consisting of operators, analysts, developers, agreements officers, legal advisers, and other mission-relevant support personnel all integrated into a single command structure. While the Cyber Force pooled developer unit will provide the specialized "man, train, and equip" squadrons, other cyber force generators will provide further key work roles, such as operators.

This model draws from three precedents in the acquisition and capability development realm:

- **Navy Cyber Warfare Development Group (NCWDG):** Originally established as "Station Oscar," NCWDG is the Navy's premier entity for the research, development, and delivery of tailored cyber capabilities. Its success is rooted in the fusion of special technical operations planners with engineering teams. The Cyber Force could explore how to scale this "fused cell" concept, ensuring that developers are not merely fulfilling requirements but are embedded in the mission-planning process to understand the physical and logical constraints of the target environment.
- **Space Force Integrated Mission Deltas (IMD):** The Space Force IMD construct merges operations and sustainment under a single mission commander. Historically, the personnel who operated a system and those who maintained or updated it reported to different chains of command (operations versus acquisition and sustainment). The IMD model places both under one leader to ensure that the officer responsible for a mission effect also holds authority over the software assets required for that mission. The Cyber Force could examine options to adopt this "mission-owner" model to prevent software readiness from being treated as a separate administrative function, acknowledging instead that it is a constant, rather than a cyclical, requirement. In Cyber Force implementation, the developer who builds a capability will be administratively and operationally aligned with the mission owner who employs it, creating a unified "cradle-to-grave" accountability loop that mirrors modern DevOps practices in the industry.
- **Rapid Capabilities Offices (RCO):** RCOs—successfully utilized by the Air Force, Army, and special operations forces—are designed to bypass the traditional, multilayered Joint Capabilities Integration and Development System to field urgent capabilities. This includes the use of delegated 10 USC 4021/4022 Other Transaction Authority to execute contracts at the speed of the operational requirement. Crucially, this model requires the assignment and delegation of agreement officer authority down to the field and company grades. The Cyber Force could operate as an RCO at scale. By similarly placing the authority to obligate funds and execute non-traditional contracts directly within the operational task forces, the Cyber Force will remove the administrative distance between identifying a mission gap and procuring the technical solution.

Resource and Policy Reform: Software Appropriation Models

Agility is impossible without flexible resourcing. The Cyber Force should request a unified software appropriation, in the spirit of, and similar to, the Budget Activity 08 (BA-08) model. This eliminates the false dichotomy between RDT&E and O&M.

In a domain where software is in a state of continuous iteration, a "unified color of money" approach enables better portfolio management. This allows task force commanders to shift resources dynamically between procuring commercial research from the defense industrial base and building internal capabilities based on the tactical prevalence identified by the force employer. It also provides the necessary funding for operational IT (e.g., range infrastructure and inference compute) distinct from the enterprise IT maintained by the legacy services.

Continuous Institutional Feedback

The dynamic nature of the cyber domain requires that the Cyber Force develop institutional feedback mechanisms that are inherently self-correcting. It is important to acknowledge that because the cyber domain is in a state of constant flux, the recommendations provided are not fixed. Cyber Force leaders should expect these organizational designs and authorities to require adjustment as the threat landscape evolves.

The objective is to provide a blueprint for a service where iteration and improvement are not byproducts of the system, but the primary weapon system itself.

This iterative process of feedback and improvement for Cyber Force capability development is achieved through integration with both the operational commands and Cyber Force training organizations. The Cyber Force should continuously evaluate and refine the presentation and integration of capability developers through experimentation in both training and operational environments. As new processes and development approaches are validated in training and operational environments, these lessons are integrated into doctrine and training requirements. This process of institutional feedback will help improve Cyber Force doctrine and ensure that capability development is directly improving operational outcomes.

By pooling technical talent at the ADCON level and deploying it through fused units of action guided by a self-correcting doctrinal loop, the Cyber Force will provide a ready force. The objective is to provide a blueprint for a service where iteration and improvement are not byproducts of the system, but the primary weapon system itself.

5

Enabling Pillars for Success

Foundational, Scientific, and Technical Intelligence Centers for Cyberspace

Each of the existing armed forces has validated the need for—and long sustained their own tailored intelligence organizations around—general military intelligence (GMI), also known as foundational intelligence, and scientific and technical intelligence (S&TI). From as early as 1882 with the Office of Naval Intelligence, the military services have prized and consistently invested in their own intelligence collection and analytic production capabilities.[36] While each of the service intelligence centers has broad responsibilities, they fulfill two primary roles: (1) direct intelligence support to their service and (2) the production of foundational intelligence through all-source analysis on foreign military service capabilities and operational art.[37]

For years, leaders at CYBERCOM have highlighted significant gaps and a basic lack of foundational intelligence for the cyber domain. In public remarks in 2022, Brig. Gen. Matteo Martemucci, then director of intelligence at CYBERCOM, noted that:

> None of [the Service Intelligence Centers] that I've mentioned are producing the sort of foundational adversary cyber order of battle [necessary]. . . . A large and capable cyber force—like China or Russia or the forces of violent extremist organizations—need to be assessed and catalogued and tracked in the way we assess, catalog, track and measure adversary armies, navies and air forces.[38]

Brig. Gen. Martemucci went on to detail the scope of the deficiency, commenting that of the more than 600 requirements added to the U.S. Intelligence Community's database, only approximately 270 had been validated by the interagency.

The following year, Col. Candice Frost, then commander at CYBERCOM's Joint Intelligence Operations Center, offered a similar perspective, underscoring the need for "a center that is focused on all-source intelligence to support Cyber Command in the cyber domain."[39] In response, Congress mandated the establishment of a "cyber intelligence capability" in 2024. However, this was generally limited, with no funding from the National Intelligence Program permitted for the effort.[40]

To be successful, the Cyber Force will require a dedicated intelligence center for both GMI and S&TI. A "Cyber Force Intelligence Center" will serve as the focal point for all-source intelligence analysis concerning cyberspace. This organization will be expected to analyze intelligence across signals intelligence (SIGINT), as well as open-source intelligence (OSINT), human intelligence (HUMINT), measures and signatures intelligence (MASINT), and imagery intelligence (IMINT)—among others—to report on adversary cyber forces' orders of battle, tactics, geographic disposition, technological development, and technical infrastructure. The center will likely require the development of a wholly new cadre of intelligence professionals with backgrounds in engineering, computer science, target development, critical languages, and foreign military organizations. This new center will pursue the following types of activities, among others:

- Tracking changes to adversaries' physical and network layers employed in cyberspace operations
- Developing target profiles for individuals associated with adversaries' cyber operations and threat actors
- Building and refining collection requirements for intelligence collection operations through HUMINT, IMINT, measures and signatures intelligence, OSINT, and SIGINT
- Establishing counterintelligence strategies to support cyberspace operations
- Centralizing the DOD's cybersecurity support to the defense industrial base
- Engaging with foreign allies and partners in the development of releasable intelligence products in support of combined cyberspace operations
- Supporting foreign materiel exploitation with technical expertise in network and data link layer analysis

Unique Counterintelligence and Military Investigative Requirements for Cyberspace

U.S. adversaries have demonstrated the use of cyberspace for intelligence activities like espionage, counterespionage, and sabotage operations in targeting both military and industrial targets. To adequately address these challenges, the commission considered how a Cyber Force could build the requisite investigative and counterintelligence capabilities to defeat current and future adversaries in cyberspace.

Within each military department, the authority to conduct counterintelligence activities resides within a Military Department Counterintelligence Organization (MDCO). Among the military departments, there are significant differences in how each organizes their MDCO as well as their Military Criminal Investigations Organization (MCIO).

DEPARTMENT OF THE ARMY

The Department of the Army is the only military department that assigns the MDCO and MCIO responsibilities to separate organizations, having designated the Army Criminal Investigation Division (CID) as the MCIO and Army Counterintelligence Command (ACIC) as the MDCO. While the CID director, a civilian, reports to the undersecretary of the Army, the ACIC commanding general reports to the commanding general of Army Intelligence and Security Command.

DEPARTMENT OF THE NAVY

The Department of the Navy relies on the Naval Criminal Investigative Service (NCIS), a civilian-led agency, to serve as both MDCO and MCIO for the department, the Navy, and the Marine Corps. The NCIS director reports to the secretary of the Navy. Uniquely, the Marine Corps also has its own dedicated CID with credentialed special agents and criminal investigators; however, CID typically investigates misdemeanor-level offenses and military-specific misconduct, operating in close coordination with NCIS. Unlike NCIS, CID is a component which falls under the U.S. Marine Corps Provost Marshal's Office.

DEPARTMENT OF THE AIR FORCE

On behalf of the Department of the Air Force, the Air Force Office of Special Investigations (AFOSI) is both a MDCO and MCIO, serving the department, the Air Force, and the Space Force. AFOSI is led by a one-star Air Force general officer and is overseen by the inspector general of the department. On behalf of the DOD, the Department of Air Force also serves as the executive agent for the DOD Cyber Crime Center (DC3), a federal center providing cyber capabilities to enable and inform law enforcement with specialized training, forensics, and support for the defense industrial base. Originally a component under AFOSI, DC3 was elevated to report directly to the inspector general of the Department of the Air Force in 2021.

COMMISSION PERSPECTIVE

Statutorily, the legal authority to perform both counterintelligence and criminal investigative activities are assigned to the secretary of defense and the secretaries of the military departments. By extension, the commission recognizes that a potential recommendation for a MDCO and MCIO is contingent on whether Cyber Force is organized within the Department of the Army or a new Department of the Cyber Force. Regardless of the question of military departments, the commission recommends organizationally transferring DC3 to fall under the Cyber Force rather than the Department of the Air Force.

Table 6: Military Department Counterintelligence and Criminal Investigations Organizations

Armed Forces	Military Department Counterintelligence Organization (MDCO)	Military Criminal Investigations Organization (MCIO)
Army	Army Counterintelligence Command	Army Criminal Investigation Division
Marine Corps	Naval Criminal Investigative Service	Naval Criminal Investigative Service *(*for major felonies*)*
		USMC Criminal Investigation Division (*for lesser felonies and misdemeanors*)
Navy	Naval Criminal Investigative Service	
Air Force	Air Force Office of Special Investigations	
Coast Guard	Coast Guard Counterintelligence Service	Coast Guard Investigative Service
Space Force	Air Force Office of Special Investigations	

Source: CSIS Commission on U.S. Cyber Force Generation.

WITHIN THE DEPARTMENT OF THE ARMY

As part of the Department of the Army, the Cyber Force will be positioned to leverage existing institutional structures. While the Army has CID and ACIC today, there were varying opinions among the commissioners on whether these organizations could evolve and provide commensurate focus on the cyber domain. The conclusion was an approach in which CID continues to serve as MCIO for the department (to include the Cyber Force), but where a dedicated counterintelligence organization is built within the Cyber Force. While the commission finds that the DOD writ large will benefit from an organization that is both technically competent and proficient in counterintelligence operations in cyberspace, the commission was less clear that Cyber Force and the needs of the domain necessitated a new criminal investigative organization for cyber operations, particularly when Army CID could provide that function.

An MDCO under the Cyber Force will have the authority to conduct operations and investigations in and through the cyber domain to identify, exploit, and neutralize threats. It will also provide a cadre of technically competent agents to serve in joint-qualified assignments at the Joint Staff and combatant commands to better advise senior leaders on multidomain threats. Cyber Force personnel trained and certified in counterintelligence will also fill critical roles within the interagency as domain experts to coordinate national efforts to defeat foreign nations' intelligence collection activities.

WITHIN THE DEPARTMENT OF THE CYBER FORCE

Housed under a new Department of the Cyber Force, the new service will be unable to leverage existing organizations such as CID. This will necessitate that, in addition to establishing a uniformed service, a secretary of the Cyber Force will also have to build both an MDCO and an MCIO. Under this scenario, the commission recommends that the secretary build the requisite functions for criminal investigations and counterintelligence within one organization, mirroring NCIS and AFOSI.

With combined authorities for both criminal investigative and counterintelligence authorities, the new Cyber Force MCIO/MDCO will employ fully credentialed federal agents trained to operate at the intersection of cyber operations, law enforcement, and criminal investigation. These agents will possess authorities and technical expertise similar to the hybrid investigative roles currently employed across a number of DOD components today, such as ACIC, AFOSI, NCIS, and DC3.

Cyber Force JAG Corps

Judge advocate generals (JAGs) serve as officers and attorneys within the military, providing legal advice to commanders and staff. Their support ensures that operations are conducted lawfully, aligned with the mission and the authorities granted by the president, federal law, a commander's rules of engagement, and the chain of command. Traditional legal structures designed for conventional warfare and intelligence are ill-suited to address the unique challenges posed by digital conflicts. Cyberspace demands specialized legal expertise. Establishing embedded legal professionals within the Cyber Force will better position the United States to meet these emerging challenges.

The Cyber Force should move quickly to develop a career field for legal professionals, which will promote improved transparency, consistency, and responsible conduct. A JAG Corps will also ensure that operational commanders are properly equipped with the requisite legal counsel to guarantee that activities are legal and defensible, including when conducted covertly. It will further enable expertise that keeps pace with frequent advances and emerging threats. Lawyers will support the development of policies and standards that balance operational secrecy with accountability, establishing norms aligned with U.S. interests and values.

Current legal career models across the military services do not support the long-term focused expertise that cyber operations demand. Few service members are permitted to dedicate their careers exclusively to this discipline. The services prioritize well-rounded attorneys for promotion boards. Judge advocates frequently transition between roles, such as military justice, operations, and individual legal support, without allowing for sustained specialization.

This lack of continuity interrupts the development of the deep expertise cyber operations law demands. A judge advocate who moves from military justice to cyber operations and then to leadership roles will rarely accumulate the consistent, in-depth experience necessary to master this rapidly evolving domain. Major incidents like the Sony and OPM breaches, changes in presidential administrations, and global conflicts inevitably lead to significant readjustments of the cyber landscape. A judge advocate leaving CYBERCOM for three years, for example, effectively starts

over when they return. Given the competitive nature of promotion and career advancement, many talented attorneys are disinclined to serve at the same command or in the same general field twice, limiting the cultivation of outstanding cyber operations attorneys.

Establishing a dedicated cyber force with structured career paths will enable attorneys to build expertise, maintain continuity, and adapt to the rapid pace of technological change.

Cyber Operations and Occupational Resiliency

Developing an occupational resiliency capability or function within Cyber Force will ensure cyber operations and the operators themselves are as effective as possible. Principles around occupational resiliency could also factor into screening, selection, and accession, as well as acquisition and capability development.

The commission identified several potential ways to facilitate occupational resiliency, including specialized assessment and selection, embedded psychological support, protection of operational focus, and learning best practices from the special operations community's approach to deployment cycles.

SUPPORT TO THE JOINT FORCE

The service cyber components under CYBERCOM are currently organized to align to the unified combatant commands.[41] To represent the service cyber components and present cyber capability, each of the components forms and positions Cyber Operations-Integrated Planning Elements at the respective combatant commands.

Table 7: Service Cyber Component Areas of Responsibility

Service Cyber Component	Area of Responsibility
Marine Corps Forces Cyberspace Command / Joint Forces Headquarters-Cyber (Marines)	Special Operations Command (SOCOM)
Army Cyber Command / Joint Forces Headquarters-Cyber (Army)	Central Command (CENTCOM) Africa Command (AFRICOM) Northern Command (NORTHCOM)
Fleet Cyber Command / Joint Forces Headquarters-Cyber (Navy)	Indo-Pacific Command (INDOPACOM) Southern Command (SOUTHCOM) Forces Korea (USFK)
Air Force Cyber Command / Joint Forces Headquarters-Cyber (Air Force)	European Command (EUCOM) Strategic Command (STRATCOM) Transportation Command (TRANSCOM) Space Command (SPACECOM)

Source: CSIS Commission on U.S. Cyber Force Generation.

This design has recently faced criticism. In 2025, the Senate and the House of Representatives separately advanced legislation requiring evaluations of the command and control (C2) of cyber elements in support of regional and functional combatant commands. Rep. Don Bacon, chair of the House Armed Services Committee's cyber subcommittee, noted, "I've grown increasingly concerned that we are not correctly organized for the cyber fight we find ourselves in today. . . . I want to ensure our Cyber team is postured right for a potential fight with China over Taiwan."[42]

The commission analyzed existing C2 designs employed today by the military services in presenting forces to combatant commands in its analysis of potential courses of action for the Cyber Force in its force presentation responsibilities. The commission determined that the greatest efficacy will be realized through a C2 construct that mirrors the force presentation model of the existing services, with a service component command (or in this scenario, a "Cyber Force Component Command") aligned to each of the unified combatant commands.

UNIFIED COMPONENT COMMANDS

The commission recommends that the Cyber Force develop Cyber Force Component Commands (CFCCs) at each of the unified combatant commands, consolidating and assuming the functions currently assigned to the service cyber components and their embedded Cyber Operations-Integrated Planning Elements. Most importantly, CFCCs, answerable to their respective combatant commanders as well as to the chief of the Cyber Force, will be expected to align the development of Cyber Force capabilities with combatant commands' operational requirements and their Joint Integrated Prioritized Target Lists. CFCCs will work toward integrating cyber capabilities into operational and concept plans, and they will coordinate efforts with other component commands at their respective combatant command. The CFCCs will also be responsible for the C2 of cyber units assigned as direct support within their AORs (for geographic combatant commands), where the various echelons will plan and conduct actual operations.

Each CFCC will require sufficient resources (i.e., personnel, access, and infrastructure) to support the combatant commands' operational and concept plans, even though some of the resources may not be confined to a given area of operation. Unlike the other services, which mostly have large inventories of personnel and weapons platforms which can be redirected toward a new mission in a relatively short period of time, the intricacies of cyber operations necessitate that the Cyber Force is continuously updating and maintaining capabilities to be effective when called upon.

Special Operations Command (SOCOM) and Cyber Force

U.S. Special Operations Command is one of the only combatant commands, other than CYBERCOM, that conducts cyberspace operations with capabilities embedded within multiple components, in addition to the command's headquarters.[43] Additionally, Marine Corps Forces Cyberspace Command (MARFORCYBER) is CYBERCOM's assigned service cyber component. Given the utilization of cyberspace operations within the special operations enterprise, the commission saw particular value in a Cyber Force Component Command for SOCOM.

Similar to other CFCCs, a CFCC for SOCOM (referred to as CYBERSOC) will operate as the integrator for cyber operations into the SOCOM planning process and maintain visibility and ADCON for assigned Cyber Force elements. Finally, CYBERSOC will also serve as a proponent for capabilities particular to special operations within the Cyber Force's Planning, Programming, Budgeting, and Execution processes.

Unlike other CFCCs, a component within SOCOM will have a fully global mission and a higher likelihood of close-access-type operations. Due to the increased expeditionary nature and shorter duration of missions, the teams supporting SOCOM will need to consist primarily of military personnel capable of meeting unique physical requirements and demands and be trained for different mission sets and technologies.

Force Provider to NSA and Central Security Service

The military services all provide personnel to support the NSA's intelligence mission. Their skills include, but are not limited to, all-source and specialized intelligence analysis (e.g., SIGINT), linguistics, and cyber operations. If established, the Cyber Force will play an important role in providing personnel to the NSA for operational roles, such as on-net operators and capability developers. While occupying billets inside operational components, such as CYBERCOM, these individuals will operate under Title 10 authorities, but they could also be leveraged for similar roles at the NSA where they will operate under Title 50 authorities. It is important to clarify that the Cyber Force will not become the sole force provider to NSA. The Army, Navy, Marine Corps, Air Force, and Space Force still have a vested interest in having their service members assigned to NSA in a multitude of roles and responsibilities.

Force Generation and Training Command

The Cyber Force should also establish a Cyber Force Generation and Training Command with the responsibility for generating, sustaining, and certifying ready cyber forces for operational employment. This role will extend beyond operating schools or administering curricula. It will connect training, qualification, mission rehearsal, and readiness validation into a single

force-generation enterprise to ensure personnel and units are prepared for the missions they will perform.

Presently, some elements either exist or are being planned. Entities such as the National Defense University's College of Information & Cyberspace and the CYBERCOM 2.0-connected Advanced Cyber Training & Education Center will be important initial building blocks for the Cyber Force's own Force Generation and Training Command.

The Force Generation and Training Command will institutionalize processes for continuous development and course changes to keep pace with the threat. The command should have both the responsibility and the authority to translate changes in mission requirements, operating conditions, target environments, and technical practice into corresponding changes in training, qualification, rehearsal conditions, and readiness standards. The avoidance of "training drift" should therefore be treated as a core tenet of the command design, not as an occasional corrective action.

The Force Generation and Training Command should bring together the major functions required to keep the force current: formal training and qualification; training environment design and sustainment; lessons learned and doctrinal refinement; and standards, evaluation, and readiness validation. These functions may be carried out by different subordinate organizations, but they should remain within one command structure so that the authority to identify change, the means to incorporate change, and the authority to certify readiness are not separated from one another.

The command should also maintain a shared service training and readiness environment that supports the full force generation continuum. That environment should be able to support accession training, specialty qualification, continuation training, mission rehearsal, and other force preparation activities under different conditions and levels of protection, while still allowing relevant scenarios, target representations, mission conditions, and evaluation tools to move efficiently across the enterprise. The essential point is not a particular technical architecture but a common backbone that allows the service to preserve continuity between training, rehearsal, and readiness validation and distribute those updates broadly rather than recreate them separately across disconnected systems.

Force Generation and Training Command should treat all training and readiness conditions as subject to review, refresh, and replacement as mission demands evolve. No part of the training continuum should be assumed current by default. Qualification events, training environments, scenario libraries, and mission-representative conditions should remain authoritative only so long as they reflect operational need. This should place the burden on the institution to keep the enterprise current, rather than on individual units to compensate for outdated training conditions on their own.

The Cyber Force should assume that training relevance cannot be preserved by a schoolhouse acting alone—it requires an institutional connection between those who generate the force and those who employ and develop it.

A permanent feedback relationship with operational forces should be built into the command structure. Operators, intelligence personnel, capability developers, instructors, and evaluators should all have formal roles in identifying needed changes and ensuring that relevant updates move into the training and readiness enterprise without delay. This should not be a matter of occasional coordination—it should be a standing feature of how the command functions. The Cyber Force should assume that training relevance cannot be preserved by a schoolhouse acting alone—it requires an institutional connection between those who generate the force and those who employ and develop it.

The Force Generation and Training Command should also be the authoritative source of readiness validation for force presentation. Course completion alone should not be treated as proof of readiness. Individuals and units should be assessed through performance in mission-representative conditions aligned to the missions for which they are being prepared. In this model, training and readiness remain linked but distinct: Training develops capability, while validation confirms the ability to perform under relevant conditions. The same command should oversee both so that readiness standards remain tied to the realities reflected in the training enterprise.

Personnel policies should reinforce this design. The Force Generation and Training Command should remain connected to current practice by drawing recent operators and technical specialists into instructor, evaluator, and training-development roles while allowing those personnel to return to operational or developmental assignments afterwards. This will reduce the risk that institutional training becomes isolated from the force it exists to support and will help ensure that the command remains a current and credible authority for readiness generation.

The success of the Force Generation and Training Command should be judged accordingly. Throughput and course production matter, but they are not enough. The more important measure is whether the command keeps the force ready: whether training, qualification, and validation reflect present mission demands, whether readiness assessments match assigned missions, and whether operational change is consistently translated into updated standards and training conditions across the service.

The Force Generation and Training Command should be designed as the Cyber Force's force generation engine for readiness. Its defining feature should not be the number of schools it operates but its ability to convert accessions and experienced entrants into qualified personnel, sustain their relevance over time, and certify forces against conditions that remain aligned with operational reality.

Summary of Recommendations

The Commission on U.S. Cyber Force Generation was tasked with articulating a vision, mission, and implementation plan for a notional Cyber Force, rather than with reprising existing debates about whether such a force should be established. The report's core recommendations center on the elements required to stand up a United States Cyber Force, a new military service with a narrowly defined, cyber-specific mission. Its central obligation would be to organize, train, and equip forces to conduct offensive and defensive cyberspace operations. Critically, this ensures that DODIN Operations are retained by the Army, Navy, Marine Corps, Air Force, and Space Force. If established, the Cyber Force would assume most of the "service-like" responsibilities currently held by CYBERCOM, mirroring the relationship between the existing services and the combatant commands established following Goldwater-Nichols reforms.

Several important assumptions flow from this core recommendation. First, the Cyber Force would be established as an independent branch of the Armed Forces within the DOD with force generation responsibilities comparable to the existing military services. Second, in executing this transition, priority would be given to minimizing disruptions to current and ongoing cyber operations being carried out by the existing services. Finally, the Cyber Force would need to be stood up within the DOD at a meaningful speed to meet the evolving threat environment.

Notably, the commission recommends establishing a Cyber Force totaling around 30,000 personnel—with an end strength of 20,000 active-duty uniformed personnel, an additional 3,500-5,000 National Guard personnel, and a civilian complement of 5,000–6,000 personnel. Among uniformed personnel, the commission recommends the Cyber Force consist of

commissioned officers and warrant officers, but not an enlisted cadre. The commission recommends against standing up a Cyber Force Reserve capability, preferring to have a National Guard construct able to operate under both federal and state authorities, a model enabling the DOD to leverage part-time talent and support recovery efforts for cyberattacks on critical infrastructure.

Building on current DOD funding levels, the commission estimates the initial budget requirement to stand up the Cyber Force would be around $10–$11 billion. The commission considered two viable options for the Cyber Force's institutional alignment with the DOD, including the benefits and trade-offs of each option. The first option is alignment within the Department of the Army. This would allow the Cyber Force to fit within the existing DOD bureaucracy, which could then be leveraged for speed and efficiency. A key trade-off of this option is the risk that the Cyber Force would be considered lower priority than the much larger Army organization.

A second option is aligning the Cyber Force in its own military department within the DOD, a new Department of the Cyber Force. This option would ensure maximum prioritization of cyber issues across the Pentagon as required by the current threat environment and force generation challenges. The key trade-off is that standing up an entirely new Pentagon bureaucracy would require significant time and resources and thus take significantly longer to implement.

Commissioners estimated that, regardless of institutional alignment, reaching initial operating capacity for the new Cyber Force would take between 12 and 18 months and proceed through several sequential phases: setting conditions; fielding an initial operating capacity; growing iteratively over several years; and refining institutionally. This phased approach emphasizes maintaining force quality over establishing force mass and preferences experimentation through novel approaches rather than rigid design features.

Following a presidential decision or legislative action to establish a new Title 10 service, this force generation model would address longstanding structural challenges and build the Cyber Force the United States needs for this critical domain of warfare.

About the Authors

Joshua Stiefel is vice president for government relations at Second Front, a public benefit, venture-backed technology company specializing in national security and accelerating government access to commercially proven software. Previously, he spent nearly seven years as a professional staff member for the House Armed Services Committee (HASC) where he was responsible for the oversight, legislation, and policy for the Department of Defense's cyber warfare, cybersecurity, and information technology activities, a portfolio of more than $25 billion annually. He conceived, authored, and negotiated nearly 400 provisions of law enacted across seven annual National Defense Authorization Acts. Prior to Capitol Hill, Josh spent 10 years in the executive branch with the Departments of Defense and the Treasury. He is a former term member at the Council on Foreign Relations and served for eight years as a commissioned officer in the U.S. Navy Reserve. He holds a master of public policy from Harvard University and a bachelor of arts with honors from Lehigh University.

Lieutenant General (Retired) Ed Cardon's service to our nation spans over 36 years, with extensive experience establishing, leading, and transforming 14 very different organizations with diverse mission sets such as operations, education, cyber, and innovation. He commanded the 2nd Infantry Division in the Republic of Korea. He both transformed and scaled Army Cyber Command into a world-class cyber force while simultaneously standing up new cyber organizations to meet the demands of this contested domain, including CYBERCOM's Task Force ARES, the offensive cyber task force against ISIS. He spearheaded the creation of the Cyber Branch for the U.S. Army, the first new branch of the twenty-first century. His last assignment was as the director of business transformation for the Army, and he led the task force that helped create Army Futures Command

responsible for modernizing the Army. Today, General Cardon is a founding partner and co-CEO of Touchstone Futures, a senior counselor with the Cohen Group, a visiting scholar at the Vanderbilt Institute of National Security, and a senior adviser for the Army Cyber Institute.

Lauryn Williams is the deputy director and senior fellow in the Strategic Technologies Program at the Center for Strategic and International Studies. Until January 2025, she was chief of staff to the assistant secretary of defense for industrial base policy within the Office of the Under Secretary of Defense for Acquisition and Sustainment, where she spearheaded the release of the National Defense Industrial Strategy Implementation Plan. From 2022 to 2024, Lauryn was director for strategy in the White House Office of the National Cyber Director and led the strategic initiative on space system cybersecurity, which leveraged extensive government agency, industry, and international collaboration. This work resulted in the first-ever minimum cybersecurity requirements for federal space systems. Prior to the White House, Lauryn served as a policy adviser in the Pentagon space policy office and led efforts to leverage commercial space and develop norms of responsible behavior. She has also served in the Department of Energy's National Nuclear Security Administration, where she led international export control projects, and worked at the Carnegie Endowment for International Peace. Lauryn received her master's degree in public and international affairs from Princeton University and her bachelor's degree in political science, with honors in international security studies, from Stanford University.

Taylar Rajic is an associate fellow for the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS). Her research focuses on the cyber threat landscape, adversarial capabilities in cyber warfare and cyber espionage, and the protection of critical and digital infrastructure. Prior to joining CSIS, she conducted research on irregular warfare at the National Defense University in Washington, D.C. She received an MA in international peace and conflict resolution from American University and a BA in political science and Russian from the University of Melbourne.

Matt Pearl is director of the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS), where he focuses on the intersection of technology, national security, and geopolitics. A veteran of the White House and the Federal Communications Commission (FCC), he brings more than a decade of experience shaping U.S. technology policy. Prior to joining CSIS in 2025, Mr. Pearl served on the White House National Security Council as director for emerging technologies and special adviser to the deputy national security adviser. In this role, he coordinated interagency strategy and helped lead initiatives such as the National Spectrum Strategy, the U.S. Cyber Trust Mark for Internet of Things security, and the International Joint Statement on 6G Principles. His portfolio spanned data security, cloud computing, space governance, critical infrastructure resilience, and the national security review of foreign investments through the Committee on Foreign Investment in the United States and Team Telecom. Previously, Mr. Pearl spent more than ten years at the FCC, where he rose to associate bureau chief of the Wireless Telecommunications Bureau. There, he managed major spectrum transitions to support next-generation wireless networks. An expert on U.S.-China technology competition, he has testified before the Senate Committee on Commerce, Science, and Transportation. His commentary

has appeared in the *New York Times*, the *Washington Post*, *Politico*, and NPR. Mr. Pearl was a research affiliate at Harvard's Berkman Klein Center and clerked for both federal district and appellate courts. He earned his JD from Yale Law School, where he served as an editor of the *Yale Journal on Regulation*.

Erica D. Lonergan is an assistant professor in the School of International and Public Affairs (SIPA) at Columbia University. Previously, Erica held several positions at the United States Military Academy at West Point. These include serving as an assistant professor in the Departments of Social Science and Electrical Engineering and Computer Science; a fellow at the Army Cyber Institute; and executive director of the Rupert H. Johnson Grand Strategy Program. She has also held positions as a senior fellow at the Carnegie Endowment for International Peace and the Atlantic Council. Beyond her academic and research appointments, Erica has an extensive background in strategy and policy. Erica served as a member of the Board of Visitors of the U.S. Army War College. Previously, she was a writer of the 2023 U.S. Department of Defense Cyber Strategy. Prior to that, Erica served as a senior director on the U.S. Cyberspace Solarium Commission, a bipartisan congressional commission established to develop a new strategy and policies to defend the United States in cyberspace. Erica continues to serve as a senior adviser to the Cyberspace Solarium Commission 2.0. She also held an appointment as a Council on Foreign Relations international affairs fellow, with placement at JPMorgan Chase and U.S. Cyber Command at the Cyber National Mission Force.

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Founded in 1962, CSIS is led by General Joseph F. Dunford, who was appointed chief executive officer in 2026, succeeding John J. Hamre. The CSIS Board of Trustees is chaired by Thomas J. Pritzker, who has held the position since 2015.

CSIS brings together more than 275 full-time staff and a global network of affiliated scholars working across four core areas of public policy: defense and security, geopolitics and foreign policy, economic security and technology, and global development. Our scholars are regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer recommendations to improve U.S. strategy.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—non-partisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

What sets CSIS apart is not only the quality of its research but how that research is conveyed: through original data and open-source analysis; through multimedia and data visualization; and through connecting relevant analysis with key audiences at the moments that matter most. This combination of rigor, independence, and reach has made CSIS a driving force in the policy debates shaping American security and prosperity.

Appendix

Table A-1: Service-by-Service Function Comparison Today (as of 2026)

	Army	Air Force	Navy	Marine Corps	Space Force	Cyber
Senior Civilian	Service secretary	Service secretary	Service secretary	Service secretary	Service secretary	Assistant Secretary
Senior Uniformed Officer	Four-star general officer (O-9)	Four-star general officer (O-9)	Four-star flag officer (O-9)	Four-star general officer (O-9)	Four-star general officer (O-9)	
Dedicated Acquisition Personnel	Acquisition cadre	Acquisition cadre	Acquisition cadre	Acquisition cadre	Acquisition cadre	
Dedicated Budgeting Personnel	Budgeting and resourcing cadre	Budgeting and resourcing cadre	Budgeting and resourcing cadre	Budgeting and resourcing cadre	Budgeting and resourcing cadre	
Foundational Intelligence Support	Service intel center (NGIC)	Service intel center (NAISIC)	Service intel center (ONI)	Service intel center (MCIA)	Service intel center (NSIC)	
Dedicated Legal Support	JAG corps	JAG corps	JAG corps	JAG corps		
Domain-centric Educational Programs	Senior development education school(s)	Senior development education school(s)	Senior development education school(s)	Senior development education school(s)	Senior development education school	
Medical Personnel	Dedicated medical support	Dedicated medical support	Dedicated medical support	Dedicated medical support		
Force Generation-responsible Command	Force generation command (FORSCOM)	Force generation command (ACC)	Force generation command (Fleet Forces Command)	Force generation command (Marine Corps Forces Command)	Force generation command (Space Training and Readiness Command)	
Dedicated MDCO	MDCO (CID)	MDCO (AFOSI)	MDCO (NCIS)			
Dedicated MCIO	MCIO (Army CIC)	MCIO (AFOSI)	MCIO (NCIS)			
Research Organization	Army Research Lab	Air Force Research Lab	Naval Research Lab	Naval Research Lab	Air Force Research Lab	
Legislative Proponency	Major general (O-8)	Major general (O-8)	Vice admiral (O-9)	Major general (O-8)	Major general (O-8)	Colonel (O-6)

Source: CSIS Commission on U.S. Cyber Force Generation.

Endnotes

1 The White House, *President Trump's Cyber Strategy for America* (Washington, DC: The White House, March 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf.

2 Tim Starks, "Former NSA, Cyber Command chief Paul Nakasone says U.S. falling behind its enemies in cyberspace," CyberScoop, February 22, 2025, https://cyberscoop.com/former-nsa-cyber-command-chief-paul-nakasone-enemies-cyberspace/.

3 Anne Neuberger, "China is Winning the Cyberwar," *Foreign Affairs*, September, October 2025. https://www.foreignaffairs.com/china/china-winning-cyberwar-artificial-intelligence.

4 Katie Sutton, "Statement by Honorable Katherine Sutton, Assistant Secretary of War for Cyber Policy, before the Committee on Armed Services, United States Senate," 118th Cong., 2nd sess., April 28, 2026, https://www.armed-services.senate.gov/imo/media/doc/sutton_opening_statement1.pdf.

5 U.S. Department of Defense, *DODD 5100.01, Functions of the Department of Defense and Its Major Components* (Washington, DC: DOD, revision published September 17, 2020), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/510001p.pdf.

6 10 U.S.C. § 7013(b).

7 Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. No. 99-433, 100 Stat. 992 (1986), https://www.congress.gov/bill/99th-congress/house-bill/3622.

8 Donald J. Trump, "Presidential Memorandum for the Secretary of Defense–SUBJ: Elevation of U.S. Cyber Command to a Unified Combatant Command," presidential memorandum, August 18, 2017, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-secretary-defense/.

9 Joseph W. Kirschbaum et al., *DOD Cyberspace Operations: About 500 Organizations Have Roles, with Some Potential Overlap*, GAO-25-107121 (Washington, DC: GAO, September 2025), https://www.gao.gov/assets/gao-25-107121.pdf.

10 Ibid., 16–17.

11 Ibid., 2.

12 Matthew Olay, "Hegseth, Caine Laud Success of U.S. Strike on Iran Nuke Sites," DOD News, June 22, 2025, https://www.war.gov/News/News-Stories/Article/Article/4222533/hegseth-caine-laud-success-of-us-strike-on-iran-nuke-sites/.

13 National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, 139 Stat. 718 § 401 (2025).

14 Kirschbaum et al., *DOD Cyberspace Operations*.

15 Carl Levin & Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, 128 Stat. 3292 § 1631 (2014), https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf.

16 Catherine A. Theohary, "FY 2026 Department of Defense Cyber Budget Request," Congressional Research Service, IN12616, November 24, 2025, https://www.congress.gov/crs_external_products/IN/PDF/IN12616/IN12616.1.pdf.

17 National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, 135 Stat. 1542 § 1507 (2021).

18 DOD Comptroller, *FY2021 Defense Budget Overview* (Washington, DC: DOD, February 2020, revised May 2020), https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Budget_Request_Overview_Book.pdf; and *National Defense Authorization Act for Fiscal Year 2020*, Pub. L. 116-92, 133 Stat. 1198 (2019).

19 "Tech Force," U.S. Office of Personnel Management, accessed May 27, 2026, https://techforce.gov/.

20 As of May 2026, the Space Force does not present operational forces to CYBERCOM.

21 Matt Pearl, host, *Cache Me If You Can*, podcast, "Views from the Cyber Trenches: Understanding U.S. Military Cyber Dynamics," Center for Strategic and International Studies, November 25, 2025, https://www.csis.org/podcasts/cache-me-if-you-can/views-cyber-trenches-understanding-us-military-cyber-dynamics.

22 Brenda S. Farrell et al., *Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking*, GAO-23-105423 (Washington, DC: GAO, December 2022), https://www.gao.gov/assets/d23105423.pdf.

23 U.S. Department of War, "Department of War Establishes CYBERCOM 2.0 – Revised Cyber Force Generation Model," press release, November 6, 2025, https://www.war.gov/News/Releases/Release/Article/4330204/department-of-war-establishes-cybercom-20-revised-cyber-force-generation-model/.

24 While the USPHS does not leverage the authority, the service is authorized by law to appoint warrant officers for the purpose of providing support to the health and delivery systems maintained by the Public Health Service (42 U.S.C. §204).

25 U.S. Department of Defense, "Basic Pay," DoD Financial Management Regulation, DoD 7000.14-R, vol. 7A, chap. 1, May 2024, https://comptroller.war.gov/Portals/45/documents/fmr/current/07a/07a_01.pdf.

26 Department of Defense, *2024 Demographics: Profile of the Military Community* (Washington, DC: DOD, 2024), https://download.militaryonesource.mil/12038/MOS/Reports/2024-demographics-report.pdf.

27 William Hartman, "Posture Statement of Lieutenant General William J. Hartman, USA, Acting Commander, United States Cyber Command, before the 119th Congress, House Armed Services Committee, Subcommittee on Cyber, Information Technologies, and Innovation," 118th Cong., 1st sess., May 16, 2025, 16, https://armedservices.house.gov/uploadedfiles/5.16_hartman_testimony.pdf.

28 John Fernandes, Erica D. Lonergan, and Alexander Master, "Why Culture Matters: Organizational Culture and Force Generation for the Cyber Domain," Cyber Defense Review, January 27, 2026, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4390474/why-culture-matters-organizational-culture-and-force-generation-for-the-cyber-d/.

29 Jesse Chace, "Special Operations Forces' Structured Readiness Model Makes Conventional Military Intelligence Unit More Effective," *Military Intelligence Professional Bulletin* (January–March 2021): 35–39, https://www.ikn.army.mil/apps/MIPBW/MIPB_Features/Chace.pdf.

30 Within the commission's deliberations, the Department of the Army was considered the only credible option within which a United States Cyber Force could be aligned. None of the commissioners viewed the Department of the Navy nor the Department of the Air Force as legitimate options, given that each already has the responsibility for two military services.

31 10 U.S.C. §7013.

32 The White House, "Establishment of the United States Space Force," press release, February 19, 2019, https://www.spaceforce.mil/About-Us/SPD-4/.

33 Department of War, *FY2027 Budget Request Overview Book* (Washington, DC: DOW, April 2026), https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2027/FY2027_Budget_Request_Overview_Book.pdf; and Department of Defense, *Defense Budget Overview Fiscal Year 2020 Budget Request* (Washington, DC: DOD, March 2019), https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2020/fy2020_Budget_Request_Overview_Book.pdf.

34 Erica D. Lonergan and John Snyder, "Cultural Change in Military Organizations: Hackers and Warriors in the US Army," *Texas National Security Review* 8, No. 3 (Summer 2025): 74– 95, https://doi.org/10.26153/tsw/60740.

35 Ibid.

36 The "service intelligence centers" refer to the National Air and Space Intelligence Center (Air Force), Office of Naval Intelligence (Navy), Marine Corps Intelligence Activity (Marine Corps), National Ground Intelligence Center (Army), and National Space Intelligence Center (Space Force).

37 Nicholas Drauschak, Robert Rupe, and Philip Massine, "Building the Base: Using the Army's Intelligence Program of Analysis to Drive Foundational Intelligence," *Military Intelligence Professional Bulletin* (January-March 2020): 14–19, https://mipb.ikn.army.mil/media/kibjbqed/2020-01-03-building-the-base-using-the-armys-intelligence-program-of-analysis-to-drive-foundational-intelligence.pdf.

38 George I. Seffers, "Cyber Command Advocates Cyber Intel Center," Signal, November 14, 2022, https://www.afcea.org/signal-media/intelligence/cyber-command-advocates-cyber-intel-center.

39 Mark Pomerleau, "Cyber Command working to create an intelligence center," DefenseScoop, February 28, 2023, https://defensescoop.com/2023/02/28/cyber-command-working-to-create-an-intelligence-center/.

40 Sec. 1612, Servicemember Quality of Life and National Defense Authorization Act for Fiscal Year 2025, Pub. L. No. 118-159, 138 Stat. § 1612 (2024).

41 Royal A. Davis III et al., *Air Force Cyber Law Primer* (Montgomery, AL: Air University, November 2022), https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/CPP_009_Davis_Air_Force_Cyber_Law_Primer.pdf.

42 Mark Pomerleau, "Congress pushing Joint Task Force-Cyber, shaking up how DOD employs digital capabilities," DefenseScoop, July 24, 2025, https://defensescoop.com/2025/07/24/ndaa-fy26-joint-task-force-cyber-shake-up-how-dod-employs-digital-capabilities/.

43 Kirschbaum et al., *DOD Cyberspace Operations*.