FOUNDATION FOR DEFENSE OF DEMOCRACIES

Building the Future U.S. Cyber Force

What Right Looks Like

Dr. Erica Lonergan and RADM (Ret.) Mark Montgomery

September 2025

Building the Future U.S. Cyber Force

What Right Looks Like

Dr. Erica Lonergan

RADM (Ret.) Mark Montgomery

September 2025

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

EXECUTIVE SUMMARY 6

THE STATUS QUO IS UNSUSTAINABLE 7

VISION AND MISSION OF THE CYBER FORCE 9

CORE DESIGN DECISIONS:
THE BUILDING BLOCKS OF ESTABLISHING THE CYBER FORCE 11

- What the Cyber Force Will Not Be 14
- Defining the Primary Force Generation Responsibilities 15

HOW TO BUILD THE SERVICE 16

- Which Existing Organizations Would Be Subsumed by the Cyber Force 16
- Design Principles 18

A PROPOSED IMPLEMENTATION PLAN 21

- Phase I: Planning and Conditions Setting (First 3 Months) 21
- Phase II: Progressive Build (Approximately First 2 Years) 25
- Additional Critical Decisions in Phases I and II 26

CONCLUSION: THE FUTURE OF THE CYBER FORCE 28

Executive Summary

The U.S. military has tried almost everything to fix its cyber problems — except for the one solution that would work: standing up a U.S. Cyber Force as a new branch of the armed forces. Today, the military lacks sufficient readiness to fight and accomplish other missions in cyberspace, and only a Cyber Force can generate the human and technical resources the nation requires to fight and win the conflicts of today and the wars of tomorrow.

This study builds on the authors' previous report making the case for establishing a Cyber Force. Beginning with that conclusion, this study outlines the practical steps necessary to stand up the new service. It presents an adaptable framework to address the choices and challenges that will likely accompany the Cyber Force's creation. It is imperative that the Cyber Force gets four fundamental elements right from the outset: personnel, leadership, capabilities, and culture.

The first steps toward the creation of the Cyber Force are to lay out its vision and mission and define its functions. The Cyber Force will be the nation's principal military force for the cyber domain. Its purpose will be to organize, train, and equip the personnel the military requires to employ cyber power to achieve tactical, operational, and strategic objectives. How it achieves these objectives will change over time given the dynamism of technology and international politics. Still, its core mission will endure.

The Cyber Force will have the primary force generation responsibility for offensive and defensive cyber operations, as well as cyber intelligence. Force generation refers to organizing, training, and equipping forces for military operations. The roles that remain outside the Cyber Force's core mission set will include generating capabilities for information operations, Department of Defense Information Network (DODIN) operations (securing the Defense Department's networks and systems), and cyber-related emerging technologies (such as artificial intelligence).

Next, the report advances a set of basic propositions about the Cyber Force's place within the armed forces, its relationship to U.S. Cyber Command (the combatant command with the primary responsibility for operating in cyberspace) and existing armed services, and its personnel and budget. These serve as the building blocks for creating the Cyber Force. In turn, this study details how existing cyber-related organizations within the Defense Department, such as the various operational groups within the Cyberspace Operations Forces (COF) and other relevant organizations, would relate to the Cyber Force.[1] Several will be subsumed by the new service.

Several design principles inform our approach to building the service: prioritizing quality over quantity of personnel, implementing an expertise-based career progression model, accommodating a force structure that can adapt over time, adopting a phased approach to building the service, and cultivating the right organizational leadership and culture.

Finally, no amount of strategic thinking will catalyze the creation of a Cyber Force without an implementation plan. This report outlines such a plan with a phased approach for the service's initial build. The plan first identifies the core tasks to address in the first several years following the service's establishment. Crucially, the process must be iterative and adaptive. This is to avoid getting locked into suboptimal paths, allowing the organization to adapt to changing needs and missions.

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. The question of establishing an independent service for cyberspace is more a matter of "when" than "if." This paper sets a mark for future policymakers who will grapple with the complex and challenging decisions surrounding how best to establish the Cyber Force.

1. For a definition of the COF, see: U.S. Air Force, "Air Force Doctrine Publication 3-12: Cyberspace Operations," February 1, 2023. (https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf)

The Status Quo Is Unsustainable

The fiscal year 2025 National Defense Authorization Act (NDAA) directs the National Academies of Sciences, Engineering, and Medicine (NASEM) to "conduct an evaluation of alternative organizational models for the cyber forces of the Armed Forces." This includes assessing the "feasibility and advisability of establishing a separate Armed Force in the Department of Defense dedicated to operations in the cyber domain."[2] A bipartisan group of lawmakers believes the NDAA-directed study does not go far enough. In January, Reps. Morgan Luttrell and Pat Fallon, both Texas Republicans, together with Sen. Kristen Gillibrand (D-NY), sent a letter to NASEM and Secretary of Defense Pete Hegseth urging NASEM to explicitly address "the question of whether or not the nation is best served through the establishment of a United States Cyber Force as a seventh branch of the armed forces."[3]

The congressionally mandated NASEM study reflects many years of debate in Washington about whether the Defense Department is appropriately organized — and whether the military is at a sufficient level of readiness — to address the scope, scale, and magnitude of cyber threats. Most experts agree that the status quo is unsustainable.[4] In February 2025, the former commander of Cyber Command, retired Gen. Paul Nakasone, noted publicly that the United States is falling "increasingly behind" its adversaries in cyberspace. He remarked that incidents attributed to the People's Republic of China, such as the Volt Typhoon compromise of critical infrastructure, "[illustrate] the fact that we're unable to secure our networks, the fact that we're unable to leverage the software that's being provided today, the fact that we have adversaries that continue to maintain this capability."[5] These revelations about nation-state intrusions only underscore the urgency and scale of the challenge.

> **"Force generation in cyberspace is suffering, and the nation's readiness to fight in cyberspace is lagging."**

In 2024, we proposed a solution to address these readiness challenges: the United States should establish a new military service, a Cyber Force, with primary responsibility for generating forces for warfighting in the cyber domain.[6] Extensive interviews with more than 75 active-duty and retired U.S. military officers, each with deep operational and command experience in the cyber domain, informed our conclusions.[7] The overwhelming sentiment among this experienced cadre of officers was that the current force generation model is the root cause of the military's insufficient readiness. Meanwhile, current programs to address existing cyber workforce and talent management shortfalls are valuable but

2. Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, H.R. 5009, 118th Congress (2024). (https://docs.house.gov/billsthisweek/20241209/RCP_HR5009_xml%5b89%5d.pdf)
3. Martin Matishak, "Lawmakers push for guardrails, deadline on cyber military study," *The Record*, January 30, 2025. (https://therecord.media/lawmakers-push-for-guardrails-deadline-cyber-force-study)
4. Barbara Booth, "The Pentagon's battle inside the U.S. for control of a new Cyber Force," *CNBC*, November 22, 2024. (https://www.cnbc.com/2024/11/22/pentagon-battle-military-control-new-national-cyber-force.html)
5. 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); U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a)
6. Erica Lonergan and retired Rear Adm. Mark Montgomery, "United States Cyber Force A Defense Imperative," *Foundation for Defense of Democracies*, March 2024. (https://www.fdd.org/analysis/2024/03/25/united-states-cyber-force)
7. Erica Lonergan, Todd Arnold, and Nick Starck, "The Case for a Prospective U.S. Cyber Force," *War on the Rocks*, May 22, 2024. (https://warontherocks.com/2024/05/the-case-for-a-prospective-u-s-cyber-force); Eugenia Lostri, Erica Lonergan, and Jen Patja, "Lawfare Daily: The Case for a U.S. Cyber Force," *Lawfare*, April 22, 2024. (https://www.lawfaremedia.org/article/lawfare-daily-the-case-for-a-u.s.-cyber-force)

cannot rectify military cyber readiness shortfalls.[8] Put simply, force generation in cyberspace is suffering, and the nation's readiness to fight in cyberspace is lagging. There are negative implications for force employment in terms of the pace, inventiveness, and conduct of cyber operations, which are a consequence of the current force generation challenges.

At the crux of our argument is the distinction between force generation and force employment. Following the 1986 Goldwater-Nichols Act's reorganization of the Defense Department, the U.S. military has distinguished between the roles and responsibilities of the services to generate — organize, train, and equip — forces and those of the unified combatant commands (the geographic and functional military commands) to employ forces and request manpower from each of the services.[9]

Each service is oriented toward force generation for specific warfighting domains: land, air, sea, and space. The Defense Department has defined cyberspace as a domain of warfare for more than two decades.[10] However, no single entity has primary responsibility for recruiting, training, promoting, retaining, and equipping the right personnel, with the unique skill sets and competencies required for warfighting in the cyber domain. With the creation of the U.S. Space Force in 2019, cyberspace is now the only domain of warfare for which there is no corresponding service.[11]

Each service is optimized for recruiting, training, managing, and equipping personnel for the distinct warfighting requirements of its own operational domain. In the current force generation model for cyberspace, established in 2012, each of the services also organizes, trains, and equips cyber forces. However, each service views cyberspace as a peripheral concern; none regards cyberspace as its primary responsibility. As a result, the services are not providing quality forces in quantity to the Cyber Mission Force (CMF) — Cyber Command's "action arm."[12]

As things now stand, the overall force generation model is fractured, resulting in extraordinary inconsistencies and shortfalls in proficiency and readiness and deep struggles to recruit and retain top cyber talent. Internal surveys routinely reveal frustration and dismay among the cyber personnel about leadership, culture, mission, and climate.[13] The current model is also insufficient for the scope and scale of the cyber threat.

---

8. Ali Crawford, "Highlights from the National Cyber Workforce and Education Strategy," *Center for Security and Emerging Technology*, August 10, 2023. (https://cset.georgetown.edu/article/highlights-from-the-national-cyber-workforce-and-education-strategy); Examples of existing or proposed programs include the CyberCorps Scholarship for Service program, which is an effort to recruit and train cyber professionals across the federal workforce; efforts by states to establish volunteer Civilian Cyber Corps (C3) programs; proposals to establish a similar type of C3 program at the federal level, or the DOD Cyber Service Academy; "CyberCorps®: Scholarship for Service," *U.S. Office of Personnel Management*, accessed August 3, 2025. (https://sfs.opm.gov); Michael Razeeq, "Laying the Legal Foundation for Civilian Cyber Corps," *Lawfare*, September 19, 2024. (https://www.lawfaremedia.org/article/laying-the-legal-foundation-for-civilian-cyber-corps); "Cyber Volunteer Programs (Region 5)," *U.S. Cybersecurity and Infrastructure Security Agency*, accessed August 3, 2025. (https://www.cisa.gov/audiences/high-risk-communities/cybervolunteerresourcecenter/cyber-volunteer-programs-region-5); Natasha Cohen and Peter Warren Singer, "The Need for C3: A Proposal for a United States Cybersecurity Civilian Corps," *New America*, October 25, 2018. (https://www.newamerica.org/cybersecurity-initiative/reports/need-c3); "Cyber Service Academy," *U.S. Department of Defense Chief Information Officer*, accessed August 3, 2025. (https://dodcio.defense.gov/Cyber-Workforce/Cyber-Service-Academy)

9. Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. 99-433, 100 Stat. 992 (1986). (https://history.defense.gov/portals/70/documents/dod_reforms/goldwater-nicholsdodreordact1986.pdf)

10. "National Security Strategy Archive," *National Security Strategy Archive*, accessed August 3, 2025. (https://nssarchive.us/wp-content/uploads/library/nms/nms2004)

11. Jim Garamone, "Trump Signs Law Establishing U.S. Space Force," *DOD News,* December 20, 2019. (https://www.defense.gov/News/News-Stories/article/article/2046035/trump-signs-law-establishing-us-space-force)

12. U.S. Cyber Command, "CYBER 101 – Cyber Mission Force," November 1, 2022. (https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force)

13. Chad Bates and Charlene Rose, "Understanding—and Fixing—the Army's Challenge in Keeping Cyber Talent," *Modern War Institute at West Point*, May 17, 2022. (https://mwi.westpoint.edu/understanding-and-fixing-the-armys-challenge-in-keeping-cyber-talent); John Cobb, "Cyber Campaign Plans and Other Fairy Tales," *War on the Rocks*, December 20, 2024. (https://warontherocks.com/2024/12/cyber-campaign-plans-and-other-fairy-tales)

Calling on Cyber Command for Help Is Not Enough

To address the cyber force generation problem, lawmakers have turned to Cyber Command, even though it is a force employer, not a force generator. They have given it increasingly "service-like" authorities, including some for budgeting, training, and workforce development.

In fiscal year 2024, Congress provided the command with Enhanced Budgetary Control (EBC), giving it oversight of approximately $2 billion in acquisitions for that fiscal year.[14] Additionally, Cyber Command's "CYBERCOM 2.0" effort aimed to develop a new force generation model in response to years of unfulfilled congressional mandates to address the matter.[15]

The reliance on Cyber Command entails policymaking by analogy, in this case drawing on the precedent set by U.S. Special Operations Command (SOCOM), which also possesses service-like authorities. In theory, adopting a "SOCOM-like" or "Joint Special Operations Command (JSOC)-informed" model would address the current force generation challenges (JSOC is a component of SOCOM). However, the CYBERCOM 2.0 initiative, which critics describe as simply "status quo-plus," has not been implemented as the Pentagon assesses "whether that plan goes far enough."[16]

Even if fully implemented, such solutions are, at best, incomplete. For one, there is no consensus about what a "JSOC-informed" or "SOCOM-like" model for cyberspace actually entails.[17] There are also critical differences between special operations and cyber operations — not to mention problems with the SOCOM model itself. For one, each of the services generates special operations forces that reflect the distinct skill sets and requirements for conducting special operations within that particular domain (such as Army Rangers or Navy SEALs). Yet cyberspace is its own domain. For the most part, there are no skills particular to cyber operations on land as opposed to at sea or in the air. Moreover, there is a good deal of overlap between the desired profile of potential recruits for special operations and the recruiting profile for any of the services. However, this is not the case for the ideal cyber recruit. Additionally, there are practical and legal limitations to what Cyber Command as a combatant command can impose on the services with respect to force generation. While the command can set higher standards for the services to ostensibly meet, it has little recourse if they fail to do so. The predominant shortfalls in the current force generation model — critical gaps in recruitment, failure to retain quality personnel, and insufficient mastery of the skills needed to successfully operate in the cyber domain[18] — can be addressed only through the establishment of a Cyber Force.

Vision and Mission of the Cyber Force

The Cyber Force will become the nation's principal military force for the cyber domain. Its enduring purpose will be to organize, train, and equip personnel for the cyber domain, although precisely how the service fulfills this purpose must evolve along with cyber technology.

14. U.S. Cyber Command, "CYBER 101 – Cyber Mission Force," November 1, 2022. (https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force)
15. Martin Matishak, "After prodding from lawmakers, Cyber Command readies a plan for the future," *The Record*, October 22, 2024. (https://therecord.media/cyber-command-2-0-project-progress-military-congress); Matishak, "Cyber Command overhaul gets Austin's approval, but plan faces uncertain future," *The Record*, January 8, 2025. (https://therecord.media/cyber-command-overhaul-secdef-approval)
16. Mark Pomerleau, "DOD leadership asks for Cybercom 2.0 relook," *DefenseScoop*, May 20, 2025. (https://defensescoop.com/2025/05/20/cybercom-2-0-relook-dod-leadership)
17. Skyler Onken, Nick Starck, Erica Lonergan, JC Fernandes, Todd Arnold, and Maggie Smith, "Beyond Binaries: Cyber Force Generation and the SOCOM-like Model," *Irregular Warfare Initiative*, November 7, 2024. (https://irregularwarfare.org/articles/beyond-binaries-cyber-force-generation-and-the-socom-like-model)
18. John Cobb, "An Insider's Guide to Cyber Readiness," *War on the Rocks*, May 1, 2025. (https://warontherocks.com/2025/05/an-insiders-guide-to-cyber-readiness)

But the fundamental mission remains the same: (1) to ensure the nation has ready, capable forces across active, guard, and reserve components to compete, deter, fight, and win in the cyber domain; (2) to support unified action across the joint force, which involves the integrated and synchronized employment of the various military capabilities of the armed forces; and (3) to leverage cyber power, together with other instruments of power beyond the military, to achieve strategic objectives. Below, we offer a proposed mission statement for Cyber Force that encapsulates these core ideas.

Proposed Cyber Force Mission Statement

The United States invented the internet. We are a digital nation. The Cyber Force defends America in cyberspace, deters threats in and through cyberspace, and fights and wins in cyberspace should deterrence fail. We are a global force and a professional force, dedicated to technological excellence for sustained engagement in the cyber domain during peacetime, competition, crisis, and conflict. The Cyber Force will produce the world's dominant cyber force, develop innovative and agile cyber leaders, and continually equip personnel with the most advanced cyber warfighting capabilities.

Similar to the existing services, the Cyber Force will need to develop concepts, doctrine, tactics, techniques, and procedures, as well as organize, train, equip, and provide forces to perform specific military functions. In a cyber context, these functions include:

1. Defending the nation in cyberspace;
2. Deterring and defeating aggression in, from, and to the cyber domain;
3. Conducting offensive and defensive operations in and through the cyber domain;
4. Conducting intelligence, surveillance, reconnaissance, and the targeting of threats in cyberspace;
5. Interdicting and neutralizing cyber threats to the land, sea, space, and air domains;
6. Supporting messaging, strategic communications, information operations, and military deception through cyberspace; and
7. Creating and maintaining cybersecurity policies, standards, and procedures that guide all DOD cybersecurity activities.

To achieve this vision, the Cyber Force must get four things right:

- **Produce the world's preeminent military cyber personnel**. Currently, most of the nation's top cyber talent pursue careers outside of the military. The Cyber Force must find a way to effectively recruit, train, and retain a portion of this talent for its purposes. This will require looking beyond traditional recruitment pools. It will also require new mechanisms that leverage personnel elsewhere within government, as well as in industry and academia, in flexible full-time and part-time capacities. Pursuing nontraditional models for the guard/reserve components of the Cyber Force will be integral to this effort.
- **Develop innovative and agile cyber leaders**. The Cyber Force must develop leaders who grasp the technical and social complexities of cyberspace. These leaders must be able to bridge the gap between cyber forces and the broader military so that the latter understands and appreciates the relevance of cyberspace at operational and strategic levels. While effective leadership is important for all organizations, it is especially critical for the Cyber Force to be able to foster a distinct service culture within the broader military as described further below.
- **Equip cyber forces with the most advanced cyber warfighting capabilities**. The technological ecosystem relevant for cyber operations is continuously evolving. The Cyber Force must become the world leader in the development and employment of effective cyber capabilities, leveraging commercial, experimental, and exquisite technologies for offense, defense, and intelligence across the spectrum of conflict.
- **Establish a service culture attuned to the cyber domain**. Cyberspace is defined by its own unique features, logics, and dynamics, distinct from those of the other warfighting domains. The service will require adaptable organizations and individuals to embrace behaviors, values, norms, and paradigms that reflect and reinforce these attributes.

Core Design Decisions: The Building Blocks of Establishing the Cyber Force

Standing up a new service requires making core design decisions related to organization, personnel, and budget. Suggested approaches to these core decisions are outlined below and subsequently developed further.

What the Cyber Force Will Be

Core Design Decisions About the Cyber Force

Organization within the armed forces

- It will be a separate and independent military service of the armed forces under the Department of the Army.
- It will be responsible for developing joint concepts in cyberspace operations and will drive requirements across doctrine, organization, training, material, leadership and education, personnel, facilities, and policy.

Relationship to Cyber Command and existing services

- Cyber Command will continue to exist as a unified combatant command and be the primary force employer for the cyber domain.
- Existing services will retain some cyber capability for those situations where it directly supports their distinct joint functions.
- Existing services will retain cybersecurity-related capabilities for the establishment, maintenance, and defense of its information technology (IT) and operational technology (OT) infrastructure and defense of its segments of the Department of Defense Information Network.

Personnel and budget

- The Cyber Force will initially draw personnel from across the existing services.
- Only volunteers from their respective services should move over to the Cyber Force.
- There will be common standards for vetting cyber personnel from disparate services who seek to join the Cyber Force.
- The proportion of civilians to uniformed military personnel will be higher than that of the other services.
- The existing budget for DOD cyberspace activities is sufficient to build a new military service.

Organization Within the Armed Forces

The **Cyber Force will be a separate military service of the armed forces**. It will be independent of existing civilian cyber organizations within the federal government that operate under distinct authorities. Title 10 of the U.S. Code defines the unique organization, missions, and roles for the armed forces and the Department of Defense.[19] The Cyber Force will have the responsibilities and authorities for generating cyber forces within the legal framework provided by Title 10. The establishment of a Title 10 military service, however, should not preclude assessing whether the Cyber Force will need a unique blend of authorities, similar to the U.S. Coast Guard model. In addition to Title 10 military authorities, the Coast Guard also possesses Title 32 authorities (homeland security), Title 18 authorities (law enforcement), and Title 50 authorities (intelligence).

Some experts have called for the creation of a stand-alone military department for cyberspace.[20] In practice, the political feasibility, as well as the overhead and administrative costs, are likely too significant in the short- to medium-term. Instead, **the most pragmatic course of action would be to establish the Cyber Force within the Department of the Army**. The Department of the Navy oversees and manages the U.S. Navy and U.S. Marine Corps, and the Department of the Air Force oversees and manages the U.S. Air Force and Space Force. Presently, the Department of the Army oversees and manages only the U.S. Army and therefore has greater bandwidth to oversee an additional service.

19. Armed Forces, 10 U.S.C. (https://uscode.house.gov/browse/prelim@title10&edition=prelim)
20. See: James Stavridis, "The US Military Needs to Create a Cyber Force," *Tufts Fletcher Russia and Eurasia Program*, March 8, 2023. (https://sites.tufts.edu/fletcherrussia/the-us-military-needs-to-create-a-cyber-force); There are currently three military departments: the Departments of the Army, Navy, and Air Force. The current five services each fall under one of these departments.

As part of the armed forces, the Cyber Force will be integrated into the Joint Force and all of its related organizations, processes, and outcomes. The Cyber Force will be the **proponent for (i.e., responsible for) joint concepts for cyberspace operations, which influence how requirements are defined and gaps are identified across doctrine, organization, training material, leadership and education, personnel, facilities, and policy (DOTMLPF-P)**.[21]

Relationship to Cyber Command and Existing Services

Establishing a Cyber Force will bring clarity to the distinction between force generation and force employment in cyberspace. Therefore, the Cyber Force should not subsume Cyber Command's responsibilities, and there should not be a single individual who is dual-hatted as both the commander of Cyber Command and the chief of the Cyber Force. Essentially, both these approaches would result in a single entity that acts as both the force generator and the force employer, blurring that critical line. This is problematic because it runs counter to how the military organizes itself in all other domains. It also raises concerns about civilian oversight, especially in the absence of a White House-appointed and Senate-confirmed civilian service secretary. The Space Force's creation did not prompt Space Command's dissolution. Following the establishment of the Cyber Force, **Cyber Command will continue to exist as a unified combatant command and will continue to be the primary force employer for the cyber domain**. Indeed, Cyber Command will continue to develop the requirements that the service will then fulfill.

The Cyber Force will not be the sole entity responsible for force generation for the cyber domain. Rather, it will be the entity with primary responsibility. **All the other services will retain some responsibility for generating cyber capabilities that directly support their respective service functions**. This is by no means a novel concept. Despite the creation of the Air Force, the Army and Navy continue to retain sizable aviation capabilities that support unique requirements for operations on land (such as close air support or casualty evacuation) and at sea (such as carrier-based aircraft), respectively. So, too, in cyberspace, **each service will also need to retain cybersecurity-related capabilities for the establishment, maintenance, and defense of the IT/OT infrastructure it owns and operates, as well as the defense of its segments of the DODIN.** For example, the Army may need to retain some organic cyber capabilities to support integrated tactical cyber formations (i.e., electronic warfare — EW — which the Army currently considers part of its internal cyber forces) at the brigade combat team level. The other services might be better positioned to provide specific capabilities to Cyber Command and the CMF, especially in areas of expeditionary operations.

Personnel and Budget

The Space Force was largely created entirely out of Air Force assets and personnel. However, cyber personnel and capabilities are currently spread out across five different services. Therefore, **the Cyber Force will initially draw personnel from across all the existing services**. Additionally, the transfer of personnel from the existing services to the Cyber Force should not be compulsory; **only volunteers from their respective services will move over to the Cyber Force**. This would be similar to the voluntary process for transitioning personnel to the Space Force as part of the service's talent management approach to populate the service with only the most capable and motivated personnel.

However, there must be **common standards for vetting cyber personnel from disparate services who seek to join the Cyber Force**. This will be challenging as the Army, Navy, Air Force, Marine Corps, and, most recently, Space Force have defined cyber-specific designations and career paths for various cyber functions

21. Chairman of the Joint Chiefs of Staff, "Guidance for Developing and Implementing Joint Concepts." August 17, 2016. (https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cjcsi_3010_02e.pdf?ver=2018-08-01-134826-593)

and specialties.[22] Cyber personnel from the Coast Guard should also have an opportunity to accede into the Cyber Force. As the services do not all share career designations and initial training requirements, the Cyber Force will need to develop a mechanism to assess competency that takes into account current intra-service disparities. A deeper challenge is how the Cyber Force can inculcate a unique but shared service culture, one that is distinct from the various service cultures in which personnel have been steeped. Developing and executing a common training pipeline for the cyber personnel from the disparate services offers the opportunity to both vet incoming personnel and impart the new cultural values of the Cyber Force. In developing the service's approach to training and education, policymakers should look beyond military programs to consider civilian education, certifications, and training where appropriate. Ensuring that all personnel are trained and held to a shared baseline technical standard further ensures that Cyber Force personnel have a common cultural and technical foundation.

The current proportion of civilian to military personnel within the existing services is skewed toward military personnel.[23] For example, in 2023, civilian employees funded through congressionally appropriated funds comprised 23 percent of the Defense Department's total workforce.[24] Within operational units, such as a brigade combat team or carrier strike force, the civilian workforce percentage approaches zero. For the Cyber Force, however, **the ratio of civilians to uniformed military personnel will be higher**. Relaxing the proportion of military to civilian personnel opens up a range of novel and creative opportunities to structure the Cyber Force — particularly the guard and reserve components — in ways that could draw on the considerable civilian sector talent pool. Many of the tasks associated with cyber operations, such as capability development or even conducting some operations, could just as easily be performed by civilians as uniformed military personnel. This reality is reflected in the fact that civilians comprise approximately 20 percent of the CMF. With the creation of a Cyber Force, this percentage could be even larger.

The initial funding for a new service will be budget neutral. Some detractors have argued that creating a new service will be inefficient and expensive. The authors' previous analysis demonstrated, however, that the Cyber Force would be more efficient and cost-effective because it would reduce the duplicative force generation efforts across the current services. Based on fiscal year 2025 budget requests for the DOD's cyberspace activities budget plus additional relevant budget items (such as some portion of Cyber Command's EBC), a reasonable estimation of the initial budget for the Cyber Force is approximately $17 billion.[25] This is far less than the fiscal year 2025 Space Force budget request, which is $29.4 billion, up from that service's initial budget request of $15.4 billion in fiscal year 2021.[26]

22. For a breakdown of how Cyber Command defined work roles compared with service-specific cyber career field designations and titles, see: Erica Lonergan and retired Rear Adm. Mark Montgomery, "United States Cyber Force: A Defense Imperative," *Foundation for Defense of Democracies*, March 2024, page 18. (https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf); Mark Pomerleau, "After prodding from Congress, Navy creates dedicated cyber work roles amid readiness concerns," *DefenseScoop*, June 28, 2023. (https://defensescoop.com/2023/06/28/after-prodding-from-me-congress-navy-creates-dedicated-cyber-work-roles-to-boost-readiness)
23. For an extensive breakdown of DOD demographics as of 2020, see: U.S. Department of Defense, "2020 Demographics: Profile of the Military Community," November 2021. (https://download.militaryonesource.mil/12038/MOS/Reports/2020-demographics-report.pdf)
24. U.S. Department of Defense, "2023 Demographics: Profile of the Military Community," December 2024, page 5. (https://download.militaryonesource.mil/12038/MOS/Reports/2023-demographics-report.pdf)
25. U.S. Cyber Command, "Fiscal Year 2025 Budget Estimates," March 2024. (https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/CYBERCOM_OP-5.pdf); Erica Lonergan and retired Rear Adm. Mark Montgomery, "United States Cyber Force: A Defense Imperative," *Foundation for Defense of Democracies*, March 2024, pages 29-30. (https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf)
26. U.S. Air Force Financial Management and Comptroller, "Department of the Air Force President's Budget Requests FY25," accessed August 15, 2025. (https://www.saffm.hq.af.mil/FM-Resources/Budget/Air-Force-Presidents-Budget-FY25); U.S. Department of Defense, Press Release, "DOD Releases Fiscal Year 2021 Budget Proposal," February 10, 2025. (https://www.defense.gov/News/Releases/Release/article/2079489/dod-releases-fiscal-year-2021-budget-proposal)

What the Cyber Force Will Not Be

Defining limits and scoping boundaries for any new organization is essential to ensure that it meets the original intent. It is imperative that the new service is not stretched beyond its core objectives in a (misplaced) attempt to remedy the myriad and significant cybersecurity issues that exist across the DOD enterprise, the federal government, and the nation writ large.

What the Cyber Force Is Not

- Responsible for providing cyber forces or personnel for the entire federal government.
- The IT and network service provider for the DOD.
- A replacement for the National Security Agency (NSA) and the Central Security Service (CSS).
- A force provider only for Cyber Command.
- The only service providing forces for Cyber Command.

The Cyber Force will not be the force provider for the entire federal government. It should not be responsible for recruiting, training, and equipping personnel filling cyber work roles in other departments and agencies, such as the Department of Homeland Security or the Federal Bureau of Investigation. Doing so would require building an exponentially larger organization, would be a radically more expensive undertaking, and would demand wholesale change to key statutes. It would also detract from the unique force generation requirements for military cyber operations.

The Cyber Force will not be the IT and network service provider for the DOD enterprise. The DODIN is one of the world's largest and most complex networks, encompassing "over 34 billion IP addresses, more than 3.2 million endpoints, 4 million computers, and 145,000 mobility devices,"[27] according to the Pentagon. Responsibilities for acquisitions of IT equipment and services, operation and maintenance of networks and systems, the protection and defense of those networks and systems, and training for these roles and responsibilities are currently spread across several entities in the DOD, including the Office of the DOD Chief Information Officer, the Defense Information Systems Agency (DISA), the Department of Defense Cyber Defense Command (DCDC), service cyber components, the NSA, and Cyber Command. Consolidating this vast set of responsibilities under the Cyber Force would place an enormous strain on the organization and detract from — and most likely completely overtake — the core mission of generating forces for offensive and defensive cyber missions carried out by Cyber Command and other relevant force employers.

Similarly, **the Cyber Force will not replace the NSA/CSS.** Instead, its creation may be an important complement to, or enabler of, the NSA's cyber missions. As the nation's premier signals intelligence and cryptography agency, the NSA has a unique intelligence mission and responsibility to conduct collection in support of national intelligence priorities and, as a combat support agency, the warfighter. There is overlap between the NSA and Cyber Command that extends beyond the dual-hat leadership structure, including some tools and infrastructure, training/certification, as well as some personnel. An optimized force generation model for cyberspace will offer numerous benefits to the NSA and may potentially create opportunities for support to NSA missions. However, the NSA will continue to have a distinct mission, budget, capabilities, and personnel.

Finally, **the Cyber Force will not be a force provider solely for Cyber Command**. It will also generate forces for other force employers with roles and missions in the cyber domain, such as Special Operations Command, Space Command, and potentially other combatant commands. While Cyber Command is the primary force employer in the cyber domain, it is not the sole force employer. Similarly, **the Cyber Force will not be the sole force provider for Cyber Command**. Other services may be better positioned to provide some cyber-related capabilities to support the operational needs

27. U.S. Department of Defense Cyber Defense Command, "What is the DoDIN and Why is It So Special?" December 9, 2024. (https://www.dcdc.mil/News-Information/Information-Series/InfoSeriesArticles/Article/3989830/what-is-the-dodin-and-why-is-it-so-special)

of Cyber Command. This could include, for example, expeditionary capabilities for forward-deployed tactical operations on the ground to gain close access to adversary information or operational technology or to integrate cyber and electromagnetic spectrum effects.

Defining the Primary Force Generation Responsibilities

The Cyber Force's primary force generation responsibilities follow from its core missions articulated above. These missions shape what capabilities the Cyber Force must provide to the joint force, as well as what capabilities are beyond the scope of its responsibilities. In turn, this delineation sets the foundation for all the other elements of building the service.

Three major functions are directly relevant to capability generation for the cyber domain: **cyber defense, cyber offense, and cyber intelligence.** For each of these, in addition to recruiting, organizing, training, and equipping suitable personnel, the Cyber Force will be responsible for conducting the research and development (R&D) necessary to equip the Cyber Force with the most cutting-edge capabilities. Three additional DOD functions involve cyberspace, but the Cyber Force will not have the primary force generation responsibility: cyber-enabled information operations, DODIN operations, and the development of cyber-related emerging technology.

U.S. Cyber Force will have primary force generation responsibility	U.S. Cyber Force will NOT have primary force generation responsibility
• Cyber defense • Cyber offense • Intelligence as it relates to cyberspace	• Information operations • DODIN operations • Cyber-related emerging technology (e.g., AI/ML and quantum computing)

The Cyber Force should be responsible for generating capabilities for national-level defensive cyber operations and missions. The Cyber Force should, for example, generate forces to support the defense of the enterprise and joint portions of the DODIN against active and ongoing threats. This is distinct from building, operating, securing (e.g., patching, updating, and configuring networks), and maintaining the DODIN, which would be outside of the Cyber Force mission set. The Cyber Force will not be the cybersecurity service provider (CSSP) for the DODIN. However, over the long term, the service could be a force provider to the other services to assist with these cybersecurity functions. The Cyber Force should also generate capabilities that support the defense of national and defense critical infrastructure and key resources and, relatedly, generate capabilities to support Defense Support of Civil Authorities missions, where the military provides support to civilian agencies upon request. The service should also retain capabilities to support and liaise with law enforcement as appropriate and authorized.

The Cyber Force will organize, train, and equip personnel for offensive cyber missions that project power in and through cyberspace, both as an independent function and in concert with or in support of joint force missions and objectives. This includes capabilities to conduct cyber effects operations in support of geographic combatant commanders' (GCCs') operational and contingency plans; capabilities to conduct cyber effects operations that are integrated with other military capabilities to achieve joint objectives; and capabilities for the independent employment of offensive cyber power in competition, crisis, and conflict.

The Cyber Force will generate capabilities to support military intelligence activities as they relate to the conduct of military operations and missions in and through cyberspace. This includes intelligence operations and collection that support operational preparation of the environment for current and future military cyber operations — gaining and maintaining access to targeted networks and systems, moving and maneuvering within networks and systems, and emplacing cyber capabilities. Like all services, the Cyber Force will deconflict these efforts with the intelligence community. Generating such capabilities also includes cyber intelligence and information collection activities that support military cyber operations and missions, as well as cyber intelligence relevant for joint force missions more broadly. Crucially, it

must also include developing capabilities for foundational and scientific and technical (S&T) intelligence relevant to the cyber domain. This encompasses all-source intelligence collection and analysis about adversary cyber capabilities, key leadership, strategy, organizations, vulnerabilities, systems/infrastructure/architecture, and centers of gravity to enable military planning.[28] Additionally, Cyber Force would generate forces in support of CMF work roles that are also resident in the NSA.

The Cyber Force will not be the information warfare/information operations service. The Defense Department defines cyberspace as a warfighting domain; it does not take the same position regarding the "information environment." Many activities occur in the information environment that are wholly outside of cyberspace, such as public affairs or psychological operations. The Cyber Force should play some role in supporting operations in the information environment as part of the joint fight when those operations are directly relevant to cyberspace. For example, the Cyber Force may generate capabilities needed for those aspects of information operations that originate from or traverse the cyber domain.

The Cyber Force will not be responsible for generating capabilities for DODIN operations. The Cyber Force should not generate forces to secure, configure, operate, extend, maintain, or sustain those segments of cyberspace that are owned and operated by the Defense Department, nor should the service ensure the confidentiality, availability, and integrity of the DODIN.[29] This is distinct from the defensive cyber operations and missions described above. However, the Cyber Force should play a role as the executive agent for setting standards to secure the DODIN and make defending it less onerous.

The Cyber Force will not have the primary responsibility for generating capabilities for all of the emerging technologies that relate to cyberspace. The Cyber Force must not be the "AI service." Artificial intelligence/machine learning, quantum computing, encryption, and agile software development may rely on and intersect with cyberspace or may enable cyberspace operations. Therefore, the Cyber Force will have some equities in generating capabilities for these emerging technologies to the extent that they are relevant to its core missions and functions. Generating such capabilities can be a supporting task for other primary tasks, but it should not be the service's primary task.

How to Build the Service

Building on the Cyber Force's vision, mission, and core responsibilities, this section outlines a strategic approach to building the Cyber Force. The subsequent section lays out a more specific implementation plan. There must be a dynamic, iterative process of building, assessing, and reassessing the model for the Cyber Force as the nature of the threat environment changes, innovations in technology occur, and core requirements and best practices evolve. This strategic approach should be taken as a guiding light that provides a set of core values and key principles, rather than a reified blueprint that cannot be modified.

Which Existing Organizations Would Be Subsumed by the Cyber Force?

Detailing Cyber Force's roles and responsibilities offers a blueprint for more specific decisions about which existing organizations should be subsumed by the Cyber Force and which should remain external. It also drives the development of organic military occupational specialties (MOS) and support functions and organizations that the Cyber Force will need to develop. However, this does not presume that all the personnel who currently occupy cyber work roles within existing organizations would automatically become part of the new service.

28. Mark Pomerleau, "DOD renewing focus on foundational cyber intelligence," DefenseScoop, April 12, 2024. (https://defensescoop.com/2024/04/12/dod-renewing-focus-foundational-cyber-intelligence)
29. Department of Defense, Joint Chiefs of Staff, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, Section II-2. (https://irp.fas.org/doddir/dod/jp3_12.pdf)

Existing Organizations' Proposed Relationships to the Cyber Force	
CMF (COF 1) and subordinate command elements (COF 2)	The Cyber Force will assume responsibility for generating the majority of the forces that are responsible for the COF 1 and 2 missions. The existing services may continue to provide certain elements based on the latter's relationship to other service responsibilities, expertise, and domain-specific needs.
CSSPs (COF 3)	Existing services will retain responsibility for their own CSSPs. However, the U.S. Cyber Force may need to provide liaisons, subject matter experts (SMEs), or other integration mechanisms (akin to Air Liaison Officers, Joint Terminal Attack Controllers, and other roles that are focused on coordinating and integrating military actions and effects).
Service Organic Forces	The Cyber Force will not generate forces that are considered organic to existing services (i.e., EW forces in the Army or Navy). However, the Cyber Force may need to provide liaisons, SMEs, or other integration mechanisms to the other services.
CCMD staffs	The Cyber Force will be responsible for filling those billets at the combatant commands (CCMDs) tied to the execution and planning of cyber effects.
SOCOM	The Cyber Force may become responsible for providing personnel to SOCOM based on mission needs and the requirements placed upon the service components.
DISA	The Cyber Force will likely share the responsibility for providing some personnel to DISA, along with the other military services.
NSA	The Cyber Force will likely share the responsibility for providing some personnel, especially personnel in cyber-specific work roles but fulfilling Title 50 purposes.
Service Generating Force	The Cyber Force will assume force generation responsibilities that are currently being performed by the other services, including entities within the existing services that are dedicated to force generation responsibilities for cyberspace, as well as elements of organizations where such responsibilities are part of a larger portfolio. This is especially relevant for training, education, and acquisition responsibilities. Examples include existing cyber schools at the services, portions of the services that generate cyber concepts and doctrine, entities responsible for cyber-related acquisitions and materiel solutions, and others.
Other Dedicated Cyberspace Units	Other organizations dedicated to cyberspace, such as the Army's Cyber Military Intelligence Group (CMIG) or Army Cyber Institute (ACI), etc., will be evaluated on a case-by-case basis.

The current structure of COF contains five operational groups. COF 1, the CMF, includes Cyber Protection Forces, Cyber National Mission Forces (CNMFs), and Cyber Combat Mission Forces. COF 2 includes subordinate command elements, such as CNMF-HQ, DCDC, Joint Force Headquarters-Cyber (JFHQ-Cs), and service cyber component HQs' Cyber Operations-Integrated Planning Elements (CO-IPEs).[30] The DOD's component network operations centers and CSSPs comprise COF 3. Finally, COF 4 and COF 5 include special capability providers and specially designated units, respectively.[31] Beyond the COF, there are additional organizations relevant to cyberspace missions, including Special Operations Command and the NSA. The Pentagon will need to decide how these organizations relate to the Cyber Force. Below, we provide our recommendations to address this issue.

What's In, What's Out from Cyber Command's Perspective

With the Cyber Force's establishment, Cyber Command will be able to refocus on operations against adversaries. This does not necessarily mean that Cyber Command

30. The JFHQ-Cs, for example, conduct cyber operations in support of the geographic combatant commands, and the CO-IPEs help coordinate and deconflict between Cyber Command and the other combatant command staffs.

31. For a more complete definition of these elements, see: U.S. Air Force, "Air Force Doctrine Publication 3-12, Cyberspace Operations," February 1, 2023, pages 13-15. (https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf); Special capability providers are forces that have been organized to conduct offensive cyber operations or defensive cyber operations response actions, and specially designated units are designated by the president or secretary of defense to conduct activities that support DOD cyber operations. The Cyber Force would play a role in generating capabilities for COF 4 and COF 5, but this would depend on the specific nature of their missions and activities.

must relinquish all its current "service-like" authorities. Currently, Cyber Command is contributing to the development of cyber doctrine, conducting training, and curating work roles. These responsibilities will fall under the Cyber Force once it is established, although Cyber Command will likely continue to be responsible for additional training, similar to SOCOM. Existing frameworks and definitions developed by Cyber Command will inform the Cyber Force's efforts — for example, current work roles defined by Cyber Command could inform the development of MOSs.

The Pentagon will have to wrestle with additional questions about how establishing the Cyber Force will affect Cyber Command's roles and responsibilities and relationships with the other CCMDs, such as Cyber Force component commands.

"The new service must focus its initial efforts on recruiting and retaining the right people to perform the mission and providing them with an environment that enables them to develop the required skills and expertise."

Design Principles

The Cyber Force can achieve its vision and mission by creating a force that is flexible and adaptable to the changing technological and threat environment in which it operates. Generating such a force will require an approach centered on recruiting, training, and retaining personnel with deep technical expertise in the cyber domain. The service's culture and leadership should foster a climate conducive to agility, adaptation, creativity, and innovation. To achieve such a highly capable cyber force, the policymakers building it should adhere to a set of core design principles.

Core Design Principles

- *Quality over quantity:* It is essential to recruit and retain the right people to perform the mission.
- *Expertise-based career progression model:* Career progression should follow from demonstrated expertise rather than time in service.
- *Iterative and adaptive force structure:* Force structure should be modeled after the dynamic nature of the domain; capabilities should be tailorable and adaptable by providing organizations composed of smaller, specialized formations.
- *Phased transition:* Standing up the service should take due care to minimize impact to ongoing cyber operations.
- *Organizational leadership and culture:* The service will be successful to the extent that it can foster an organizational culture conducive to the cyber domain; early leadership will be critical to enable and foster this culture.

Quality over quantity: The new service must focus its initial efforts on recruiting and retaining the right people to perform the mission and providing them with an environment that enables them to develop the required skills and expertise. While quantity has a quality of its own, the immediate priority for the Cyber Force should be to focus on the latter while building to the former over the long term. The Cyber Force must optimize recruiting for offensive and defensive cyber operations — the ability to perform the service's core missions — rather than other, less critical attributes, such as physical fitness. The service can also recruit and assess individuals for particular skills or attributes to fill specific MOSs. While technical expertise is critical, other skills and knowledge are also necessary for generating effective cyber forces (e.g., strategists).[32] Cyber space has social and cultural components, so robust cyber expertise encompasses social and cultural expertise — political, psychological, economic, organizational, and so on. The Cyber Force will therefore need structures and processes to manage personnel with such expertise and integrate their diverse skill sets. Additionally, cultivating high-quality talent will require periodic reassessment of personnel, similar to the process for evaluating special operations forces.

32. Col. Gregory Conti, Lt. Col. David Raymond, Maj. Rob Harrison, and Maj. Todd Arnold, "Shaping the Army's Cyber Operations Force: The Human Dimension," *Cyber Defense Review*, February 12, 2015. (https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1135993/shaping-the-armys-cyber-operations-force-the-human-dimension)

As a result of its emphasis on quality over quantity, the service may leave some billets unfilled in the short term to ensure the right individuals are selected for the service in the medium to long term. There must not be a rush to fill 100 percent of the Cyber Force's allocated billets in its first year.

Relatedly, the Cyber Force should take a flexible approach to filling billets with civilian versus uniformed military personnel, with priority given to finding the best person for a particular MOS regardless of whether the individual wears a uniform. However, some roles will be inherently uniformed. Such flexibility is absent from the current team structure in the CMF, where approximately 20 percent of the team structure is allocated for civilian personnel, and there is little room to adjust. Beyond the need for quality, maintaining a sizable portion of the Cyber Force's operational billets available to civilian personnel opens up a viable career path for personnel who want to serve but not in an active-duty capacity, for whatever reason. Creating additional opportunities for civilians will also allow more flexibility in career paths, enabling easier on- or off-ramp options, such as transitioning from civilian to military, active duty to reserve/guard component, or vice versa.

Expertise-based career progression model: The current career progression model across all of the services is based on time-in-service and time-in-grade requirements, with limitations on advancing. Time-in-grade requirements for active-duty officers are defined in Title 10 of the U.S. Code. For example, an Army captain (O-3) must, at the very minimum, serve three years in that grade before being considered for promotion to major (O-4). While some exceptions are possible, they are highly limited and made at the discretion of the service secretary.[33] The existing services are also defined by an "up or out" model — if one is not promoted, one must leave the service.

The Cyber Force should reconceptualize the traditional military career progression model because it is not compatible with the first design principle of prioritizing talent. Instead, the Cyber Force model should draw on a civilian/corporate approach where progression depends on expertise and multifarious experiences rather than time in service and a standardized set of checkboxes. By the same token, the Cyber Force should not adopt an "up or out" model. Few corporations force out skilled employees who do not qualify for (or decline) promotion. The same is true for the civil service model within the federal government, including within the Defense Department. Instead, the Cyber Force should accommodate individuals who cultivate deep technical expertise over the course of a multi-decade career, without necessarily getting promoted to higher ranks or assuming leadership roles. It should also consider decoupling billet from rank, such that a senior officer could fill an otherwise "less senior" position if desired or if it meets service needs, without harming their career progression. The Cyber Force must also be able to recruit individuals from the private sector with the requisite skills to enter the service at a higher level of seniority. Currently, there are direct commissioning programs for cyber officers across the services, but these have not been fully utilized and are not of sufficient scope, scale, and flexibility.[34]

Iterative and adaptable force structure: The dynamic nature of the cyber domain means that operations and tactics need to be rapidly adaptable. In turn, force structure should also be adaptable. The CMF's less adaptable, team-based structure illustrates these challenges. The Pentagon authorized the CMF's creation in 2012 and organized it according to a specific force structure — at the time, 133 teams — into which it has been locked ever since (even as the number of teams

33. Eligibility for consideration for promotion: time-in-grade and other requirements, 10 U.S.C. § 619, as updated through August 2, 2025. (https://www.law.cornell.edu/uscode/text/10/619)
34. "Army Cyber Direct Commissioning Program," *U.S. Army Cyber Command*, June 13, 2025. (https://www.arcyber.army.mil/Resources/Fact Sheets/Article/2060387/army cyber direct commissioning program); "Cyber Direct Commissioning Program," *U.S. Air Force*, accessed August 15, 2025. (https://www.airforce.com/careers/specialty-careers/cyber-direct-commissioning)

has grown slightly).[35] While CMF teams and personnel are organized by task according to changing missions, the number of people per team is static.

Rather than generating capabilities in a set number of predefined teams, the Cyber Force can build a more agile and adaptable force structure by generating smaller, more specialized elements that can combine into teams of various shapes and sizes in accordance with mission needs. Similarly, the force can use this flexible structure to manage readiness and rotate forces without disrupting operational flow while providing highly specialized components to the operational force based on mission requirements. This provides an opportunity to develop mastery within the force while cycling units through the various phases of readiness in the same manner as the existing services. It would also enable a more adaptable manner of structuring the operational force in both offensive and defensive operations.

Phased transition to minimize disruption of ongoing operations: America had the good fortune of creating the Air Force and Space Force when they were not actively engaged in conflict with the nation's adversaries. While the United States is not currently in a state of outright warfare, the nature of competition in cyberspace means that Cyber Command and the CMF are actively engaged daily in operations against peer and near-peer adversaries. Therefore, the Cyber Force's instantiation and assumption of responsibility for ongoing mission sets must be performed with the utmost care to minimize disruptions and mitigate those that arise. A phased transition will require decision-makers to carefully assess the tradeoffs between reducing the chances of operational disruptions and potentially incurring greater costs associated with a longer transition time.

Focus on organizational leadership and culture: The establishment of a Cyber Force is necessary, but not sufficient, to fix the military's readiness challenges. The service also needs to cultivate a distinct organizational culture, enabled and supported by leadership. Each of the existing services is defined by a unique service culture that shapes how it approaches generating forces for warfighting in its respective operational domain.[36] Indeed, tensions between existing service cultures and those cultural attributes that are conducive to generating cyber forces have contributed to the current problem. The Cyber Force will need a distinct culture that reflects the requirements and realities of the cyber domain. Establishing a cyber-relevant culture will enable the Cyber Force to recruit and retain the right personnel, adapt over time to meet complex and evolving requirements, and integrate personnel from across the existing services.

Cyber Force Culture

The Cyber Force should build a culture that emphasizes adaptability, agility, and innovation. It should facilitate and celebrate the "hacker mindset" — "someone who is passionate about technology and enjoys creatively overcoming or circumventing limitations."[37]

Cyber Force culture must match the cyber domain's unique nature, and the new service will need the time, space, and, most importantly, autonomy to foster such a culture. Such a culture should place a premium on technical skill and proficiency to the same degree that tactical proficiency is valued in other domains. The Army's 2014 creation of a new basic branch for cyberspace is illustrative. The mismatches between "hacker" culture and the Army's broader service culture posed an impediment to cultivating a distinct cyber subculture within the Army.[38] Many of the same cultural attributes that the Army's thought leaders attempted to instantiate (with varying degrees of success) in the cyber branch — especially the attempt

35. "Our History," *U.S. Cyber Command*, accessed August 4, 2025). (https://www.cybercom.mil/About/History)
36. Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore: Johns Hopkins University Press, 1989).
37. Lt. Col. Gregory Conti and Lt. Col. Jen Easterly, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," *Small Wars Journal*, July 29, 2010, page 5. (http://www.gregconti.com/publications/482-conti-easterly.pdf)
38. Erica D. Lonergan and Jack Snyder, "Cultural Change in Military Organizations: Hackers and Warriors in the US Army," *Texas National Security Review*, July 1, 2025, pages 74-95. (https://tnsr.org/2025/07/cultural-change-in-military-organizations-hackers-and-warriors-in-the-us-army)

to define a "hacker culture" within the Army — are relevant to creating a Cyber Force service culture.[39]

Some "hacker attributes" dovetail with the Army's broader service culture and will help the Cyber Force fit within the department. For example, the Army's people-centric approach, focus on small teams, mission command concept (where decision-making and mission execution are delegated to lower echelons within accepted boundaries), and inculcation of initiative to solve problems are cultural values compatible with core attributes of hacker culture.[40] In other areas, the Army's culture is antithetical to an effective cyber culture. For instance, hacker culture is fundamentally about finding creative ways to break rules and make systems work in unintended ways. The Army's career progression model and priorities for the promotions process are also in tension with cyber culture. With the Cyber Force being established under the Department of the Army, policymakers will be able to leverage some of the overlaps between Army and hacker culture while allowing the new service to flourish in areas where tensions exist. Yet because the Cyber Force will integrate members from all existing services, it will have a unique opportunity to adapt those attributes from other service cultures that reinforce the values, beliefs, and norms the Cyber Force aims to inculcate.

The goal should be to establish a unique service culture, similar to how the Marine Corps has a distinct culture within the Department of the Navy.[41] To achieve this goal, policymakers will need to carefully select early leaders. The Cyber Force will need a service chief who has credibility within the cyber community — someone with demonstrated, foundational expertise in the cyber domain. That leader will also need to have enduring political support from above and outside of the organization, especially to protect the new service from efforts to force its culture into existing roles. Accordingly, policymakers should take a broad view of potential candidates for key leadership roles.

A Proposed Implementation Plan

This section provides an implementation pathway for policymakers to build the Cyber Force. The most immediate decision should be for the White House and Pentagon to establish a transition team to decide the first critical details of standing up the new service. During Phase I, the transition team should focus on initial planning and setting the conditions to build out the service in Phase II.

Phase I: Planning and Conditions Setting (First 3 Months)

The transition team should consist of representative leaders from each of the existing services, as well as other relevant stakeholders from across the Department of Defense (such as the Office of the Secretary of Defense, the NSA, Cyber Command, and Special Operations Command). External voices and perspectives, including those from academia, the scientific and research communities, and the private sector, will be valuable. Within the overall planning team, designated representatives or sub-teams should focus on each of the core tasks to be addressed in Phase I. As an essential prior step, the planning team should identify and onboard the key leaders, described below, who will guide subsequent efforts.

39. Lt. Col. Gregory Conti and Col. John "Buck" Surdu, "Army, Navy, Air Force, Cyber: Is it Time for a Cyberwarfare Branch of the Military," *Information Assurance Newsletter*, Spring 2009, pages 14-18. (http://www.gregconti.com/publications/2009_IAN_12-1_conti-surdu.pdf); Todd Arnold, Rob Harrison, and Lt. Col. Gregory Conti, "Professionalizing the Army's Cyber Officer Force," *U.S. Army Cyber Center*, November 23, 2013. (http://www.gregconti.com/publications/pro_cyber.pdf)

40. On mission command, see: U.S. Department of the Army, "ADP 6–0: Mission Command, Command and Control of Army Forces," July 2019, pages 1-3. (https://web.archive.org/web/20230610234809/https:/armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34403-ADP_6-0-000-WEB-3.pdf)

41. For instance, while the Marine Corps prioritizes small unit leadership and delegating authority to lower levels, the Navy is hierarchical and is focused on size as measured by number of ships.

The transition team does not need to be composed of equal and proportional representation from each existing service. Instead, the composition should be determined by the knowledge each member brings to the team. These representatives should possess a mix of experience in the CMF and thought leadership on the future of cyber force generation. Establishing the optimal team membership will set the tone for the first and subsequent phases. While many transition team members may subsequently join the Cyber Force, not all will join by default.

Identification of key leaders: At the outset of Phase I, the transition team must identify and onboard key leaders. The first cadre of leadership will have a significant impact on fostering the Cyber Force's initial culture. The transition team should select leaders who already embrace core attributes of the service's desired culture.

Two key positions should be considered "no fail": the first chief of cyber operations (the service's top general or flag officer) and the first commandant of the Cyber Accession, Training, and Education Command (the general or flag officer in charge of recruiting, training, and education). These leaders will need to work closely both with each other and the commander of Cyber Command to get the Cyber Force off the ground and ease the transition from five disparate force providers to a single, unified fighting force. The transition team should strongly consider selecting the first cyber chief from outside of the Army. The team should also consider nontraditional candidates from outside of the current active component force, such as retired general/flag officers, civilian leaders, and current members of the existing guard/reserve components. This would help establish a clear delineation between the Army and the Cyber Force despite both existing within the same department. The following table summarizes this task and the remaining core tasks to initiate in Phase I.

Core Tasks To Initiate in Phase I for Subsequent Build	
Key leader selection	• Identify the first chief of cyber operations • Identify the first commandant for accessions, training, and education
Initial force structure	• Establish a Cyber Operational Forces Command • Consolidate JFHQ-Cs and CO-IPEs • Identify organic support functions to grow in subsequent phases
Personnel: Initial selection, accessions, and personnel transfers; personnel model guidelines	• Identify roles, assessments, and selection process • Prioritize technical proficiency and cultural alignment • Determine education requirements and equivalencies • Begin initial personnel transfers into the service • Define a personnel model
Basing location selection	• Leverage the virtual aspects of the cyber domain • Capitalize on existing footprint in the short term • Explore expanded footprint in the long term to co-locate with key civilian hubs/innovation centers
Key policy updates	• Identify policies that must be modified or created

Key Decisions in Phase I To Set Conditions for Phase II

Key leader selection: The first cyber chief will set the vision for the force and ensure the new service has the resources necessary to be successful. Additionally, as noted, the first cyber chief will face a unique challenge that previous inaugural service chiefs did not face: the new service will be an amalgamation of personnel from every service. The cyber chief will need to embrace all of their available inherited authorities, as well as any authorities granted by the legislation that creates the new service. The chief should leverage these authorities

to cultivate an integrated and coherent new service culture, distinct from existing service cultures.

The commandant will need to execute the cyber chief's vision by assessing initial and future transfers to the service; conducting leveling training and education so the force has a common baseline at appropriate ranks and positions; determining appropriate ranks and qualification levels; and developing an accession model. The commandant will also be responsible for implementing these standards to build the force for the future.

Additional key leaders include the vice chief of cyber operations and the commander of the Cyber Systems Acquisition and Development Command, the top general/flag officer focused on research, development, and acquisitions for the service.

Initial force structure: The Cyber Force will need a starting point for its force structure to assume responsibility for its missions. The transition team will need to organize and stand up a Cyber Operational Forces Command. This command will house teams not assigned directly to Cyber Command or other combatant commands, serving as their home for (re)training and rest and refit. The transition team should also establish intermediate-level commands between the Cyber Operational Forces Command and individual teams (however they are organized going forward), as well as between the Cyber National Mission Force and its teams. These teams must possess operational control (organizing and directing forces to conduct operations) — not just administrative control (control over administrative tasks like training, logistics, and personnel management) — and be properly staffed and equipped to facilitate involvement in operations.

The creation of the Cyber Force will also allow for the consolidation and standardization of the various JFHQ-Cs and CO-IPEs. These can be the starting point for Cyber Force component commands to support the GCCs, which will be the receiver commands for teams from the Cyber Operational Forces Command.

Finally, the service must also grow organic support functions. For example, the Cyber Force will need internal intelligence functions and support while providing support to the other services from a Cyber Intelligence Center (equivalent to the National Ground Intelligence Center and National Air and Space Intelligence Center). Other organic functions include networking and technology support for daily operations, recruiting, lawyers, and strategists. Some of these functions will rely more heavily on civilians than in other services. All of these functions have cyber-specific components that the service must handle internally.

Personnel: Having established organizations, the transition team will then need to identify career pathways and the personnel to fill the organizations. This will require a process to bring in personnel in the immediate term, as well as a process for how to sustain recruitment and retention over time. The team's deliverables should focus on identifying the MOSs that need to be filled, which will determine the initial number of MOSs, which, in turn, will drive how assessments are conducted. The selection process should focus on identifying individuals to build toward teams that can be phased into assuming existing missions in Phase II.

Initial selection, accessions, and transfers: The transition team must develop a deliberate process to assess and select personnel for the Cyber Force. The team should assess prospective personnel for fit, skill sets, cultural acumen, and team composition. Selection should not entail simply moving all current CMF personnel into the new service. Instead, all personnel seeking to transfer to the service will have to apply to join and then pass a selection process. The process should have a component that intentionally accounts for the Cyber Force's desired culture. For example, the Army's early Cyber Branch selections process incorporated questions not only regarding technical proficiency but also understanding of and fluency with hacker culture.

Accessions and selection will be different from past instances of service creation (such as the Air Force or Space Force), where personnel for the new service were

largely drawn from a single parent service. Instead, the Cyber Force will draw personnel from across all five existing services. Therefore, personnel who recently entered the accession pipelines (e.g., in the Reserve Officers' Training Corps [ROTC] or service academies) for their respective services should have the opportunity to accede into the new service without restriction. However, over time, the Cyber Force will cultivate indigenous talent as pipelines mature.

As part of initial personnel transfers, the transition team must determine how to reconcile discrepancies in MOSs and ranks for similar skills and abilities across the existing services. A related consideration is the ranks and skill levels that personnel from the various services will receive upon entry into the Cyber Force. Existing services are not standardized with respect to whether officers (including warrant officers, who rank below commissioned officers but above enlisted personnel and are highly technical and specialized) or enlisted personnel hold various positions. Therefore, the transition team should build temporary exemptions, such as "battlefield commissions," into the selection process. It should also explore options for breveting, where personnel receive temporary opportunities to serve at higher ranks. For example, an Army master sergeant who is a senior interactive on-net operator (ION) should be eligible to transfer into the Cyber Force even if the transition team determines that an officer in the rank of captain (O-3) should fill that role. Going forward, if the career progression model decouples role from rank (even if some roles are coded as requiring a minimal grade level, such as O-4), in the future, an O-6 could fill an O-5 or O-4 role if they have the expertise and desire, without being constrained by an artificial coding of the role. Doing so could also ensure that talent features most prominently in promotion and career progression. Additionally, the standards and requirements for some Cyber Command work roles may translate directly to the Cyber Force. However, the Cyber Force should not assume that all personnel who currently hold such a position are automatically qualified to hold it in the Cyber Force.

Personnel model guidelines: Traditionally, the Army's initial entry training model mandates accessions at the lowest level of skill or rank. New enlisted personnel enter as privates, new officers as second lieutenants. However, accessions into the Cyber Force should include opportunities for various forms of lateral entry. Rather than being an ancillary or one-off aspect of accessions, direct commissions at various ranks and positions should be a core part of the process.[42] An individual who has the skills necessary to serve as a captain or major should be able to enter at that rank. Additionally, the career model for the new service must support development of both broad and deep expertise and institutional knowledge, including on- and off-ramps between the public and private sectors.

After the initial personnel transfer, the service will still need a process to enable interservice transfers over the next several years and possibly beyond. During the first three years of the Cyber Force, personnel from existing services who meet the qualification standards defined by the transition team should be allowed to apply for an interservice transfer with a seamless application process. The losing service should not be able to veto or deny such a transfer. After the initial fill period of three years, the regular interservice considerations and process could be instituted.

Basing location selection: The Cyber Force should embrace the virtual and distributed aspects of cyberspace in considering its basing locations. At least initially, the Cyber Force should be a tenant organization on the various posts, camps, and stations where the forces are developed. Where it makes sense, the new service should leverage the investments of the original parent services, as each has invested resources into expanding facilities at their primary locations near NSA facilities to

42. Direct commissioning programs exist but have struggled to scale and represent more of the exception than the rule, especially at higher echelons. Regarding the March 1 ceremony at Fort Belvoir, Virginia, see: Sgt. Meghan Keller, "91st Cyber Brigade direct commissions veteran as LTC," *Virginia National Guard News*, March 6, 2025. (https://va.ng.mil/News/Article/4113732/91st-cyber-brigade-direct-commissions-veteran-as-ltc)

accommodate their original portions of the CMF. This will provide the Cyber Force with multiple locations for its forces, allowing additional options beyond the two primary locations within each existing service.

Looking ahead, the Cyber Force should explore options for expanding its footprint beyond existing locations, with an emphasis on establishing locations adjacent to civilian hubs for technology and innovation, academia, the defense industrial base, and other Defense Department sites. This would enable the Cyber Force to recruit in proximity to cyber talent and better facilitate public-private collaboration and would be optimized for a more flexible guard/reserve model, described further below. For example, an expanded capacity at NSA Colorado for closer ties with the NSA, Space Command, Northern Command, and the region's growing tech industry would be beneficial. This is similar to the Defense Innovation Unit's regional hub offices in Mountain View, CA, Austin, TX, Chicago, IL, and Boston, MA.[43]

Key policy updates: The transition team should include a policy sub-team responsible for deciding core standards and policies for the Cyber Force. The work of other transition team elements should inform this sub-team's work. Rather than shoehorning the force to fit existing policies, the team should adapt or develop new policies that are optimized to the requirements of the new service.

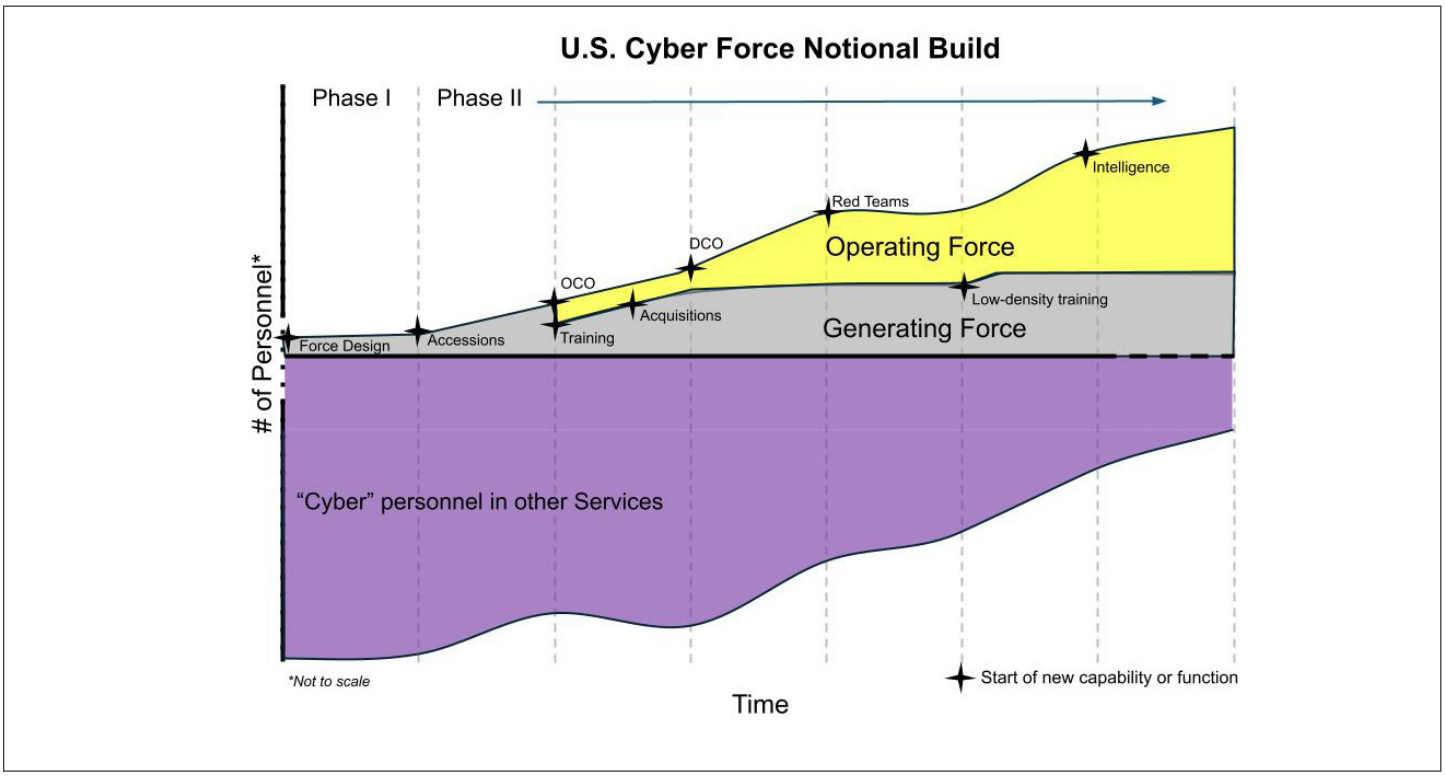
Phase II: Progressive Build (Approximately First 2 Years)

During its first two years, the Cyber Force should incrementally identify the structure, personnel requirements (including training and education), R&D, and methodology required to build both the capabilities required by the Joint Force and the internal functions and capabilities required to generate these joint capabilities. Initially, much of the Cyber Force and its personnel will come from the existing CMF. There will need to be substantial changes to existing concepts and structures to enable the Cyber Force to establish a force generation model that supports operational requirements.

During Phase II, the Cyber Force will need to build a baseline capacity in the generating force that can perform the force design and assess the future force. Once there is sufficient capacity, the focus will shift to the operating forces. Rather than merely transferring operating forces to the generating force (the Cyber Force), the service should generate new organizations tailored to operational and mission requirements. These organizations will gradually replace the ones that the existing services now provide. This will lessen other services' demands for cyber personnel so that the Cyber Force may continue to assess personnel for potential transition into the Cyber Force. During this phase, the transition team will also need to consider decisions related to sustaining the force, such as training, education, and acquisitions (including R&D and capability development) as the service stands up organizations and takes increasing responsibility for force generation functions.

The most important decisions during Phase II will focus on sequencing and phasing the build. The following graphic depicts a notional timeline for building the force. In our proposed timeline, the first key tasks in Phase II are building capabilities to support offensive cyber missions and building the Cyber Force's training and education capabilities. While the transition team will make specific decisions about sequencing and prioritization, the key thrust is that building the Cyber Force should be deliberate and conditions-based, taking into account and mitigating impact to ongoing missions. The build of the generating force, especially the training and education aspects of force generation, will also be critical to developing the service culture.

43. "DIU's New Regional Focus," *Defense Innovation Unit*, November 4, 2021. (https://web.archive.org/web/20211105030334/https://www.diu.mil/latest/dius-new-regional-focus)



Sequencing, phasing, and progressive assessment

Throughout and beyond Phase II, building the force will require continuous assessment and decisions to ensure that it continues to meet the desired intent prior to scaling capabilities. Cyber Force leaders should expect to refine unit structures and force design elements based on lessons learned as they field capabilities to the combatant commands and replace those capabilities being provided by the existing services.

The table below denotes a generalized mapping of the timing of major decisions to the DOTMLPF-P process.

DOTMLPF-P Tasks by Phase	
Doctrine	The starting point will be existing doctrine developed by Cyber Command and the existing services, which will be refined as needed during Phases I-II and beyond
Organization	Initiated in Phase I; refined and expanded in Phase II
Training	Phase II
Materiel	Phase II
Leadership and Education	Leadership decisions occur in Phase I; education decisions take place across Phases I and II, with education criteria for initial selection determined in Phase I and continuing education established in Phase II
Personnel	Initiated in Phase I; refined and expanded in Phase II
Facilities	Phase I
Policy	Phase I

Additional Critical Decisions in Phases I and II

The dynamic nature of cyberspace compels a departure from existing models and norms of force structure. For example, it will be important for the transition team to explore more flexible training regimens, the potential for rotational and on-demand service, resume- and merit-based pathways to promotion, opportunities for specialization, lateral entry, and more fluid transitions (to and from the private sector or other government agencies, or between active-duty and guard/reserve status).

These issues have particular relevance to establishing a guard/reserve component, determining the role of civilians in the Cyber Force, and exploring the benefits of an officer-only model for the service.

"The guard/reserve structure must reduce bureaucratic hurdles to enable reservists and guardsmen to be ready and mobilized in as little as 24 to 72 hours rather than waiting months in accordance with traditional processes."

Defining a guard/reserve component model: The essential roles of the guard/reserve components will include facilitating connections with the private sector and critical infrastructure, academia, as well as the broader cyber talent pool within the United States. To do so, the service must offer new and flexible forms of guard and reserve participation that enable recruitment of the talent with specialized skill sets from across the nation. The Cyber Force will also need to structure its guard/reserve components to generate rapid response capabilities that match the pace of the cyber domain. This is distinct from the current guard/reserve model, where units augment active-duty elements following a traditional mobilization process.

The Unique Importance of a Cyber Guard

The traditional National Guard structure offers a unique blend of authorities, making the Guard essential for domestic response. Typically, the Guard operates under Title 32 authorities under the command of the state's governor, enabling Guard units to conduct missions in support of emergency and disaster response at the state level. However, the Guard can also be federalized and operate under Title 10 authorities under the command of the president during times of war or national emergency. In the current model, there are various state National Guard units across the existing services that can be mobilized to respond to cyber incidents, especially cyber incidents targeting critical infrastructure.[44] However, there is no unified approach, and various guard units organize, train, and equip differently. Creating a Cyber Force would cohere these disparate guard units under one service umbrella and would align organizing, training, and equipping across all of the service's components. Most importantly, given the unique nature of its authorities, a Cyber Guard would be an essential element of critical infrastructure defense at both the state and the national levels.

There are three approaches to guard/reserve service that the Cyber Force should employ in addition to the standard types. One is to create an auxiliary or Volunteer Cyber Corps. This could include technical experts who may not meet the standard drilling requirements but are credentialed, cleared, and ready to respond on short notice. The second encompasses hybrid part-time and consulting roles involving individuals from industry, academia, and other relevant sectors who serve as subject matter experts. They would be pre-cleared, with government-furnished equipment and credentials, and would be able to work remotely or deploy on-site for defined durations. Finally, the Individual Ready Reserve (IRR) could serve as a mechanism to facilitate transitions between the private sector, the civilian service, and the uniformed service. The Cyber Force could allow members of the IRR to apply for open uniformed positions.

The guard/reserve structure must reduce bureaucratic hurdles to enable reservists and guardsmen to be

44. "Guard Units Hone Cyberwarfare Skills," *National Guard Association of the United States*, May 27, 2025. (https://www.ngaus.org/newsroom/guard-units-hone-cyberwarfare-skills)

ready and mobilized in as little as 24 to 72 hours rather than waiting months in accordance with traditional processes. To that end, the Cyber Force should capitalize on the virtual features of the cyber domain itself. Service infrastructure and decentralized locations should allow for virtual, remote, or local muster, enabling a more practical and painless process than traveling to a specific location. Cyber operations often require near immediate action to contain breaches or to support contingency operations and interagency partners. The reserve component should institute ongoing, easily accessible training; pre-positioned security clearances, accesses, and accounts; a streamlined bureaucratic process with minimal administrative steps for activation; and response frameworks that integrate seamlessly with local and state authorities, or other federal agencies.

Role of civilians in the Cyber Force: By incorporating a greater percentage of civilians than other services, the Cyber Force can meet its need for deep and broad technical expertise, as well as institutional knowledge. The NSA's utilization of civilian talent demonstrates the potential of this approach. Having a greater proportion of civilians can also help address the challenge of attracting and retaining talent that might otherwise be lost to rigid participation requirements (especially physical fitness, grooming, and other lifestyle restrictions) or administrative obstacles.

While Title 10 authorities delineate clear roles and responsibilities for uniformed military personnel versus civilians, a wide range of critical roles within the Cyber Force could just as easily be performed by the latter rather than the former. An additional opportunity for synergy would be to have the same individual perform both civilian and military roles, as a good portion of the full-time civilians in the Cyber Force may also have guard/reserve roles.

All-officer model: Another nontraditional force model to consider is for the service to be an all-officer force. This would address systemic problems that our prior research detailed relating to competitive pay and required expertise while ensuring a higher educational baseline for initial entry. During the initial build phases, exceptions should be made for skilled personnel who lack appropriate degrees but nevertheless meet the standards. This model is premised on many of the administrative functions for the service being performed by civilians rather than having enlisted, uniformed personnel fill administrative roles.

Implementing an all-officer model would require a process to select personnel directly from existing commissioning sources, especially West Point given its role as the Army's primary individual commissioning program, as the Cyber Force will fall under the Department of the Army. During the initial build phase, the Cyber Force should be able to accept a number of officers from all service academies. Over the long term, the service will need to define its own commissioning pathways that are independent from those of the existing services.

This approach goes beyond the current Air Force model, which employs an all-officer model for pilots but does not extend this model to other roles. While there is no equivalent officer-only model in the armed forces, there are models in the uniformed services more broadly, specifically the Public Health Services Commissioned Corps and the National Oceanic and Atmospheric Administration Commissioned Officer Corps. The transition team should study these models and identify best practices that would be most relevant for the Cyber Force.

Additional Decisions

This study focused on laying the conceptual groundwork that should inform the establishment of the Cyber Force. As a next step, there are a number of specific, immediate issues enumerated below that the team responsible for the initial standup of the service must tackle. Addressing these in detail is beyond the scope of this analysis, but leaders and decision-makers should examine them closely as the service begins to take shape.

Identify specific individuals for key leadership roles: As previously noted, early leadership will be essential. Therefore, as an immediate task, the team responsible for building the Cyber Force should develop a list of named individuals who would be ideal candidates for the roles of chief of cyber and commandant. The team should cast a wide net in terms of prospective candidates, beyond the current group of uniformed general/flag officers serving in cyber-related roles in the armed forces.

Determine the initial criteria for accessions: The right personnel are at the core of an effective Cyber Force. An immediate first step must be to develop the initial criteria for accessions into the service. This should include a specific plan of action and transition period for current prospective officers across the service academy and ROTC programs.

Define the initial force structure: While the force structure will likely evolve over time as the environment and needs change, it will be imperative to define the initial composition and structure of the subordinate units within the Cyber Force, how the initial cadre of personnel will be allocated to various units, those units' capabilities, and their command-and-control relationships.

Codify the initial foundational vision and mission documents: The Cyber Force's first vision and mission documents will articulate the fundamental purpose of the service and set the stage for cultivating its organizational culture and purpose.

Refine and update existing cyber doctrine: While there is already a starting point for joint and service cyber doctrine, an important task of the Cyber Force will be to revise and update existing doctrinal publications to reflect the creation of the service and to put in motion the promulgation of doctrine that embodies the foundational principles of warfighting in the cyber domain.

Conclusion: The Future of the Cyber Force

It is imperative to establish a Cyber Force to ensure America's military is ready to fight and win in the cyber domain. The current force generation model is fractured across the existing services, with none prioritizing organizing, training, and equipping personnel at scale with the technical skills, competencies, and abilities to fight in the cyber domain. While Cyber Command is attempting to address some of these challenges, ultimately, its ability to induce the services to make the necessary changes is limited. Only a new service — with the primary responsibility for generating forces for the cyber domain — can address the current readiness issues and position the United States for the future of warfare.

The policymakers tasked with building the Cyber Force must design a force generation model that is geared toward the unique demands of the cyber domain. The enduring purpose of the service will be to produce the world's dominant cyber force by developing personnel with domain mastery, equipped with the most advanced cyber capabilities. But how the Cyber Force does so will necessarily evolve over time as technology, threats, and missions change. Therefore, building the service will be an iterative process. Decisions made in the short term will need to be readdressed over the medium- to long-term. This approach allows the planners to make decisions at the appropriate time and refine those decisions with consideration for minimizing operational impacts, risks, and costs.

The success of the Cyber Force over the long term will depend on four factors: leadership, personnel, capabilities, and culture. Building the right transition team, selecting the optimal set of initial key leaders, and prioritizing selecting personnel with the right skill set and domain acumen will together set the conditions for establishing the right culture from the outset to build a capable, effective force.

Acknowledgments

The authors would like to thank the numerous experts who shared their insights and expertise over the many years of research that culminated in the release of "United States Cyber Force: A Defense Imperative" last March and this follow-on monograph exploring how to methodically and strategically create a Cyber Force. In particular, the authors would like to thank Josh Stiefel for his dedication to improving the military's cyber readiness and Ed Cardon, Rob Lee, Colin Ahern, and Frank Smith for providing thoughtful feedback, which strengthened the final product and will inform future research. The input from subject matter experts across diverse fields made this paper stronger, but any errors of fact or judgment remain the authors' alone.

The authors are also indebted to the world-class editing team led by David Adesnik, whose meticulous and inquisitive feedback strengthened the final product. Allie Shisgal's thorough production management ensured the report reached publication, and Daniel Ackerman's creativity and aesthetic mastery enhanced the final product.

Cover Illustration by Daniel Ackerman/FDD

About the Authors

Dr. Erica Lonergan (née Borghard) serves as an adjunct fellow at FDD's Center on Cyber and Technology Innovation and a senior advisor to CSC 2.0, having previously served as a director on the congressionally mandated Cyberspace Solarium Commission. She is also an assistant professor in the School of International and Public Affairs at Columbia University. Previously, Erica held several positions at the United States Military Academy at West Point, including assistant professor in the Department of Social Science and the Department of Electrical Engineering and Computer Science, fellow at the Army Cyber Institute, and executive director of the Rupert H. Johnson Grand Strategy Program.

RADM (Ret.) Mark Montgomery is the senior director of FDD's Center on Cyber and Technology Innovation. He also directs CSC 2.0, having served as the Cyberspace Solarium Commission's executive director. Previously, Mark served as policy director for the Senate Armed Services Committee, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

About the Foundation for Defense of Democracies

The Foundation for Defense of Democracies (FDD) is a Washington, DC-based, nonpartisan policy institute focusing on foreign policy and national security. For more information, please visit www.fdd.org.

FDD's Center on Cyber and Technology Innovation (CCTI)

CCTI seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats and opportunities to national security posed by the rapidly expanding technological environment.

FDD's Center on Military and Political Power (CMPP)

CMPP promotes understanding of the defense strategies, policies, and capabilities necessary to deter and defeat threats to the freedom, security, and prosperity of Americans and our allies, by providing rigorous, timely, and relevant research and analysis.

FDD values diversity of opinion and the independent views of its scholars, fellows, and board members. The views of the authors do not necessarily reflect the views of FDD, its staff, or its advisors.

FDD
FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.fdd.org