

National Academies of Science, Engineering and Medicine
National Academies Study on Cyber Forces Organization

Establishing a Cyber Force: A Defense Imperative

RADM (RET.) MARK MONTGOMERY

Senior Director and Senior Fellow,
FDD's Center on Cyber and
Technology Innovation
Foundation for Defense of Democracies

Washington, DC
November 21, 2025

This is not about CYBERCOM.

That bears repeating — this is NOT about CYBERCOM.

This is about a failed cyber force generation model — with regard to both personnel and equipment.

This stems from the U.S. military's failure to recruit, train, promote, and retain talented cyber warriors.

The Army, Navy, Air Force, and Marines each run their own recruitment, training, and promotion systems - engineered for a service side need — instead of having a single pipeline for cyber talent.

The end result is a shortage of qualified personnel at CYBERCOM, which has responsibility for both the offensive and defensive aspects of military cyber operations.

For the last decade, Congress, on a bipartisan basis, has made clear its sharp concern about cyber personnel issues.

Often, however, military leaders have addressed personnel shortages by massaging statistics or promising iterative changes rather than fixing the underlying problem.

In 2018, CYBERCOM appeared to reach a major milestone when it certified that all 133 of its Cyber Mission Force (CMF) teams had enough properly trained and equipped personnel to execute their missions.

Yet we now know these certifications were hollow: CYBERCOM merely shifted a limited number of effective personnel from team to team to make them appear complete at the time of certification.

Our research paints an alarming picture. The inefficient division of labor between the Army, Navy, Air Force, and Marine Corps prevents the generation of a cyber force ready to carry out its mission.

Recruitment suffers because cyber operations are not a top priority for any of the services, and incentives for new recruits vary wildly.

The services do not coordinate to ensure that trainees acquire a consistent set of skills or that their skills correspond to the roles they will ultimately fulfill at CYBERCOM.

Promotion systems often hold back skilled cyber personnel because the systems were designed to evaluate service members who operate on land, at sea, or in the air, not in cyberspace.

Retention rates for qualified personnel are low because of inconsistent policies, institutional cultures that do not value cyber expertise, and insufficient opportunities for advanced training.

We concluded that resolving these issues requires the creation of new independent armed service — a U.S. Cyber Force — alongside the Army, Navy, Air Force, Marine Corps, and Space Force.

There is ample precedent for this approach: Battlefield evolutions led to the establishment of the Air Force in 1947 and Space Force in 2019.

An independent cyber service would naturally prioritize the creation of a uniform approach to recruitment, training, promotion, and retention of qualified personnel whose skills correspond to CYBERCOM's needs.

In addition to a single, dedicated cyber training and development schoolhouse, an independent service could, without the responsibility for procuring planes, tanks, or ships, also prioritize and possibly excel at — the rapid acquisition of new cyber warfare systems.

This cyber force need not be large. An examination of existing cyber billets suggests it would initially comprise about 15,000 personnel but might grow over time. As the Space Force has shown, a smaller service can be more selective and agile in recruiting skilled personnel.

Some military experts have proposed alternative approaches to addressing the U.S. military's cyber personnel shortage, but each has major shortcomings.

For example, some argue CYBERCOM should become more like U.S. Special Operations Command, to which each service provides elite personnel uniquely trained for the land, sea, and air domains. But that model makes little sense for cyberspace since there are no cyber functions specific to the other warfighting domains.

Others argue CYBERCOM should assume responsibility for manning, training, and equipping cyber forces in addition to employing them on the virtual battlefield. But this approach would break with 40 years of precedent and would overwhelm CYBERCOM's leadership, which is already dual hatted with the National Security Agency, an arrangement that serves U.S. national security well.

America's cyber force-generation system is clearly broken. Fixing it demands nothing less than the establishment of an independent cyber service.

Force Employment versus Force Generation

Cyber Command and the geographic Combatant Commands are responsible for America's *Force Employment*—employing military force in and through cyberspace

- Despite additional resources and authorities, *the readiness of these forces has not sufficiently improved*
- At the same time, America's adversaries continue to grow their cyber capabilities and can conduct increasingly brazen and aggressive cyber-attacks against critical infrastructure

The five military Services—Army, Navy, Air Force, Marine Corps, and Space Force—are largely responsible for *Force Generation* in cyberspace: organizing, training, and equipping cyber forces

- The existing Services prioritize generation for their operational domains; they are *not recruiting, training, maintaining, and retaining the forces we need for cyberspace*

The Desired End State:

The Department produces the world's dominant cyber force, develop innovative and agile cyber leaders, and continually equip the most advanced cyber warfighting capabilities.

Specifically, the Department can generate forces to perform the following missions and functions:

- Defend the nation in cyberspace;
- Deter and defeat aggression in, from, and to the cyber domain;
- Conduct offensive and defensive operations in and through the cyber domain;
- Conduct intelligence, surveillance, reconnaissance, and the targeting of threats in cyberspace;
- Support messaging, strategic communications, information operations, and military deception through cyberspace; and
- Design and develop the tools to fight in cyberspace
- Create and maintain cybersecurity policies, standards, and procedures that guide all DOD cybersecurity activities.

To Achieve this Mission — We Need to Get Four things Right

- 1 - Produce the world's preeminent military cyber *personnel*
 - Recruit in the right places - fully capitalize on the Nation's talent pool
 - This will require looking beyond traditional recruitment pools
 - Non-traditional Guard/Reserve component models are critical
- 2 - Develop innovative and agile cyber *leaders*
 - Leaders must grasp the technical and social complexities of cyberspace
 - Leaders will be essential for bridging the gap between cyber and traditional military components while fostering a distinct service culture
- 3 - Equip cyber forces with the most advanced cyber warfighting *capabilities*
 - 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
- 4 - 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

Core Design Principles for a Cyber Force

- ***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.

What the Cyber Force Will Be: Core Design Decisions

The Cyber Force will be organized **within** the Armed Forces

- A separate, independent Title 10 military service
- Organized under the Department of the Army
- Responsible for developing joint concepts in cyberspace and will drive requirements across doctrine, organization, training, material (cyber tools), personnel, facilities, and policy.

How the Cyber Force relates to **Cyber Command and existing Services**

- Cyber Command will continue to be the primary force ***employer*** for the cyber domain
- Existing services will retain some cyber capability where it directly supports their distinct functions
- Existing services will retain cybersecurity-related capabilities for the maintenance, and defense of their own IT and OT infrastructure and segments of the Department of Defense Information Network.

Personnel and budget Issues

- The Cyber Force will initially draw personnel—on a volunteer basis—from across the existing services
- The proportion of civilians to uniformed military personnel will be **MUCH** higher than that of the other services

- A Cyber National Guard and Reserve element will be aligned to the Cyber Force and organized to support our NCI
- The existing budget for DOD cyberspace activities is sufficient to build a new military service.

I feel I should address the two main Counterarguments

Counterargument 1: The SOCOM model is a better fit for cyberspace than a Cyber Force.

Perhaps the most common counterargument to the creation of a Cyber Force is that CYBERCOM should apply the SOCOM model to cyberspace — notwithstanding SOCOM’s own growing pains over its 30-year history.¹

However, while SOCOM and CYBERCOM both possess highly skilled operators, they are otherwise very different.

In the SOCOM model, each of the services provides the force employer — SOCOM — with expert personnel who possess skills suited to their particular domain. For instance, an Army Ranger trains for special operations on land, while Navy SEALs possess skills tailored to maritime special operations. Rangers and SEALs are not interchangeable. The Army cannot train SEALs, nor the Navy Rangers. Thus, SOCOM actually gains strength from this one-of-a-kind distributed force-generation model.

However, there are no land, sea, or air-specific cyber functions that only particular services can provide. As one U.S. Navy captain noted, SOCOM’s “success is achieved by allowing each of the service-specific commands to specialize in discrete types of warfare, technologies, and operational environments.” By contrast, as a retired Navy captain noted, “Cyberattacks will not be, nor are they currently, service-specific nor sector-specific, so it does not make sense to have created service-specific mission teams, different designators, MOSs, etc. to respond to the broad scale of cyberattacks.”

Counterargument 2: CYBERCOM should absorb many of the man, train, and equip responsibilities from the services.

Rather than creating a Cyber Force, some argue CYBERCOM should evolve to absorb the force-generation responsibilities from the other services. This approach would be tantamount to carving out an exception for cyber-related military matters from the 1986 Goldwater-Nichols Act, the landmark legislation that drew the line between force generation and force employment.

In this scenario, the commander of CYBERCOM would become responsible for military cyber force-generation and force employment, in addition to his or her duties as head of the NSA.

¹ Christopher E. Paul and Michael Schwillie, “The Evolution of Special Operations as a Model for Information Forces,” *National Defense University Press, Joint Force Quarterly 100*, February 10, 2021. (<https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2497069/the-evolution-of-special-operations-as-a-model-for-information-forces/>)

While the dual-hat structure for CYBERCOM and the NSA was initially intended to be temporary, it remains advantageous, as concluded by a December 2022 study led by General (Ret.) Joseph Dunford, former chairman of the Joint Chiefs of Staff.²

The study, however, conceded that simultaneously leading both organizations is a significant amount of work for one individual. Adding what would effectively be a third hat — force-generation responsibilities — would leave the commander less time for the other two, or even force DoD to sever NSA from CYBERCOM.

What Should a Cyber Force Look Like?

Standing up this new service would be challenging but relatively straightforward.

Initially, the Cyber Force would encompass the billets that currently comprise the CMF: a 6,200-person mission group consisting of servicemembers, civilians, and contractors.³ Beyond the CMF, the Cyber Force could also absorb a select number of billets for cyberspace operators that currently fall within the SOCOM enterprise.

In addition, the Cyber Force would require the transfer of support staff billets and infrastructure. The services would likely need to retain some cyber support staff, but a percentage of the cyber-specific force-generation billets from each of the services would transfer to the Cyber Force, particularly those necessary for Cyber Force training institutions. And some Cyber Force recruitment of existing service members would be necessary to fill the remaining gaps in support staff.

This shift, however, should not strain the resources of any one service. In total, the Cyber Force would probably initially comprise approximately 10,000 — 15,000 personnel, although this number would certainly grow over time as cyber threats continue to expand.

The Cyber Force could draw on lessons from the Space Force, which has encountered few issues filling its new roles, even though it requires highly technical and skilled personnel.⁴ At a leadership level, the Space Force's establishment mostly required the lateral transfer of personnel from Air Force Space Command. The Space Force, which currently has around 15,000 billets, attributes much of its recruiting success to being small, agile, and selective with applicants. Its leaders understand they do not need to mimic the larger services. To boost recruitment, the service has also taken advantage of opportunities for direct commissioning of civilians with requisite skills for space.⁵

² Ellen Nakashima and Tim Starks, "NSA, Cyber Command should continue to share a leader, a key review suggests," *The Washington Post*, December 22, 2022. (<https://www.washingtonpost.com/politics/2022/12/22/nsa-cyber-command-should-continue-share-leader-key-review-suggests/>)

³ U.S. Cyber Command Public Affairs, "Cyber 101 - Cyber Mission Force," November 1, 2022. (<https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/>)

⁴ Lauren C. Williams, "Recruiting Crisis? Not at Space Force," *Defense One*, December 2, 2022. (<https://www.defenseone.com/policy/2022/12/recruiting-crisis-not-space-force/380369/>)

⁵ Air Force Recruiting Service, "Constructive Service Credit now offered to applicants for two Space Force career fields," *US Space Force*, October 28, 2022. (<https://www.spaceforce.mil/News/Article/3205270/constructive-service-credit-now-offered-to-applicants-for-two-space-force-career/>)

Most importantly, the creation of a Cyber Force would not require an extensive or complex shuffle of personnel, and the services would retain defensive cyber personnel and IT infrastructure management capabilities for the DoD information networks (DODIN). The creation of a Cyber Force, however, would preclude service-retained personnel from conducting offensive cyberspace operations.

An initial budget for the Cyber Force would be approximately \$16.5 billion, a fraction of the hundred-billion-dollar budgets of the Army, Navy, and Air Force. This estimate includes DoD's current allocation for the cyberspace activities budget (\$13.5 billion), minus the cybersecurity investments from the services (\$511 million). The budget estimate also includes the resources currently carved out for CYBERCOM under EBC (about \$2.9 billion), the military personnel funds (\$624.25 million), and training resources.⁶ An apt comparison is the budget for the Space Force, for which DoD requested \$30 billion for FY 2024.⁷

While the other services may see a slight reduction in their budgets after the creation of a Cyber Force, most of the decrease would come from a reduction in cyber force-generation costs, with a potential for efficiencies from eliminating redundancies.

The Cyber Force would consolidate the acquisitions process specifically for operational capabilities. It should not, however, become the IT and communications service provider for the services, a role that would distract it from operational priorities.⁸

Yet unlike land, sea, air, and space, cyberspace is an interdependent global domain, entirely human-made, and consists largely of privately owned and operated systems. The current reliance on non-cyber lawyers poorly serves U.S. cyber operations.

If done properly, overall readiness of the military's cyber forces should not suffer during a transition to an independent Cyber Force. Instead, cyber forces would gain more operational focus and direction, while consolidating acquisitions processes and maximizing budgetary effectiveness.

⁶ Estimates do not include the cyberspace activities from SOCOM-aligned units/components. U.S. Department of Defense, "Fiscal Year 2024 Budget Estimates United States Cyber Command," March 2023. (https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/CYBERCOM_OP-5.pdf)

⁷ U.S. Department of Defense, "Fiscal Year (FY) 2024 Budget Estimates. Operation and Maintenance, Defense-Wide," March 2023. (https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/OM_Volume1_Part1.pdf)

⁸ On issues of equipment and capabilities, Cyber Force should be responsible only for Deployable Mission Support Systems, a stand-alone cyber technology suite based upon an approved USCYBERCOM hardware/software baseline designed to enable the core CPT functions of hunt, clear, harden, and assess. Commander, Naval Information Forces, Press Release "DMSS on Deck," September 26, 2022. (<https://www.navifor.usff.navy.mil/Press-Room/Press-Releases/Article/3169924/dmss-on-deck/>)

Conclusion

Years after designating cyberspace as a warfighting domain, leaders must acknowledge the writing on the wall.

The scope and scale of cyber threats are growing. Cyberspace plays a central role in China's strategy as the "pacing threat" for the United States.

China has already centralized its cyber capabilities in a single Force. Russia is actively leveraging cyber operations both on the battlefield and to threaten U.S. critical infrastructure and interfere in American politics.

Conventional wisdom holds that the U.S. military is well positioned to dominate in the cyber realm given CYBERCOM's current resources, capabilities, and authorities.

However, recent congressionally mandated studies,⁹ independent analyses and audits, and the accumulated personal accounts from current and retired servicemembers demonstrate otherwise.

Previous attempts to increase U.S. cyber force readiness have failed.

Measures such as the elevation of CYBERCOM to a unified combatant command, the promised expansion of the CMF, and the delivery of EBC do not address major underlying force-generation problems.

U.S. policymakers must acknowledge the difficult reality that the military has tried and failed to salvage the status quo.

This failure stems from the basic fact that non-cyber services are responsible for cyber force generation.

The solution is to create an independent, uniformed Cyber Force.

The United States has a limited window of opportunity to reorganize, allocate resources, and develop sustainable cyber force readiness. The U.S. military has failed to fix the problem on its own. Only Congress can create a new independent service, so it is time for lawmakers to act.

⁹ John Plumb, "Testimony Before House Armed Services Committee," March 30, 2023.
(<https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/Plumb%20Testimony.pdf>)