August 2025

Expert Insights
PERSPECTIVE ON A TIMELY POLICY ISSUE

QUENTIN E. HODGSON, SUSAN M. GATES

Getting the Fundamentals of Cyberspace Force Readiness Right

Calls for a separate military service for cyberspace forces have grown louder in recent years. The Foundation for Defense of Democracies issued a report calling for the establishment of a cyberspace force as part of the Department of the Army, just as both the U.S. Navy and U.S. Marine Corps are part of the Department of the Navy (Lonergan and Montgomery, 2024). A new commission chaired by former commander of the Army Cyber Command LTG Ed Cardon and former House Armed Services Committee staffer Josh Stiefel is examining the implementation requirements for establishing a cyber service (Center for International and Strategic Studies, 2025). Congress has passed numerous National Defense Authorization Act (NDAA) provisions in the past decade that are focused on improving cyberspace force readiness and aligning authorities and organizations to support the same. The NDAA for Fiscal Year (FY) 2025 calls for a new study on the feasibility of establishing a cyber service (DiMolfetta, 2024). Calls for a cyber service stem from a sense of persistent challenges U.S. Cyber Command (USCYBERCOM) and the U.S. Department of Defense (DoD) have faced in trying

to establish and sustain cyberspace forces capable of meeting evolving challenges in the cyber domain, despite having expanded resources and increased attention on developing, training, and presenting ready cyberspace forces.

What is Cyberspace Operations Forces?

The COF consists of "any forces in any DoD Component planning, conducting, or enabling Offensive Cyberspace Operations (OCO); Defensive Cyberspace Operations (DCO); or Department of Defense Information Network (DoDIN) Operations" (Hegseth, 2025). The COF is made up of the following eight groups:

- the Cyber Mission Force
- USCYBERCOM and subordinate headquarters elements
- all cyberspace forces, units, and personnel in any military service, DoD agency, or field activity, in any component (active, National Guard, reserve), in any status (active or ready reserve) and not assigned to USCYBERCOM
- cyberspace assessment elements (e.g., cyber red teams)
- cyberspace supporting action elements (e.g., acquisition, budget organizations)
- Combatant Command Cyberspace Operations Elements
- DoD Intelligence Elements Supporting Cyberspace Operations
- cyberspace forces assigned to U.S. Special Operations Command.

SOURCE: Peter Hegseth, "Department of Defense Cyberspace Operations Forces," memorandum dated July 24, 2025.

In the NDAA for FY 2023 (Section 1533), Congress directed the Secretary of Defense to complete a study on the challenges the military services face in organizing, training, equipping, and presenting the Cyberspace Operations Forces (COF) and alternatives to address those challenges (see box below) (Pub. L. 117-263, 2022). The legislation directed the study to encompass the COF as defined at the time. Subsequent DoD guidance has expanded the definition as noted in the box below. RAND's National Defense Research Institute was asked to conduct the study. The study team conducted more than 130 interviews with more than 230 individuals across the joint and service communities; reviewed relevant literature, policies, and guidance; and analyzed personnel and readiness data. The team also conducted two policy games that involved more than 80 expert stakeholders to explore alternative approaches to cyberspace force generation.

Our study confirmed that DoD leaders face hundreds of challenges in managing the cyber workforce. Although the challenges can be grouped into logical categories, the department cannot effectively improve cyber readiness by attacking the large number of problems one at a time. Our analysis associated the problems with a set of common underlying conditions or root causes that cut across categories of challenges. It is the underlying conditions on which attention needs to be focused when developing solutions. Yet, there is also the question about whether the department is properly organized to identify and implement solutions that address these underlying conditions in a way that can achieve desired results. Therefore, we went further in our analysis and considered alternative approaches to managing the cyber workforce—among them a cyber service—and evaluated these options against a set of criteria.

KEY INSIGHTS

- The U.S. Department of Defense (DoD) faces long-standing challenges in developing and presenting sustainable cyberspace forces, including training and qualifying enough personnel and retaining them in critical roles to providing them with sufficient equipment for training and mission execution. The current approach on its own will not overcome these challenges. Trying harder is not a viable option.
- DoD can and should implement the following foundational initiatives to make progress against these challenges: Manage cyber talent commensurate with workforce needs, standardize development pipelines, align employment expectations and resources with training and certification needs, develop systems to define and track operational effectiveness, and use those systems in resourcing and cyberspace force management decisions.
- DoD could approach these initiatives in any of several ways. Although some both inside and outside DoD advocate for the immediate establishment of a cyber service, implementing these recommended foundational initiatives in the near term under the current approach would lay the groundwork for a longer-term strategic evolution toward a centralized training and career management model or a cyber service.
- U.S. Cyber Command has received new authority, including enhanced budgetary control, that expand its ability to direct and control the resources for training and equipping the Cyber Mission Force (group 1 of the COF). U.S. Cyber Command has not had sufficient time to fully leverage and assess the effectiveness of this new authority in addressing readiness challenges.

Our research highlighted the complex nature of cyberspace force generation and presentation, as well as the trade-offs involved in addressing the root causes of related well-documented and long-standing challenges. Although the focus of much public debate has been on whether to create a cyberspace force in the near term, there are actions DoD can take to address the root causes—many of which do not require the wholesale disruption of creating a new service. In this paper, we examine underlying conditions that are driving the current challenges to cyberspace readiness and analyze initiatives the department can and should undertake to address these drivers, regardless of the path it chooses.

Current Challenges to Cyberspace Readiness

Cyberspace readiness hinges on DoD having the right number of people with the right training, qualifications, and equipment to meet mission needs on an ongoing basis. In 2012, DoD created the Cyber Mission Force (CMF)—COF Group 1, comprising offensive and defensive cyber units—and spent the next six years staffing and equipping the teams and training personnel while conducting operations. ADM Michael S. Rogers, then-commander of USCYBERCOM, acknowledged in 2017 that achieving "full operational capability" was only part of the CMF's goal. He "acknowledge[d] that the true challenge will be sustaining the readiness of the CMF and the remarkable men and women who serve within the teams" (Rogers, 2017, p. 6).

Two years later, the U.S. Government Accountability Office (GAO) concluded in a report that some progress had been made in training and sustaining the CMF. In the report, GAO also noted continued problems with identifying and completing appropriate training, gaining necessary security clearances, and shifting personnel between teams without a loss in readiness (GAO, 2019).

We found similar persistent challenges to developing and sustaining ready cyberspace forces, as well as other challenges, that affected the broader COF and not just the CMF. We grouped the many challenges into the following categories for descriptive purposes:

- **Training.** The training pipelines are fraught with inefficiency: their length, the cost of operating them, DoD's return on investment from training, whether required training is available to those who need it when they need it, and whether it is sufficient (or excessive) for the current operating environment and the missions that cyberspace forces are being asked to support. Interviewees also expressed concerns about access to and the sufficiency of the training infrastructure.
- **Equipment and infrastructure.** Problems with equipment fall into two categories: (1) equipment needs for missions being underresourced and (2) those making resourcing decisions not sufficiently understanding the types of equipment that cyberspace personnel need to accomplish the mission and how equipment needs should be prioritized.
- **Employment.** Employment challenges center on one consistent theme: Cyberspace forces are presented to operational units prior to being fully trained and qualified. Operational units do not have enough capacity to qualify and employ the forces presented, which impedes readiness. Core challenges include a lack of dedicated cyber training units and lack of appropriate infrastructure, missions, and mentors to support on-the-job training.
- **Recruitment and retention.** DoD is unable to attract enough of the right people into cyber positions and retain them long enough to benefit from a training investment. Many factors are thought to affect recruitment and retention, including pay, the way cyberspace needs are (or are not) prioritized within DoD, limited technical career path options for those who prefer to stay with the cyber mission, and dissatisfaction with leadership.

The hundreds of challenges to cyberspace readiness are real problems that prevent DoD from achieving cyberspace readiness.

The hundreds of challenges are real problems that prevent DoD from achieving cyberspace readiness. But because they are numerous and often overlapping, the individual challenges do not provide a strong basis for

developing solutions to COF-readiness shortfalls. Instead, we identified the following six underlying conditions that are found across categories of challenges:

1. **Coordination shortfalls**—lack of coordination within DoD and with other government agencies
2. **Prioritization between cyber and noncyber**—decisionmakers' failure to prioritize the cyber domain, compared with other areas
3. **Prioritization within cyber**—decisionmakers' failure to effectively prioritize activities, work roles, and entities in the cyber domain
4. **Talent management shortfalls**—decisionmakers' failure to recruit and retain cyber employees
5. **What we have does not fit the mission need**—gaps between what the department has and what the mission requires
6. **Disconnect between training infrastructure and employment**—lack of infrastructure and access to infrastructure to sufficiently train employees.

These underlying conditions should be the basis for developing solutions.

Lines of Effort Could Address the Root Causes

Four comprehensive lines of effort have the potential to address the barriers posed by these underlying conditions. We recommend that DoD focus on these efforts rather than on a series of narrow solutions directed at specific challenges.

Implement Talent Management Structures to Better Support COF Readiness

Addressing the complex and interrelated challenges around highly trained and valued personnel serving in critical cyber roles requires a dedicated, focused, DoD-wide talent management effort—something we refer to as a *COF-oriented talent management structure.*

COF-oriented could be defined to include the CMF, subordinate headquarters elements, and other personnel and organizations performing cyberspace functions. It could also be defined more narrowly (especially at initial implementation stages) to focus on the CMF. The 2023 *DoD Cyber Workforce Strategy* notes that DoD has more than 225,000 military, civilian, and contractor personnel involved in cyberspace operations (DoD, 2023). Although the workforce strategy adopts a DoD-wide perspective, its scope is too broad to provide the focused attention to the issues that are most relevant for the highly trained portion of the COF, especially the CMF.

Under the current force presentation model, strategic talent management is largely left to the services. Efforts to address specific COF recruiting, retention, and training challenges require coordination across services. Such efforts also compete with other service priorities.

Several tactical solutions could be considered and executed in the context of comprehensive, DoD-wide, COF-oriented talent management structures. These solutions include increasing and standardizing bonuses, requiring back-to-back tours in critical segments of the COF, changing the force mix to increase reliance on civilians, and better leveraging the reserve component.

Our analysis suggests that the disconnect between the employment model and training pipelines is a root cause of numerous challenges to cyberspace force generation.

Standardize and Improve Personnel Development Pipelines

Existing development pipelines, including training and qualification, were the subject of intense criticism by interviewees. The root causes of these problems are dominated by the need for coordination, prioritization, and a more direct connection between the training infrastructure and employment. A systemwide approach is needed to solve this complicated set of issues.

One option for alleviating shortfalls in the training pipeline would be to consolidate training requirements, development, and delivery. Another would be to consolidate responsibility for establishing the training and certification requirements for designated COF positions into a group of career field managers.

Align Employment Expectations and Resources with Training and Certification Needs

Our analysis suggests that the disconnect between the employment model and training pipelines is a root cause of numerous challenges to cyberspace force generation and is associated with both prioritization considerations and coordination issues.

Possible solutions include establishing dedicated training units, providing funding for mentors or trainers to oversee personnel in the qualification process, increasing the number of or expanding the size of teams to support more-sustainable unit rotations, and adjusting assignment policies so that personnel are not assigned to operational teams until they have achieved basic qualification. Each of these solutions will require additional resources.

Develop Systems to Define and Track Operational Effectiveness and Use Such Systems in Resourcing and Force Management Decisions

We learned that there is no system for tracking actual performance against stated mission needs and revising force management in response. DoD needs to articulate and prioritize both measures of operational effectiveness and systems for follow-up analysis. In the event of shortfalls, these measures and systems can then feed into force management and future resourcing decisions. A better reporting structure would apply uniform methods and metrics to track readiness across services and integrate those into

a common system that can be used to support a mission-based analysis of readiness.

The Big Choices to Achieve Sustainable, Ready Cyberspace Forces

Congress directed DoD to identify and consider the pros and cons of alternative approaches to organizing, training, equipping, and presenting ready cyberspace forces. We distilled many possible methods into three core alternative strategic approaches that could address problems related to coordination, prioritization, talent management, and other underlying conditions. The three approaches are as follows:

- **Current Approach+** is an evolution of the current approach that the department is using, in which each service trains and equips cyberspace forces. A key enhancement over the current approach would be to expand comprehensive training pipelines to encompass all work roles and extend beyond foundational training to qualification activities. This option also increases USCYBERCOM's capacity to review and refine the joint training curricula and increases the capacity of USCYBERCOM subordinate command elements by institutionalizing the billet structure and standardizing the headquarters. Finally, it accounts for the development of additional operational capacity, particularly through presentation of additional CMF teams from the U.S. Coast Guard and the U.S. Space Force as well as the previously approved expansion of the CMF from 133 to 147 teams (Lopez, 2024).
- A **Centralized Training and Career Management Model** would focus on creating an accession and talent management model more like the model used for special operations forces. Personnel would only be assigned to the Cyber National Mission Force (a subunified command under CYBERCOM that counters adversary cyberspace forces) after completing at least one operational tour elsewhere in the COF (preferably, in the CMF) to achieve and demonstrate proficiency. This model would also involve USCYBERCOM establishing a training organization under its direct control that provides advanced cyberspace operations training and education for offensive and defensive cyber operations.
- A **Separate Cyber Service** is the most radical departure from the current approach. It involves establishing a service that is focused exclusively on organizing, training, equipping, and presenting cyberspace forces for employment. A question that comes up routinely in these discussions is "who's in and who's out" for a cyber service. DoD has estimated that its cyberspace workforce of military, civilian, and contractor personnel is approximately 225,000 people (DoD, 2023). This encompasses everyone who maintains, secures, defends, and operates in and through cyberspace, from the offensive pointy end of the spear to the system administrators at a base or installation.

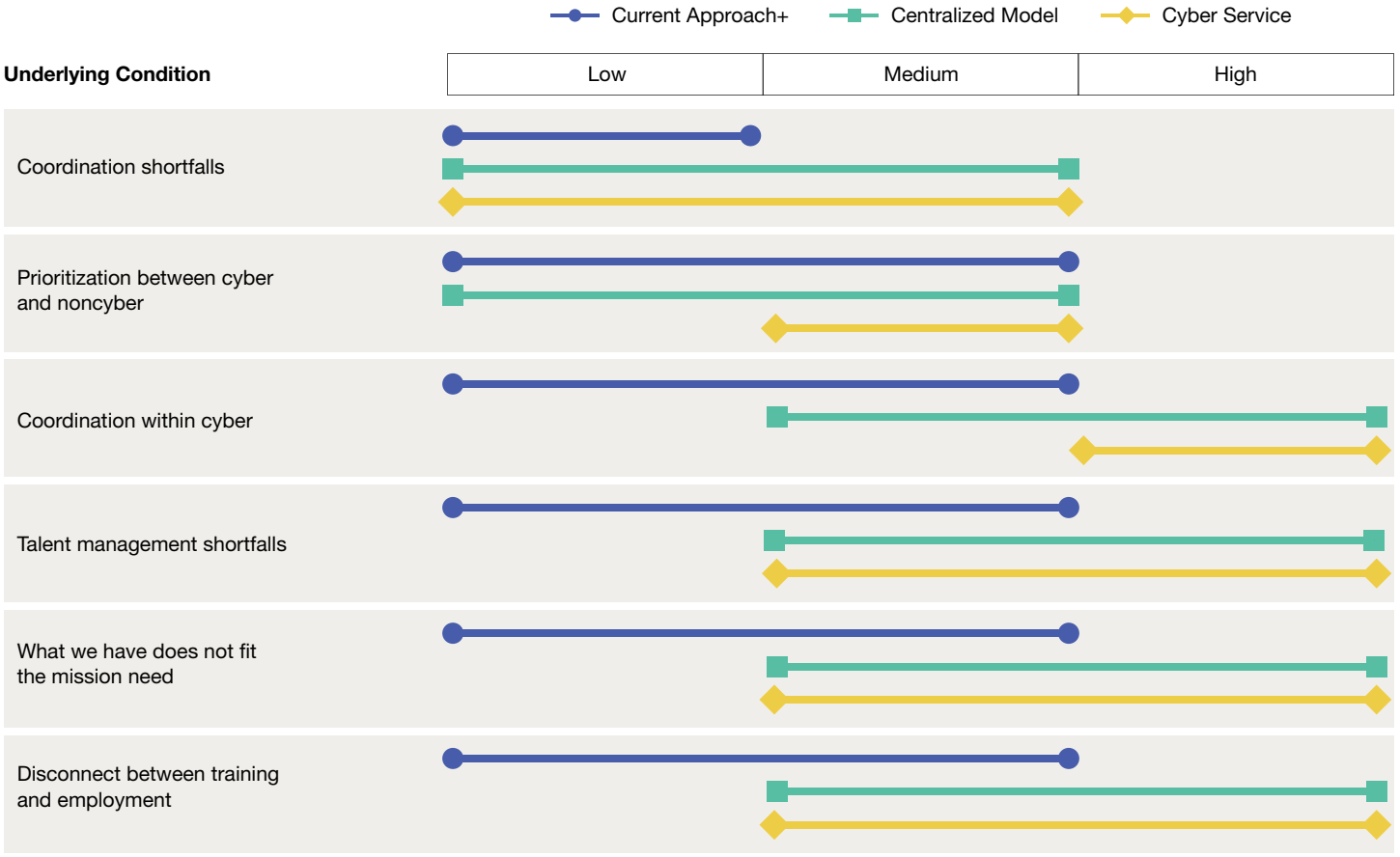
  One could instead focus the cyber service on only the personnel in the CMF—roughly 6,000 but growing with the approved expansion of the CMF—and the direct institutional support required to build and sustain them, which would create a ser-

vice roughly two-thirds the size of the next-largest service, the Space Force. For our purposes, we focus on a smaller cyber service that would consist of the current CMF and associated support structure. This structure would include direct training and equipping for the operational forces, as well as staff to engage in DoD headquarters' processes. However, it would likely have to rely on a parent military department for other such support as recruitment, procurement, or installation support.

We assessed DoD's ability to improve each underlying condition under the three alternative approaches (Figure l).

FIGURE 1

Potential for Each Alternative to Improve Underlying Conditions



In many cases, we give a range of impact because potential outcomes depend on a variety of factors that are not quantifiable or amenable to precise forecasting.

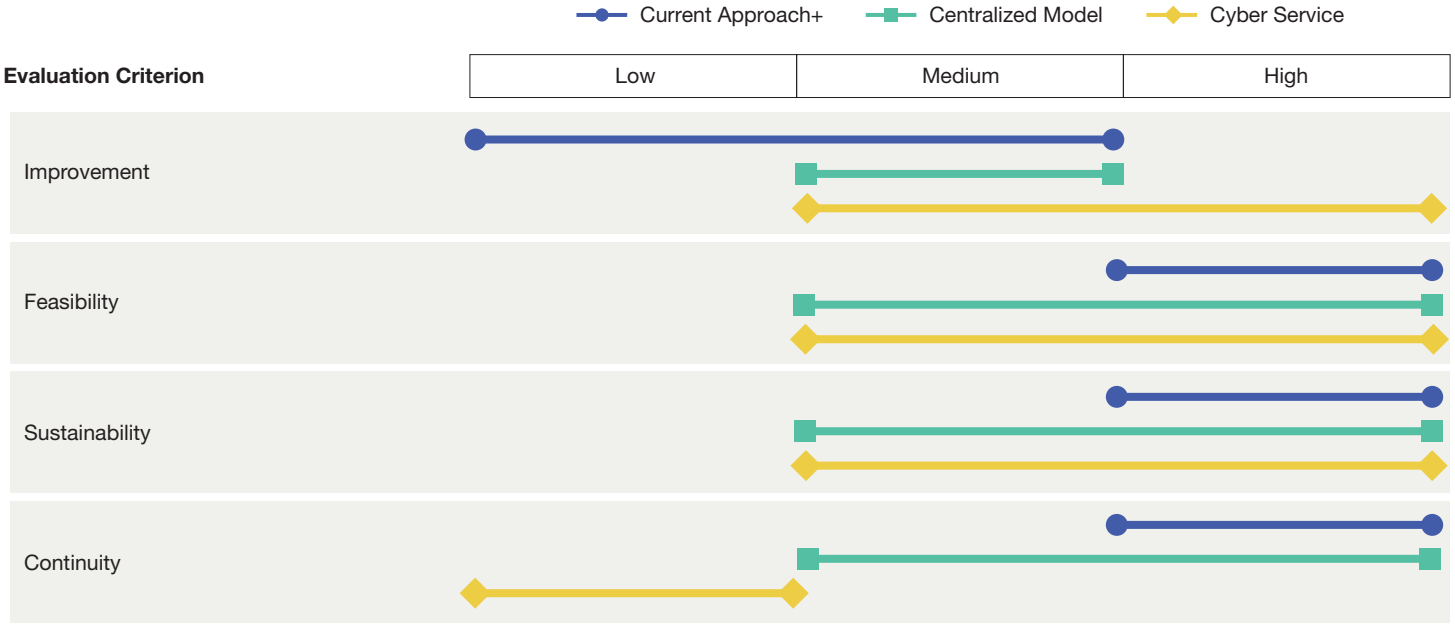
The Current Approach+ appears to have the lowest potential for overall impact on the underlying conditions and the problems associated with them. Both the Centralized Model and a Cyber Service appear to have the potential to address these problem areas more comprehensively. Coordination issues will likely persist (new seams will emerge as old ones are mitigated, for example), but the other areas will likely see more improvement.

For example, a Centralized Training Model or a Cyber Service will likely have a tighter feedback loop from operational forces to better inform the training requirements because the model or the service is wholly dedicated to cyber training. A Cyber Service will naturally have a high impact on prioritization within the cyberspace forces because the service would be focused solely on the cyber domain without competition from noncyber needs. However, that would not protect against overall shifts in prioritization across DoD where cyber needs still compete with department-wide needs.

The evaluation in Figure l is summarized as an overall improvement assessment in Figure 2. Figure 2 shows three other evaluation criteria—feasibility, sustainability, and continuity—in addition to improvement. Each criterion is

FIGURE 2

Potential Impact of Each Alternative Approach on Key Criteria



presented in the context of the ultimate goal—generating ready cyberspace forces in a sustainable manner.

Feasibility addresses the ability to implement the approach given all the actions required. Sustainability addresses the follow-on requirements to sustain focus, attention, and resources to pursue the approach. For example, the Current Approach+ has the advantage of inertia—it is what DoD is already doing, and the services have committed, at some level, to sustaining their efforts.

Continuity addresses both (1) the degree to which the approach would have an impact on DoD's ability to continue fielding and employing cyberspace forces while transitioning to the new approach and (2) the amount of change that must occur within DoD (e.g., shifting resources and establishing new systems and processes). Clearly, the Current Approach+ rates high on continuity because it is merely an expansion on current efforts. A Cyber Service, on the other hand, requires establishing the organization, transitioning personnel to a new service, and shifting resources to that service (away from the other services and potentially also USCYBERCOM), which could prove quite disruptive.

The four evaluation criteria reflect considerations that DoD will have to examine to determine the desired path forward. The evaluation criteria are presented without prioritization. In deliberations, DoD might consider giving equal weight to each of these criteria, or it could decide that some criteria are more important than others. For example, the needs of persistent engagement in cyberspace might argue for emphasizing less disruptive approaches, or the desire to pursue an approach likeliest to achieve substantial improvement could make the risks of disruption (and therefore less continuity) more palatable.

Although the Current Approach+ fares well in feasibility and sustainability, it appears likely to realize the least improvement. The Centralized Model introduces some potential disruption to operations and current training pipelines, so it could reduce continuity, but it offers higher degrees of feasibility and sustainability. Our evaluation is intended as a rubric to inform internal DoD deliberations. DoD will have to decide how to weigh these four factors when arriving at a solution.

The Path Forward

The data collection and analysis that informed this study took place between April 2023 and February 2024. Since the study began, several significant changes have occurred. Most notably, with the passage of the FY 2024 budget, USCYBERCOM has taken on full enhanced budgetary control for the CMF, and the position of the Assistant Secretary of Defense (ASD) for Cyber Policy—who also serves as the principal cyber adviser to the Secretary of Defense—was created and filled (USCYBERCOM, 2024). Like the assistant secretary responsible for special operations, the ASD for Cyber Policy's portfolio is exclusively focused on cyber concerns (rather than on a basket of issues, such as space and missile defense) and comes with authority to ensure the adequacy of the DoD cyber budget. In many respects, the ASD for Cyber Policy exercises "service-like" authority to oversee the organizing, training, and equipping of cyberspace forces (U.S. Code, Title 10, Section 392a).

Our assessment of the current state does not reflect improvements to readiness that might result from these changes. As our discussion of the comprehensive efforts suggests, there are many actions—beyond the changes just

referenced—that can and should be undertaken to develop sustainable, ready cyberspace forces. To start, the suggested efforts to establish a talent management structure and training and certification requirements could focus on the CMF and be undertaken by USCYBERCOM in a way that aligns employment expectations with training and certification needs. Meanwhile, the ASD for Cyber Policy could oversee USCYBERCOM's efforts to develop systems that define and track operational effectiveness, in coordination with its subordinate headquarters elements and their service cyber components, and use those systems to inform the new resourcing decisions.

These efforts could be implemented to some degree in the context of all three of the key strategic approaches to cyberspace force presentation addressed in our study. DoD can make progress on these critical efforts and retain the option of creating a cyber service in the future. Urgent calls for the establishment of a cyber service may distract or delay DoD from the work that must be accomplished, irrespective of which approach is pursued.

Abbreviations

ASD	Assistant Secretary of Defense
CMF	Cyber Mission Force
COF	Cyberspace Operations Forces
DoD	U.S. Department of Defense
FY	fiscal year
GAO	U.S. Government Accountability Office
NDAA	National Defense Authorization Act
USCYBERCOM	U.S. Cyber Command

References

Center for Strategic and International Studies, "CSIS Launches Commission on Cyber Force Generation," press release, August 4, 2025.

DiMolfetta, David, "Congress Approves 2025 NDAA with Important Cyber Provisions," Nextgov/FCW, December 18, 2024.

DoD—*See* U.S. Department of Defense.

Hegseth, Peter, "Department of Defense Cyberspace Operations Forces," memorandum dated July 24, 2025.

GAO—*See* U.S. Government Accountability Office.

Lonergan, Erica, and Mark Montgomery, *United States Cyber Force: A Defense Imperative*, Foundation for Defense of Democracies, March 25, 2024.

Lopez, C. Todd, "Cyber Mission Force Set to Add More Teams," *DOD News*, April 6, 2022.

Public Law 117-263, *National Defense Authorization Act for Fiscal Year 2023*, December 23, 2022.

Rogers, Michael S., "Statement of Admiral Michael S. Rogers Commander United States Cyber Command Before the Senate Committee on Armed Services," U.S. Senate Committee on Armed Services, May 9, 2017.

U.S. Code, Title 10, Section 392a, Principal Cyber Advisor to Secretary of Defense.

USCYBERCOM—*See* U.S. Cyber Command.

U.S. Cyber Command, "Fiscal 2025 Budget Estimates," U.S. Department of Defense, March 2024.

U.S. Department of Defense, "DOD Releases Plan for Implementing Cyber Workforce Strategy," *DOD News*, August 3, 2023.

U.S. Government Accountability Office, *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO-19-362, March 2019.

About This Paper

In response to long-standing challenges experienced by the U.S. Department of Defense (DoD) in developing and presenting sustainable cyberspace forces, Congress directed the Secretary of Defense in the National Defense Authorization Act for Fiscal Year 2023 to complete a study on the challenges the military services face in organizing, training, equipping, and presenting cyberspace operations forces and alternatives to address those challenges (Pub. L. 117-263, 2022). RAND's National Defense Research Institute conducted this study and published a report documenting the research. The researchers analyzed challenges faced by the cyberspace operations forces and evaluated alternatives to force development and the presentation of those forces for operational employment. This paper provides a description of the research, its findings, and discusses their implications for DoD. This paper is based on research completed in October 2024, drawing on data collected and analysis conducted from April 2023 to March 2024.

RAND National Security Research Division

This research was sponsored by the Office of the Secretary of Defense and conducted within the Personnel, Readiness, and Health Program of the RAND National Security Research Division, which operates the National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND Personnel, Readiness, and Health Program, see www.rand.org/nsrd/prh or contact the director (contact information is provided on the webpage).

Acknowledgments

We offer our thanks to the research team Karen Schwindt, Ajay Kochhar, Ryan Bauer, Liam McLane, Karishma Mehta, Jenny Oberholtzer, Phoebe Pham, and Daniel Ibarrola for their indefatigable work collecting and analyzing the data. We thank Christopher Paul for his critique of the main report and this paper, Barbara Bicksler for her help refining this paper, and Libby Sweeney for her careful edit of the final copy.

About the Authors

Quentin Hodgson is a senior international/defense researcher at RAND. His research focuses on artificial intelligence security, cybersecurity, cyber operations, risk management, operational planning, military force structure, and organizational change management. Hodgson has a M.A. in international relations and an M.S. in national resource management.

Susan M. Gates is a senior economist at RAND. Her research applies insights from the economics of organizations, personnel economics, and labor economics to address issues facing public- and private-sector organizations and to promote workforce development, innovation, and entrepreneurship. Gates has a Ph.D. in economics.

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/about/publishing/permissions.

For more information on this publication, visit www.rand.org/t/PEA2761-1.

© 2025 RAND Corporation

www.rand.org

PE-A2761-1