



United States Cyber Force

A Defense Imperative

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

March 2024



United States Cyber Force

A Defense Imperative

Dr. Erica Lonergan

RADM (Ret.) Mark Montgomery

March 2024



FDD PRESS

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

Table of Contents

EXECUTIVE SUMMARY.....	6
HISTORY AND CURRENT ORGANIZATION OF THE U.S. MILITARY IN CYBERSPACE.....	7
IN THEIR OWN WORDS: GAPS AND CHALLENGES IN THE CURRENT MODEL.....	13
COUNTERARGUMENTS TO ESTABLISHING A U.S. CYBER FORCE.....	25
WHAT SHOULD A CYBER FORCE LOOK LIKE?.....	28
CONCLUSION.....	31
APPENDIX A: SELECT QUOTATIONS FROM INTERVIEWS.....	32
APPENDIX B: HISTORICAL CASE STUDIES: THE AIR FORCE AND SPACE FORCE.....	35
APPENDIX C: THE HISTORY OF U.S. INFORMATION OPERATIONS AND THE CREATION OF CYBERCOM.....	37

Executive Summary

In the U.S. military, an officer who had never fired a rifle would never command an infantry unit. Yet officers with no experience behind a keyboard are commanding cyber warfare units. This mismatch 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 instead of having a single pipeline for talent. The result is a shortage of qualified personnel at U.S. Cyber Command (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. In 2022, it required the secretary of defense to deliver a report that addresses “how to correct chronic shortages of proficient personnel in key work roles” at CYBERCOM. The report is due on June 1.¹

Often, however, military leaders have addressed personnel shortages by massaging statistics 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 multiple officers revealed these certifications to be hollow; CYBERCOM merely shifted a limited number of effective personnel from team to team to make them appear complete at the time of certification.

To deepen the understanding of the cyber personnel system and its flaws, this study draws on more than 75 interviews with U.S. military officers, both active-duty and retired, with significant leadership and command experience in the cyber domain.² The study identifies

these officers by rank and service but withholds their names for reasons of privacy.

This 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 servicemembers 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.

Resolving these issues requires the creation of a 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 the 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 establish a cyber war college for advanced research and training, akin to the Army War College and its peers. Without the responsibility for procuring planes, tanks, or ships, a Cyber Force could also prioritize the rapid acquisition of new cyber warfare systems.

1. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 2903, §1533. (<https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf>)

2. FDD made minor edits to some of the interviews for reasons of grammar and style. No substantive changes were made. Appendix A preserves excerpts of the interviews in their original form.



*Illustrated prospective seal for U.S. Cyber Force
(Design by Daniel Ackerman/FDD)*

This Cyber Force need not be large. An examination of existing cyber billets suggests it would initially comprise about 10,000 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 that CYBERCOM should become more like the 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.

History and Current Organization of the U.S. Military in Cyberspace

For nearly 40 years, the U.S. military has separated the responsibility for force generation — the imperative to “man, train, and equip” personnel for their specific domains — from the responsibility of force employment — the use of troops in combat. The independent services — the Army, Navy, Air Force, Marine Corps, and Space Force — generate forces, while the unified combatant commands employ forces and can request manpower from each of the services.

For every domain but cyberspace, the United States has designated a single service as the one ultimately responsible for force generation for its respective domain. For example, while the Army, Navy, and Marine Corps operate significant aircraft fleets, it is primarily the Air Force's responsibility to man, train, and equip U.S. troops for air combat.

Since the establishment of CYBERCOM in 2010 and its subsequent elevation to a unified combatant command in 2018, the military has had a designated organization for force employment in and through cyberspace. But the United States still has no single entity responsible for cyber force generation.

The Creation of CYBERCOM

The pivotal role of advanced technology in the 1991 Gulf War led the Department of Defense (DoD) to recognize the importance of what were then known as “computer network operations.”³ The U.S. military began developing cyber doctrine in earnest in 2003 after the discovery of a multi-year Russian cyber espionage operation revealed the “first large-scale cyberespionage attack by a well-funded and

3. Joshua Rovner, “Warfighting in Cyberspace,” *War on the Rocks*, March 17, 2021. (<https://warontherocks.com/2021/03/warfighting-in-cyberspace>)

well-organized state actor.”⁴ The next year, the Joint Chiefs of Staff defined cyberspace as a warfighting domain,⁵ and DoD released its first National Military Strategy for Cyberspace Operations in 2006.⁶ (A more detailed account can be found in Appendix C.)

After discovering additional foreign cyber espionage campaigns targeting the department, DoD in 2010 combined existing cyber elements to establish CYBERCOM under U.S. Strategic Command. CYBERCOM is led by a commander dual hatted as director of the National Security Agency (NSA), the intelligence community component responsible for signals intelligence and cybersecurity services. CYBERCOM became responsible for defending DoD information systems, supporting joint force commanders in cyberspace, and advancing national interests in and through cyberspace.

The services also developed their own components responsible for information and cyber operations in support of operations in their respective warfighting domains. These components include what are now the 16th Air Force, Army Cyber Command, Fleet Cyber Command, and Marine Corps Forces Cyberspace Command.

In 2018, the president elevated CYBERCOM to a unified combatant command. This move retained the

dual-hatted structure and gave CYBERCOM a direct line of communication to the secretary of defense plus greater authority to request budgetary resources.⁷

“Despite standing up CYBERCOM, the military has not established a cyber-specific training academy.”

Despite standing up CYBERCOM, the military has not established a cyber-specific training academy. In other areas, institutions such as the U.S. Army War College, U.S. Naval War College, Air War College, U.S. Marine Corps University, and National Defense University provide specialized training for senior enlisted personnel and officers, preparing them for leadership positions and assignments in the joint force. This is known as force development.⁸

The 2019 National Security Commission on Artificial Intelligence argued for the creation of a Digital Service Academy to address talent deficits in the defense and intelligence communities.⁹ DoD’s failure to implement this recommendation after three years and multiple congressional initiatives¹⁰ suggests such an academy will not succeed absent an independent service that can deliver the expertise and resources to equip a cyber-specific service academy.

4. Omry Haizler, “The United States’ Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking,” *Cyber, Intelligence, and Security*, January 2017. (<https://www.inss.org.il/wp-content/uploads/2017/03/The-United-States%E2%80%99-Cyber-Warfare-History-Implications-on.pdf>)

5. The Joint Chiefs of Staff, “The National Military Strategy of the United States of America,” 2004. (<https://nssarchive.us/wp-content/uploads/library/nms/nms2004>); Michael Warner, “US Cyber Command’s First Decade,” *Hoover Institution*, December 3, 2020. (https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf)

6. Department of Defense, “National Military Strategy for Cyberspace Operations (NMS-CO),” December 11, 2005. (<https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf>)

7. Andrew Feickert, “The Unified Command Plan and Combatant Commands: Background and Issues for Congress,” *Congressional Research Service*, updated January 3, 2013. (<https://crsreports.congress.gov/product/pdf/R/R42077/11>)

8. U.S. Department of the Army, “Army Regulation 71-32. Force Development and Documentation Consolidated Policies,” March 20, 2019. (https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN8238_AR71_32_FINAL.pdf); “J7 Directorate for Joint Force Development,” *Joint Chiefs of Staff*, accessed January 8, 2024. (<https://www.jcs.mil/Directorates/J7-Joint-Force-Development>)

9. National Security Commission on Artificial Intelligence, “NSCAI Final Report Recommendations,” October 5, 2021. (<https://www.nsc.ai.gov/wp-content/uploads/2021/01/Final-Report-Slides.pdf>)

10. See, for example, “Cyber Service Academy,” *Office of Sen. Kirsten Gillibrand*, accessed January 5, 2024. (<https://www.gillibrand.senate.gov/cyberacademy>)

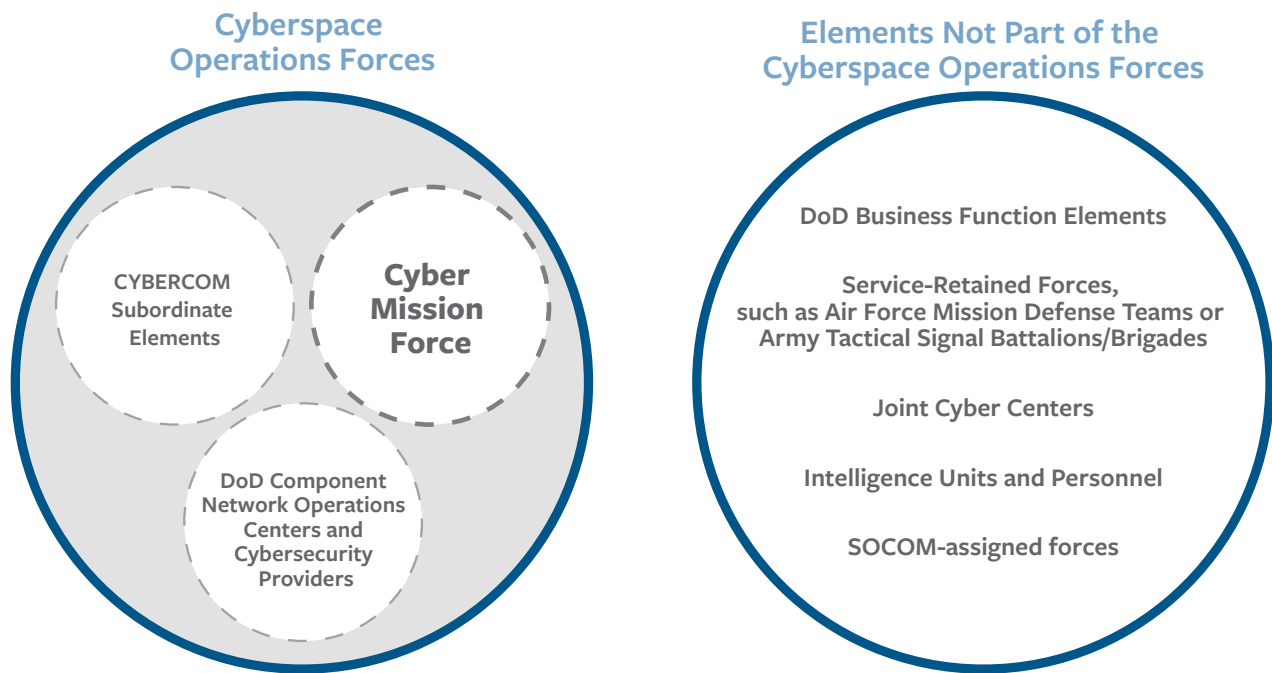
Current Organization of the U.S. Military in Cyberspace

The U.S. military’s Cyberspace Operations Forces (COF)¹¹ encompass elements that conduct reconnaissance, operational preparation of the environment, and network-enabled operations, along with subordinate logistics and administrative elements.¹² In addition, the COF includes DoD network operations centers and cybersecurity service providers that conduct traditional network defense and information technology (IT)

support functions. This latter group makes up the bulk of COF personnel.¹³ Separately, some U.S. military cyber personnel, serving outside the COF, conduct traditional business functions, protect service-specific systems, and support other functional or geographic commands (see Figure 1 below).

Within the COF, the Cyber Mission Force directs, coordinates, and executes cyber operations. It comprises less than 3 percent of the COF, or approximately 6,200 military and civilian personnel.¹⁴ The CMF currently

Figure 1: Cyberspace Operations Forces



11. Joint Chiefs of Staff, “Cyberspace Operations, Joint Publication 3-12,” June 8, 2018. (https://irp.fas.org/doddir/dod/jp3_12.pdf); Note that Joint Publication 3-12 was updated in December 2022, but there is not a public source for the updated doctrine. Department of Defense, “DoD Directive 8140.01: Cyberspace Workforce Management,” October 5, 2020. (<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf>); Department of Defense, “Memorandum for Chief Management Officer of the Department of Defense: Definition of the Department of Defense Cyberspace Operations Forces (DoD COF).” December 12, 2019.

12. U.S. Department of Defense, “Memorandum for Chief Management Officer of the Department of Defense: Definition of the Department of Defense Cyberspace Operations Forces (DoD COF).” December 12, 2019.

13. Joint Force Headquarters DODIN, Fact Sheet, “Protecting DOD Networks for Mission Success,” April 2023. (https://www.jfhq-dodin.mil/Portals/69/PDFs/JFHQ-DODIN%20Fact%20Sheet%20-%20Command%20Overview_April2023.pdf?ver=YhyI-Kbmbllkx7TsTbR4bw%3d%3d)

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

includes 133 teams. But in 2022, DoD announced the CMF would expand to 147 teams, including:¹⁵

- Thirteen Cyber National Mission Force (CNMF) teams responsible for “defend[ing] the nation by seeing adversary activity, blocking attacks, and maneuvering in cyberspace to defeat them.” These operations are largely conducted as independent campaigns, not in support of combatant command missions.
- Twenty-seven Cyber Combat Mission Teams, which “conduct military cyber operations in support of combatant commands.”
- Sixty-eight Cyber Protection Teams responsible for “defend[ing] the DOD information networks, protect[ing] priority missions, and prepar[ing] cyber forces for combat.”
- Twenty-five Cyber Support Teams, which provide analytic and planning support to CNMF and the Cyber Combat Mission Teams.¹⁶
- Fourteen new teams responsible for supporting combatant commanders in space operations and countering cyber influence.

In 2018, CYBERCOM attested that the original 133 CMF teams achieved full operational capacity (FOC). In other words, each team ostensibly had the ability

to fully employ its cyber weapons with adequately trained, equipped, and supported servicemembers.¹⁷ Of those 133 CMF teams, 41 came from the Army, 40 from the Navy, 39 from the Air Force, and 13 from the Marine Corps.¹⁸

In 2022, the CNMF became a sub-unified combatant command, endowing it with additional authorities and responsibilities. Its commander explained that this status will enable CNMF to build “a force that can move faster than our adversaries, because we have the right set of equipment, the right authorities, and the right procedures that move with agility and speed.”¹⁹

The 14 additional CMF teams are supposed to be stood up between fiscal years 2022 and 2026. Five of the new teams are slated to come from the Army, with the Air Force and Navy providing five and four, respectively.²⁰ By mid-2023, however, it became clear that CYBERCOM would need to delay its plans. In particular, the Navy will not be able to deliver new teams for at least a few years because it needs to focus on improving the readiness of its existing cyber personnel.²¹

Moreover, even the existing teams have not actually reached FOC despite what CYBERCOM claims.

15. “Our History,” *U.S. Cyber Command*, accessed January 8, 2024. (<https://www.cybercom.mil/About/History>); U.S. Department of Defense, “Fiscal Year 2024 Defense Budget Overview,” *Office of the Comptroller*, April 2022, page 24. (https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf)

16. Catherine A. Theohary, “Defense Primer: Cyberspace Operations,” *Congressional Research Service*, updated December 9, 2022. (<https://sgp.fas.org/crs/natsec/IF10537.pdf>)

17. U.S. Cyber Command Public Affairs, “Cyber Mission Force achieves Full Operational Capability,” *U.S. Cyber Command*, May 17, 2018. (<https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability>)

18. Mark Pomerleau, “Here’s how DoD organizes its cyber warriors,” *C4ISRNET*, July 25, 2017. (<https://www.c4isrnet.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors>)

19. Cyber National Mission Force Public Affairs, “The Evolution of Cyber: Newest Subordinate Unified Command is Nation’s Joint Cyber Force,” *U.S. Cyber Command*, December 19, 2022. (<https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cyber>)

20. C. Todd Lopez, “Cyber Mission Force Set to Add More Teams,” *DOD News*, April 6, 2022. (<https://www.defense.gov/News/News-Stories/Article/Article/2991699/cyber-mission-force-set-to-add-more-teams>)

21. Martin Matishak, “Cyber Command Reshuffles Force Expansion Due to Navy Readiness Woes,” *The Record*, June 14, 2023. (<https://therecord.media/cyber-command-reshuffles-cyber-mission-force-due-to-navy-readiness-woes>); Mark Pomerleau, “Following reforms, Navy seeing cyber mission force readiness improvements,” *DefenseScoop*, February 22, 2024. (<https://defensescoop.com/2024/02/22/navy-reforms-cyber-mission-force-readiness-improvements>)

Evolution of CYBERCOM's Authorities

While CYBERCOM has had the authority to conduct operations short of armed conflict outside of DoD-controlled networks since its creation,²² the Fiscal Year (FY) 2019 National Defense Authorization Act (NDAA) legislated the most important change in CYBERCOM's authorities, defining cyber operations as a "traditional military activity," and authorized DoD (and, by extension, CYBERCOM) to act in "foreign cyberspace to disrupt, defeat, and deter" cyberattacks against the U.S. government and the American people.²³ This change allowed for more extensive planning and execution of cyber operations. The new authority also largely aligned with National Security Presidential Memorandum-13 (NSPM-13), a Trump administration initiative to streamline the process for authorizing military cyber operations.²⁴ The Biden administration reportedly modified NSPM-13 but has largely kept it in place.²⁵

CYBERCOM has also gained new acquisition authority and statutory responsibility for managing personnel. Previously, the services served as the

executive agents for procurement for CYBERCOM, although CYBERCOM also possessed limited acquisition authority to execute contracts, with a \$75 million annual cap. Then, in the FY 2022 NDAA, Congress took the unusual step of providing CYBERCOM with Enhanced Budgetary Control (EBC) to directly manage resources for equipping the CMF.²⁶ These EBC authorities, which will take full effect this year, reflect congressional frustration with failures in the existing, services-led acquisition efforts on CYBERCOM's behalf. As then CYBERCOM commander General Paul Nakasone explained to Congress in March 2023, the hope is that EBC will better harmonize CYBERCOM's responsibilities and operations by providing it with control over funding for major acquisition programs.²⁷

Nevertheless, the lion's share of cyber funding in the FY 2024 budget remains with the services. CYBERCOM's budget request is approximately \$2.9 billion, while DoD's total Cyberspace Activities Budget request for the services is \$13.5 billion.²⁸ Moreover, CYBERCOM will still rely on the services to spend much of the money that Congress appropriates.²⁹

22. Robert Chesney, "Traditional Military Activities in Cyberspace: Clarifying DOD's Authority and the Line Between T10 and T50 Activities?" *Lawfare*, May 9, 2011. (<https://www.lawfaremedia.org/article/traditional-military-activities-cyberspace-clarifying-dods-authority-and-line-between-t10-and-t50>); Paul C. Ney Jr., "DOD General Counsel Remarks," *Speech before the U.S. Cyber Command Legal Conference*, March 2, 2020. (<https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference>)

23. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232, 132 Stat. 2123 and 132 Stat. 2132, §§ 1632 and 1642. (<https://www.govinfo.gov/app/details/PLAW-115publ232>); Catherine A. Theohary, "Defense Primer: Cyberspace Operations," *Congressional Research Service*, updated December 9, 2022. (<https://sgp.fas.org/crs/natsec/IF10537.pdf>); Robert Chesney, "The Law of Military Cyber Operations and the New NDAA," *Lawfare*, July 26, 2018. (<https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa>)

24. Mark Pomerleau, "What good are 'exceptional' cyber capabilities without authority?" *C4ISRNET*, July 16, 2019. (<https://www.c4isrnet.com/dod/2019/07/16/what-good-are-exceptional-cyber-capabilities-without-authority>)

25. "NSPM-13 and the Future of Cyber Warfare," *The Hudson Institute*, May 5, 2022. (<https://www.hudson.org/events/2109-virtual-event-nspm-13-and-the-future-of-cyber-warfare52022>)

26. Paul M. Nakasone, "2023 Posture Statement of General Paul M. Nakasone," *U.S. Cyber Command*, March 7, 2023. (<https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone>)

27. *Ibid.*

28. U.S. Department of Defense, U.S. Cyber Command, "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)

29. 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)

The promise of EBC was that it would bring CYBERCOM closer to the U.S. Special Operations Command (SOCOM) model, in which the force employer helps guide procurement. However, the services still retain the vast majority of cyber-specific funding, continuing CYBERCOM's dependency on the services. The persistent structural problems render CYBERCOM unable to provide for itself. It continues to rely on the military services and, in some circumstances, the NSA for personnel, funding, foundational intelligence support, procurement and acquisition activities for cyber-specific capabilities, research and development for tools, and infrastructure supporting cyber operations.

Congressional Concerns About CYBERCOM's Insufficient Maturity

Over the past five years, CYBERCOM has achieved important operational successes. It has conducted "hunt forward" operations at the invitation of allied and partner nations to help uncover and defeat cyber threats in their networks.³⁰ It has also defended U.S. elections,³¹ responded to Iranian hackers in Albania,³² and helped Ukraine shore up its cyber systems following Russia's 2022 invasion.³³ However, these successes came despite,

not as a result of, the U.S. military's current organization for cyberspace operations.

Congress has repeatedly raised concerns about these issues. At a March 2023 hearing, Rep. Mike Gallagher (R-WI) noted: "Since 2013, Congress has tried to address force design and readiness through 24 different pieces of legislation. Twenty-four. And over that same period, we have tried to address the civilian and military cyber workforce dilemma 45 times; CYBERCOM acquisition matters, 12 times; and defense industrial base cybersecurity, 42 times."³⁴

Nearly every year for the past decade, Congress has requested information or reports about military cyber readiness — a clear indication DoD has been unable to satisfy congressional concerns. In 2016, Congress mandated that CYBERCOM launch an expedited two-year force-generation effort because the CMF had not achieved sustainable readiness.³⁵ The next year, Congress requested briefings on cyber readiness shortfalls.³⁶ In the FY 2020 NDAA, Congress required the secretary of defense to analyze the benefits and drawbacks of "establishing a cyber force as a separate uniformed service."³⁷ Two years later, Congress again called for an assessment of U.S. cyber posture.³⁸

30. U.S. Cyber Command, Press Release, "Building Resilience: U.S. returns from second defensive Hunt Operation in Lithuania," September 12, 2023. (<https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania>)

31. David Vergun, "Cybercom's Partnership with NSA Helped Secure US Elections, General Says," *DoD News*, March 25, 2021. (<https://www.defense.gov/News/News-Stories/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says>)

32. Cyber National Mission Force Public Affairs, "Committed Partners in Cyberspace: Following cyberattack, US conducts first defensive Hunt Operation in Albania," *U.S. Cyber Command*, March 23, 2023. (<https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens>)

33. David Vergun, "Partnering with Ukraine on Cybersecurity Paid Off, Leaders Say," *DoD News*, December 3, 2022. (<https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say>)

34. Mike Gallagher, "Cyberspace Operations: Conflict in the 21st Century," *Hearing before the House Armed Services Committee, Cyber, Information Technologies, and Innovation Subcommittee*, March 30, 2023. (<https://armedservices.house.gov/hearings/cyber-information-technologies-and-innovation-subcommittee-hearing-cyberspace-operations>)

35. National Defense Authorization Act for Fiscal Year 2017, Pub. L. 114-328, 130 Stat. 2602, §1643. (<https://www.congress.gov/bill/114th-congress/senate-bill/2943/text>)

36. National Defense Authorization Act for Fiscal Year 2018, Pub. L. 115-91, 131 Stat. 1748 §1644. (<https://www.congress.gov/bill/115th-congress/house-bill/2810/text>)

37. National Defense Authorization Act for Fiscal Year 2020, Pub. L. 116-92, 133 Stat. 1748, §1635. (<https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf>)

38. National Defense Authorization Act for Fiscal Year 2022, Pub. L. 117-81, 135 Stat. 2033, §1509. (<https://www.congress.gov/bill/117th-congress/senate-bill/1605/text>)



Subcommittee Chairman Rep. Mike Gallagher (R-WI) (2nd L) listens during a hearing before the Cyber, Information Technology, and Innovation Subcommittee of the House Armed Services Committee on Capitol Hill on March 30, 2023 in Washington, DC. (Photo by Alex Wong/Getty Images)

The FY 2023 NDAA directed the secretary of defense to study the services’ responsibilities for cyber force generation in light of “chronic shortages of proficient personnel in key work roles.”³⁹ Among other issues, the study is supposed to explore whether a single military service should be responsible for force generation.

CYBERCOM implicitly acknowledged its force generation challenges in its May 2023 Strategic Priorities, vowing to improve readiness, recruitment, and retention.⁴⁰ DoD, meanwhile, is developing a so-called “Cyber Command 2.0” initiative to address how the military generates and trains cyber forces.⁴¹ In December 2023, General Nakasone observed that the current state of U.S. military cyber organization is unsustainable. “I think all options are on the table, except the status quo,” he said.⁴²

In Their Own Words: Gaps and Challenges in the Current Model

While force employment is the responsibility of CYBERCOM, responsibility for force generation is spread across the five military services. This system is failing to meet the unique demands of cyber-related training and acquisition. As one general officer lamented, “Our current strategy of relying on the existing Services to build the cyber expertise and capabilities required is inefficient, ineffective, and unlikely to succeed despite years of investment and the best efforts of our servicemembers.” Washington’s “only viable path forward,” the officer said, “is to establish a new Service focused on organizing, training, and equipping forces required to fight – and win – in cyberspace.”⁴³

Manning and training for cyberspace operations are not equivalent to furnishing infantry or logistics personnel. All specialties have distinct training and skill requirements, but the cyber domain requires a uniquely high level of technical training. As a result, individual cyber personnel can have outsized operational effects. As one lieutenant colonel in the Air Force noted, “10% of the [cyber] workforce provides 90% of the value.”

Additionally, acquisition processes for equipment and capabilities must move far more quickly than those for

39. Kristy N. Kamarck and Catherine A. Theohary, “FY2023 NDAA: Cyber Personnel Policies,” updated March 6, 2023. (<https://crsreports.congress.gov/product/pdf/R/R47270>); James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 2903, §1533. (<https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf>)

40. U.S. Cyber Command Public Affairs, “Commander, US Cyber Command rolls out new Strategic Priorities,” *U.S. Cyber Command*, May 18, 2023. (<https://www.cybercom.mil/Media/News/Article/3399867/commander-us-cyber-command-rolls-out-new-strategic-priorities>)

41. Grace Dille, “DoD Fleshing out Cyber Command 2.0 Options,” *MeriTalk*, December 8, 2023. (<https://www.meritalk.com/articles/nakasone-calls-for-a-revamped-cybercom-2-0>)

42. Jaspreet Gill, “With new threats, ‘CYBERCOM 2.0’ must push past ‘status quo’: Nakasone,” *Breaking Defense*, December 8, 2023. (<https://breakingdefense.com/2023/12/with-new-threats-cybercom-2-0-must-push-past-status-quo-nakasone>)

43. All of the personal accounts included in this monograph are excerpted from interviews with active and recently retired servicemembers and Defense Department civilians between December 2022 and January 2024.

the other warfighting domains. Acquisition of software or exploits, for example, must occur rapidly to ensure they are not rendered obsolete.⁴⁴ Moreover, many of the most cutting-edge capabilities reside within the private sector, including in industries not traditionally part of the defense-industrial base. Finally, there is a potentially greater role for non-uniformed civilian personnel in cyberspace capability development and employment.

“At root, the current readiness issue stems from the fact that none of the existing services prioritizes cyberspace.”

The current system compounds these force-generation challenges. Each of the services has developed its own solutions, leading to both inconsistencies and shortcomings. As outlined below, these issues span talent recruitment and retention; occupational designations and training; promotions; critical support functions; administrative control; and capability acquisition.⁴⁵

At root, the current readiness issue stems from the fact that none of the existing services prioritizes cyberspace. As a retired Navy captain observed, this fundamental mismatch “has yielded varying levels of fragmented support to cyber operations, [a] lack of continuity of cyber personnel, unclear career paths, insufficient experience, wide use of non-cyber personnel in cyber leadership positions, and cyber operations being treated always as a supporting entity across all services.”

The extensive interviews that inform this study provide the most direct and compelling evidence to date of the

deficiencies in the U.S. military’s current cyber force generation model and readiness. They also help explain why the establishment of a Cyber Force is the best and only solution to these challenges. (See Appendix A for excerpts from the interviews and a demographic breakdown of the interviewees.)

Recruitment and Retention Shortfalls

The U.S. military is failing to recruit and retain enough talented cyber personnel. The “lack of talented personnel to fill positions on the Cyber Mission Force has been and continues to be a severely limiting factor for the overall force,” one Army colonel explained. A 2022 Government Accountability Office (GAO) report similarly concluded that all the services “continue to experience challenges retaining qualified cyber personnel.” Even the Army, which has fared better in the recruitment of skilled cyber personnel, has struggled to retain its cyber workforce.⁴⁶

The current recruitment and retention shortfall stems from multiple problems, some of them inherent to the current system. First, the services are not using the tools at their disposal to bolster compensation for high-caliber personnel, nor are the services compensating them equitably. In addition, the services have inconsistent and poorly designed requirements governing how long their warfighters must serve. Worse, retention suffers from problems with service culture, leadership, and quality of life. The services’ promotion systems and CYBERCOM’s lack of administrative support also undermine retention, as discussed later in the report.

44. U.S. Department of Defense, “DoD Instruction 5000.87 Operation of the Software Acquisition Pathway,” October 2, 2020. (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF?ver=virAfQj4v_LgN1JxpB_dpA%3D%3D)

45. See also: John Fernandes, Nicolas Starck, Richard Shmel, Charles Suslowicz, and Jan Kallberg, “Assessing the Army’s Cyber Force Structure,” *The US Army War College Quarterly*, August 25, 2022. (<https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3170&context=parameters>)

46. Chad Bates and Charlene Rose, “Understanding-and Fixing-The Army’s Challenge in Keeping Cyber Talent,” *Modern War Institute*, May 17, 2022. (<https://mwi.usma.edu/understanding-and-fixing-the-armys-challenge-in-keeping-cyber-talent>). For its part, the Army still insists it does not have a retention problem because it is able to maintain its target staffing numbers. However, those numbers may be misleading given that, as discussed later, the services are currently unable to ensure they have sufficient staffing for CYBERCOM work roles. Moreover, the issue is not just the sheer number of personnel but their talent. Multiple interviewees decried the challenges of retaining talented personnel. Even if the services retain enough people, they are losing some of their most qualified.

A Cyber Force would be far better equipped to recruit and retain cyber personnel, as the success of the Space Force has shown. Despite competing with private sector firms that offer more attractive salaries, the Space Force has not faced problems recruiting high-level talent.⁴⁷ Because it is relatively small, the Space Force can selectively recruit highly skilled individuals rather than pursuing bulk accessions to fill the ranks like the larger services.⁴⁸

Services Fail to Use Tools at Their Disposal

To be fair to the services, the U.S. military is not the only one struggling to recruit cyber talent. There is a national shortage of cyber personnel, and the federal government struggles to compete with the private sector, which offers much better pay.⁴⁹

Unlike the military, civilian government agencies use creative promotion schemes to ensure their cyber workforce is well-compensated, even if salaries do not match the private sector. The military also has some tools it can use to improve compensation, but the services are not using them effectively. For example, the 2022 GAO study found that the Army was not offering enlistment bonuses to cyber personnel.⁵⁰

As one Army captain explained, CYBERCOM itself “is not able or empowered to use these options.” Meanwhile, “the service components responsible for

manning CYBERCOM refrain from pursuing these choices aggressively because cyber is only one mission and not their primary charge.” A Cyber Force, by contrast, would naturally put cyber first.⁵¹

Inconsistent Compensation

In addition to being inadequate, U.S. military compensation for cyber personnel is inconsistent across the services, damaging morale and esprit de corps.

Once the services recruit personnel, each service separately determines which ranks serve in which jobs. The Marines might assign a staff sergeant (E-6) to the same job the Air Force assigns a first sergeant (E-8). With different pay scales and incentives for these different ranks, the result is wide pay discrepancies between individuals performing identical work. Even when the servicemembers have similar levels of experience, compensation varies significantly. For example, the monthly salaries of two Interactive On-Net Operators (IONs) from different services, each with four to five years of experience, serving in the same location and performing largely the same job, may differ by more than \$700.⁵² This discrepancy does not even take into account differences in housing allowances or pay incentives.

GAO studies have found that enlistment bonuses also vary dramatically across the services. Whereas GAO found in 2022 that the Army was not offering

47. 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>)

48. Leo Shane III, “Space Force eyes easing enlistment rules to target high-demand skills,” *Air Force Times*, September 13, 2022. (<https://www.airforcetimes.com/news/pentagon-congress/2022/09/13/space-force-eyes-easing-enlistment-rules-to-target-high-demand-skills>)

49. Sue Poremba, “The cybersecurity talent shortage: The outlook for 2023,” *Cybersecurity Dive*, January 5, 2023. (<https://www.cybersecuritydive.com/news/cybersecurity-talent-gap-worker-shortage/639724>)

50. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022, page 26. (<https://www.gao.gov/assets/gao-23-105423.pdf>)

51. The Cyber Force could also remove combat fitness test requirements, establish more flexible grooming standards, or recruit neurodiverse individuals for certain work roles. For an example of how other countries are recruiting non-traditional cyber servicemembers, see: Shira Rubin, “The Israeli Army Unit That Recruits Teens With Autism,” *The Atlantic*, January 6, 2016. (<https://www.theatlantic.com/health/archive/2016/01/israeli-army-autism/422850/>); Anna Ahronheim, “IDF aims to recruit 500 soldiers with autism by end of 2022,” *The Jerusalem Post* (Israel), November 8, 2021. (<https://www.jpost.com/israel-news/idf-aims-to-recruit-500-soldiers-with-autism-by-the-end-of-2022-684354>)

52. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022, page 27. (<https://www.gao.gov/assets/gao-23-105423.pdf>)

enlistment bonuses, the Marine Corps was offering \$2,000 for cyber career fields, and the Navy was offering \$5,000 with an additional \$30,000 bonus after training completion.⁵³

The services also use bonuses and incentives inconsistently and without regard for who is a worthy recipient. According to the 2022 GAO study, the services base retention bonuses for cyber personnel on their broader military career, not their unique skill sets.⁵⁴ These findings matched conclusions from a 2017 GAO study.⁵⁵ The persistence of these issues five years after the initial GAO study underscores that the services cannot fix these problems themselves.

Inconsistent and Poorly Designed Length-of-Service Requirements

Low cyber retention rates stem in part from inconsistent and poorly designed length-of-service requirements. Because each service has its own retention policies, they have distinct requirements for how long their servicemembers, including cyber personnel, must remain on active duty. What is more, these requirements do not adequately account for the “lengthy and expensive advanced cyber training” provided to cyber personnel, according to the GAO.⁵⁶

For example, the Army usually requires officers to serve three times the length of their training. However, many advanced cyber training courses are

not included in this Army regulation. As a result, personnel could attend an expensive year-long cyber training course and leave the military soon afterward.⁵⁷ Until legislative intervention in 2023, the Marine Corps could not assign additional service obligations for lengthy and expensive cyber training.⁵⁸

Culture

Many officers have described how service culture denigrates cyber talent, damaging the morale of cyber personnel and eroding retention.⁵⁹ “Retention rates of cyber personnel are abysmal,” one retired Navy captain remarked. “The biggest reason the services hemorrhage talent is that cyber personnel do not feel valued by their service’s culture.” Similarly, a retired Army colonel shared, “I’ve seen senior warfighting leaders dismissively call cyber research ‘book reports,’ cyber operators ‘nerds,’ and cyber capability development ‘science projects.’” Only the creation of a new service dedicated to cyberspace can address these kinds of entrenched cultural challenges.

Inconsistent Career Field Designations, Skill Sets, and Training

Across the services, cyber-related career field assessments, assignments, designations, and skill sets⁶⁰ are ill-defined and disjointed. This fragmented approach undermines training and personnel management.

53. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022, page 26. (<https://www.gao.gov/assets/gao-23-105423.pdf>)

54. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022, page 11. (<https://www.gao.gov/assets/gao-23-105423.pdf>)

55. Government Accountability Office, “Military Compensation: Additional Actions Are Needed to Better Manage Special and Incentive Pay Programs,” February 3, 2017. (<https://www.gao.gov/products/gao-17-39>)

56. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022. (<https://www.gao.gov/assets/gao-23-105423.pdf>)

57. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022, pages 12-13. (<https://www.gao.gov/assets/gao-23-105423.pdf>)

58. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022, page 14. (<https://www.gao.gov/assets/gao-23-105423.pdf>); National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, 137 Stat. 243, §509. (<https://www.congress.gov/bill/118th-congress/house-bill/2670>)

59. Suzanne Smalley, “Cyber Command’s rotation ‘problem’ exacerbates talent shortage amid growing digital threat,” *CyberScoop*, August 18, 2022. (<https://cyberscoop.com/military-rotation-norms-challenge-cyber-command>)

60. While each military service refers to career fields differently, for the purposes of this section, we will refer generically to Military Occupational Specialty (MOS) in reference to both officer and enlisted career fields.

Inconsistent and Inadequate Training

Currently, servicemembers arrive at CYBERCOM with skill sets that are not only inconsistent but also insufficient to fulfill their basic work roles. This problem stems from each of the services not only using different names for their cyber operators but also training them differently — without CYBERCOM’s needs in mind.

For example, when an Air Force cyber operations officer, a Navy cyber warfare engineer, and a Marine Corps cyber operations officer complete their initial entry training, they lack a common skillset (such as knowledge of specific operating systems or exploits). And none are qualified to serve in any of CYBERCOM’s basic work roles upon arrival.

In fact, it was not until February 2023 that the Navy began using a separate designation for its cyber warfare officers, in alignment with how the other services treat their cyber operations experts.⁶¹ While the Army and Air Force generally enable personnel to devote their careers to cyber roles, the Navy had been grouping cyber officers with intelligence and information warfare officers, hampering their ability to develop expertise.

The services train cyber personnel at service-specific training centers. Army centers include the Army Cyber School’s Virtual Training Area, the U.S. Army Cyber Center of Excellence, and Fort Eisenhower Signal Training Site. Air Force personnel train at the Air Force Cybersecurity University and the Cyberspace Technical Center of Excellence. The Navy has the Naval Information Warfare Training Center and the Naval Postgraduate School Center Cybersecurity and Cyber Operations. Finally, there is the Marine Corps Air/Ground Combat Center in California.

These centers do not have a common training system or set of standards. As one Navy captain noted, “Each service has developed their own training model and paths, which do have some overlap but for the most part are not synchronized.” They each have

“different service-desired outcomes and minimal joint perspective when outside of CNMF roles,” the captain explained. “Without one overarching cyber service and related vision and clearly defined mission, cyber training will continue to produce an unbalanced and ineffective joint workforce where services will continue to prioritize efforts and service-specific career paths.”

“Instead of offering specialized training, the services provide general coursework, teach capabilities at a high level of generality, and require operators to learn a broad range of system architectures rather than honing their skills on a specific system.”

A Navy lieutenant commander agreed. “Each of the services are [*sic*] training and employing cyber personnel to do the exact same jobs, such as exploitation analyst, tool developer, and cyber planner,” the officer observed. “Despite these identical needs, there is virtually no standardization whatsoever across the entirety of the military workforce. Each separate service maintains its own training programs, its own performance evaluation processes, its own employment metrics.” In short, “the totality of the force is wholly uncoordinated. From a mission perspective, I have witnessed firsthand how this situation creates impossible problems with regard to technical expertise and training.”

Many other officers discussed the lack of specialization in operating systems, intelligence, exploits, and other techniques associated with cyber-related personnel across the services. Instead of offering specialized training, the services provide general coursework, teach capabilities at a high level of generality, and require operators to learn a broad range of system architectures rather than honing their skills on a specific system. This is like requiring Air Force pilots to learn a bit about all types of aircraft in the fleet rather than specializing in the particular craft they will pilot.

61. Geoff Ziezulewicz, “A new Navy ‘cyber’ rating is in the works,” *Navy Times*, February 15, 2023. (<https://www.navytimes.com/news/your-navy/2023/02/15/a-new-cyber-rating-is-in-the-works>)

Figure 2 contrasts CYBERCOM-defined work roles with service-specific cyber career field designations and titles for both officers and enlisted personnel.⁶² There is little overlap between the two. Furthermore, the service-based training with each military occupational specialty (MOS) does not slot into any particular CYBERCOM work role.

Compared to the other warfighting domains, the U.S. military spends relatively little time and money on training for cyber officers. The initial cost of training an Air Force fighter pilot ranges from \$5.6 to \$10.9 million, and the annual cost of training

for a Naval aviator is \$2.2 million, according to a RAND report.⁶³ By contrast, the GAO found that the training and subsequent certification to become an interactive on-net operator costs between \$220,000 and \$500,000.⁶⁴

The GAO also found that courses are “not listed in regulation or in Army or joint training systems of record.” There are long breaks between courses, and the length of the courses themselves fluctuates. In addition, there are often significant delays between when candidates are nominated for training and when they attend.⁶⁵

Figure 2: Service-Specific Cyber Career Field Designations and CYBERCOM Work Roles

	ARMY	NAVY	AIR FORCE	MARINE CORPS
Military Occupational Specialties (Officer)	Cyber Warfare Officer (17A) ION EA	Cryptologic Warfare Officer (1810)	Cyberspace Effects Operations Officer – Offense (17SXA) D ION	Cyberspace Officer (1702) EA
	Cyber Warfare Technician (170A) ION EA [W-1 to W-5]	Cyberspace Information/Information Professional (1820)	Cyberspace Effects Operations Officer – Defense (17SXB) D ION	Cyberspace Warfare Development Officer (1705) D
	Information Protection Technician (255S)	Cyber Warfare Engineer (1840) D ION EA	Developmental Engineer (62E) D	Offensive Cyberspace Warfare Officer (1710) ION EA
	Cyber Capabilities Development (17D) D	Cyber Warrant Officer (7840): ION		Defensive Cyberspace Warfare Officer (1720)
	Cyber Capabilities Developer Technician (170D) D	Maritime Cyber Warfare Officer (1880) ION		
Military Occupational Specialties (Enlisted)	Cyber Operations Specialist (17C) ION EA	Information Systems Technician (IT)	Software Dev Ops (1D71Z/P) D	Cyber Defensive Operator (1721) ION EA
	Cyber Network Defender (25D)	Cyber Warfare Technician (CWT) D ION EA	Cyber Intelligence Analyst (1N4X1A)	Cyberspace Operations Chief (1799)
			Systems Operations (1D7XXB)	
			Cyberwarfare Operations (1B4X1) D ION	
			Network Intelligence Analyst (1N4) EA	
		All Source Intelligence (1N0)		

D = Developer | **ION** = Interactive On-Net Operator | **EA** = Exploitation Analyst

Source: Adapted from the Government Accountability Office with additional research and input from interviewed experts (<https://www.gao.gov/assets/gao-23-105423.pdf> page 8).

62. Government Accountability Office, “Federal Workforce: OPM Advances Efforts to Close Government-wide Skills Gaps but Needs a Plan to Improve Its Own Capacity,” February 27, 2023, pages 18-22. (<https://www.gao.gov/products/gao-23-105528>)
 63. For more information, see also: Michael G. Mattock, Beth J. Asch, James Hosek, and Michael Boito, “The Relative Cost-Effectiveness of Retaining Versus Accessing Air Force Pilots,” RAND Corporation, March 27, 2019. (https://www.rand.org/pubs/research_reports/RR2415.html)
 64. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022, page 12. (<https://www.gao.gov/assets/gao-23-105423.pdf>)
 65. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022, page 14. (<https://www.gao.gov/assets/gao-23-105423.pdf>)

Across the services, there is also a lack of continual training for the officer corps. An April 2023 paper published by the National Defense University concluded that the cyber domain requires continual training with some technical training delivered every 18 to 24 months.⁶⁶ Although servicemembers often have the opportunity to attend graduate school, such courses are also not well suited to technical training for a dynamic, rapidly changing field. Such courses are also different from the more specialized cyber upskilling needed to create effective leaders.

Inability to Manage Cyber Personnel

Because the services do not designate personnel for particular CYBERCOM work roles, “military service officials cannot determine if specific work roles are experiencing staffing gaps,” the GAO concluded. Put simply, the services do not know if they have “the right personnel to carry out key missions.”⁶⁷

Likewise, there is no system or method to track individuals with cyber skills as they transition to and from the services and CYBERCOM. This means a servicemember may enter with initial training for a cyber-related career field but could be moved to a non-cyber career track during one of these transitions. Such reassignments stem from the reality that the services understandably prioritize their unique needs and missions, which may not allow for individual personnel to stay on a cyber-specific track for the duration of their career.⁶⁸

Promotion Processes Do Not Reward Technical Competence

The services determine promotions for their cyber personnel, but they use systems designed for the non-cyber world. These systems reward command experience — usually in non-cyber fields — over technical competence. As a result, the services are

replete with commissioned and non-commissioned officers who may be good leaders but lack the cyber-specific skills and experience necessary to excel.

Standard service processes require an individual to have held certain positions to be promoted. These roles are often entirely unrelated to CYBERCOM priorities. In the Army, for example, a lieutenant must serve as a platoon leader before being promoted. But many technically proficient cyber operators never hold the positions deemed necessary for advancement. Consequently, they are passed over for promotion, while those without cyber expertise are placed in command.

Compounding this issue, the personnel in charge of the promotion process within each service typically lack the requisite cyber knowledge to make effective promotion decisions. A U.S. Army colonel noted that the individuals on service promotion boards struggle to differentiate between “officers with advanced, skilled degrees in computer science from esteemed institutions” and “those who received online degrees in information management. ... This is akin to equating a brain surgeon with a field medic.”

It does not have to work this way. The Space Force provides an illustration. As a first lieutenant in the Air Force explained, the “Space Force gives the best-qualified commanders the best-qualified experts (long-time members who have reached the major, lieutenant colonel, or warrant officer levels), and those experts retain the ability to work a technical role while still benefiting from career progression.” By contrast, the current promotion system for cyber “robs all highly technical career fields of their most qualified experts, as our antiquated career progression system demands they go on to command something rather than do their best work at the keyboard.”

66. Lieutenant Colonel Jeffrey A Couillard, “Cyber Military Force,” *National Defense University*, April 26, 2023.

67. Government Accountability Office, “Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking,” December 21, 2022. (<https://www.gao.gov/assets/gao-23-105423.pdf>)

68. Suzanne Smalley, “Cyber Command’s rotation ‘problem’ exacerbates talent shortage amid growing digital threat,” *CyberScoop*, August 18, 2022. (<https://cyberscoop.com/military-rotation-norms-challenge-cyber-command>)

The current promotion system creates real risks to U.S. security. In a June 2023 military journal article, Navy Reserve Lieutenant Commander Eric Seligman notes that officers without cyber warfare experience struggle to assess the risks stemming from cyber operations. They face decision paralysis, improperly staff subordinate positions, and often fail to employ technical solutions necessary to achieve operational and tactical objectives. They also have difficulty translating doctrine into action, distinguishing good from bad operational and tactical advice, and predicting enemy maneuvers.⁶⁹

“Of the U.S. military’s more than 45 general and flag officers involved in cyber as of summer 2023, fewer than five had any technical experience in the cyber domain.”

As Seligman argues, a doctrinal and policy-focused understanding of cyber warfare is no replacement for hands-on experience. It would be like an officer who has “been trained on the concept of the rifle and its potential effects on the enemy” but never actually fired one.⁷⁰ Marine Corps officers stand by the tenet, “Every Marine a rifleman.” No Navy SEAL would follow an officer into battle if that officer did not go through BUD/S training. However, cyber operators and junior officers today follow the orders of a mostly inexperienced senior officer cadre. A Marine Corps captain concurred, “Leading in the cyberspace domain demands technical competency that cannot be taught in a 12-month schoolhouse alone.” He added, “Under no circumstances would a cyber officer be asked to lead a squadron of aircraft, and yet the opposite is often true.”

Indeed, interviewees for this project cite numerous examples of senior officers who have little to no experience in the cyber domain — even though the services have had 13 years since the creation of CYBERCOM to develop qualified senior leaders. Of the U.S. military’s more than 45 general and flag officers involved in cyber as of summer 2023, fewer than five had any technical experience in the cyber domain.⁷¹

CYBERCOM today has promotable talent, but the military is not properly utilizing it. A Marine Corps captain stated that he “personally had career setbacks because (he) pursued a master’s degree in computer science instead of a military war-college certificate.”

The current promotion system creates a vicious cycle. Potential cyber leaders cannot look to their superiors for mentorship or wisdom gained from experience within the domain. Facing disincentives to the further development of their skills, talented cyber officers choose other paths or exit the military altogether, depriving the next generation of cyber-experienced leadership.

Lack of Administrative, Intelligence, and Mental Health Support

CYBERCOM lacks many of the dedicated support functions that other unified combatant commands enjoy, including foundational intelligence support for operations, administrative support, and medical support, especially for mental health.

Administrative Support

Too often, CYBERCOM’s few qualified cyber operators are pulled away from operational responsibilities to handle administrative functions because the services provide CYBERCOM with inadequate administrative support. “Very few capable analysts can dedicate a significant amount of time to the operational

69. Eric Seligman, “Changing the Cyber Warfare Leadership Paradigm | Proceedings,” *U.S. Naval Institute*, June 2023. (<https://www.usni.org/magazines/proceedings/2023/june/changing-cyber-warfare-leadership-paradigm>)

70. Ibid.

71. Michael J. Vassalotti, Sofia Plagakis, and Barbara Salazar Torreon, “General and Flag Officers in the US Armed Forces: Background and Considerations for Congress,” *Congressional Research Service*, February 1, 2019. (<https://sgp.fas.org/crs/natsec/R44389.pdf>); “Leadership,” *U.S. Fleet Cyber Command/U.S. Tenth Fleet*, accessed March 9, 2024. (<https://www.fcc.navy.mil/LEADERSHIP>)

mission,” a U.S. Air Force major commented. “Less than 10 percent of team members have been on the team for over a year,” placing a significant burden on the few experienced analysts to both execute operations and train new personnel. The CNMF’s elevation to a sub-unified command in December 2022 partly resolved this issue, but the CNMF is only one-third of the CMF. The other teams continue to lack administrative support.

The administrative burden foisted onto cyber operators undermines talent retention. A 2019 internal survey of the U.S. Army Cyber Command workforce found that “a factor in their decision to leave after their contracts or service obligations expired was their inability to focus on the mission or tradecraft (i.e., time spent on keyboard) due to the constant distractions from administrative requirements.”⁷²

Intelligence Support

Cyber reconnaissance and targeting support are essential to the effectiveness of offensive cyber operations but CYBERCOM currently receives inadequate intelligence support.⁷³

Like all combatant commands, CYBERCOM does have a Joint Intelligence Operations Center, which provides operational intelligence for force employment. Cyber operations, however, lack a dedicated all-source cyberspace intelligence center to collect foundational, ongoing intelligence about adversary cyber capabilities and order of battle. The U.S. military does have such

centers for other warfighting domains, such as the Army’s National Ground Intelligence Center or the Navy’s Office of Naval Intelligence. These centers address standing intelligence requirements about adversary capabilities and strategies. Last year, the outgoing commander of CYBERCOM’s Joint Intelligence Operations Center called the absence of a comparable center for cyber intelligence a “gaping hole.”⁷⁴

In 2023, CYBERCOM announced it would establish a foundational cyber center in partnership with the Defense Intelligence Agency (DIA) and NSA. In effect, CYBERCOM attempted to build a service-like capability to remediate the gaps stemming from the absence of an independent cyber service. The final version of the FY 2024 NDAA, however, did not include the proposed provision to establish such a center.⁷⁵

If such a center were established, it would likely suffer staffing shortages unless the United States also creates a Cyber Force. The resourcing and staffing for existing intelligence entities usually falls to the parent service. While the DIA (or others) could be charged with managing the center, it would fall to the existing services to provide trained and qualified personnel, who would likely face the same training and skill development issues described earlier.

Medical Support

Cyber operators work in intense environments but are not afforded the same downtime as their counterparts

72. Chad Bates and Charlene Rose, “Understanding—And Fixing—The Army’s Challenge In Keeping Cyber Talent,” *Modern War Institute*, May 17, 2022. (<https://mwi.westpoint.edu/understanding-and-fixing-the-armys-challenge-in-keeping-cyber-talent>)

73. Michael Warner, “Intelligence in Cyber—and Cyber in Intelligence,” *Carnegie Endowment for International Peace*, October 16, 2017. (<https://carnegieendowment.org/2017/10/16/intelligence-in-cyber-and-cyber-in-intelligence-pub-73393>)

74. Alexandra Lohr, “Cyber Command plans an intelligence center to call its own,” *Federal News Network*, March 1, 2023. (<https://federalnewsnetwork.com/defense-main/2023/03/cyber-command-plans-an-intelligence-center-to-call-its-own>)

75. Mark Pomerleau, “Lawmakers nix proposal to create military cyber intelligence capability,” *DefenseScoop*, December 7, 2023. (<https://defensescoop.com/2023/12/07/congress-nixes-proposal-to-create-military-cyber-intelligence-capability>). As noted in the article, while the conference report on the bill argued that intelligence support “must be substantially improved,” lawmakers did not want to “dictate a specific organizational solution, but expect the Secretary of Defense to generate and implement one.”

in other fields.⁷⁶ Mental health initiatives exist across the DoD, including for Special Operations Forces, pilots, and operators involved with unmanned aerial flight operations.⁷⁷ However, there are no programs for the distinct challenges faced by cyber personnel.

Without an understanding of the work roles and tasks of cyber operators, the services (and specific commanders) may not appreciate the need for mental health services. One officer shared his troubling experience: “I think many folks in military cyber have been struggling with inexperienced leadership. But in [my service], those put in charge of cyber units can be downright hostile to technical cyber officers. For example, how about getting retaliated against by your [commanding officer] and your chain of command simply for going to mental health [treatment]? That thing they said in the yearly [general military training] about how going to mental health won’t affect your clearance ... it happened to me.”

Service Control and Service-Related Requirements Degrade Full Operational Capability

“Years of investment and training are lost when servicemembers are moved away from the cyber mission,” a general officer lamented. But because the services retain administrative control over cyber personnel assigned to CYBERCOM, the services can pull them out for service-related requirements unrelated to their cyber roles. This is one important reason why CYBERCOM was unable to get all 133 CMF teams up to FOC status and why it is so difficult for teams to maintain that status.

A lieutenant colonel in the U.S. Army Reserves, speaking from personal experience at the CNMF, observed a “general tension” between the administrative control and operational control commands. “[W]e are forced to pull servicemembers away from operational tasks to instead conduct service-related activities ... This is a systemic problem that, in mine and others’ opinions, hurts retention, as it undermines morale,” the officer said. Administrative control commanders “often create requirements at the expense of the mission. There are well documented times when units have closed down joint mission areas en masse to conduct unit events.”

An Air Force major shared a similar experience: “In one instance, a group commander required a 12-week ‘life skills’ course that taught new airmen how to cook, how to date, and how to be emotionally healthy. Meanwhile, the mission was manned at less than 60 percent.” The major said, “Another commander cited an ‘unwritten rule’ stating that he only owed the [NSA] 80 percent of his airmen’s time and the other 20 percent belongs to the USAF.”

In addition to impinging on cyber operators’ time, the services can also rotate them to different, non-cyber assignments. As one Army colonel explained, “Upskilling talent is hard, takes years, and as soon as someone reaches a threshold, the service rotates that person out of the team and back to a service assignment ... The demands within the services are continuing to pull talent away from the CMF.”

The services’ FOC shell game

By 2018, all the existing CMF teams had officially reached FOC, meaning they were supposed to have sufficiently trained and equipped personnel to execute

76. Jim Garamone, “Cybercom, NSA Senior Enlisted Leader Discusses Troops, Training, and Mental Health,” *Defense.gov*, May 14, 2019. (<https://www.defense.gov/News/News-Stories/Article/Article/1847532/cybercom-nsa-senior-enlisted-leader-discusses-troops-training-mental-health>)

77. “Preservation of the Force and Family,” *Special Operations Command Headquarters*, accessed March 9, 2024. (https://www.socom.mil/POTFF/Pages/mind-mental_health.aspx); U.S. Department of Defense, Press Release, “Department of Defense Mental Health Resources for Service Members and Their Families,” August 18, 2021. (<https://www.defense.gov/News/Releases/Release/Article/2737954/departement-of-defense-mental-health-resources-for-service-members-and-their-fam>)

their missions.⁷⁸ Yet fewer CMF teams are actually at FOC than official metrics indicate.

First of all, the services have not recruited and trained enough cyber personnel to fill 133 teams. As an Army colonel noted, “The lack of talented personnel to fill the positions on the teams has been and continues to be a severely limiting factor for the overall force. From the onset of U.S. Cyber Command, [the] services focused on recruiting, retaining, and filling teams to reach fully operational capable (FOC) status. Once teams achieve FOC, they often filled between 67-75 percent capacity.” As a result, teams that are officially considered to be FOC are not, in reality, at 100 percent strength.

According to multiple interviewees, proficient cyber operators are double-counted to make it appear like all the teams are at full strength. The services “play a shell game [with their] top tier talent,” one Army major warned. “It is a common occurrence that the same 50 people are constantly task-organized from across the force to solve any and all of the command’s hardest problems.” An Army captain gave a similar account of how his service initially brought its cyber teams up to FOC: “The Army’s rush to get teams to Full Operational Capability (FOC) was built on a farcical shell game in which the same personnel were moved from recently certified teams to new teams until all teams had certified. Yet few are able to provide capability if asked.”

An Army Reserve major similarly said that U.S. Army Cyber Command “consistently bent numbers, changed interpretations, and moved soldiers from team to team, or mission element to mission element, to paint the picture that teams were both fully manned and fully trained.” In fact, the officer said, “most [Cyber Protection Teams] never exceeded 75 percent of their intended manning and relied on

a core squad of fully trained people cleverly assigned to launder the reality that most soldiers were not fully trained.” This deception “was compounded by unrealistic training timelines.” U.S. Army Cyber Command “issued demanding deadlines to reach FOC, and lower-level commanders would then force timelines to move even faster — presumably to maximize their personal performance evaluations.” The result was an “environment that incentivized exaggerating how many soldiers and [Cyber Protection Teams] were FOC and disguising our numbers to higher headquarters.”

Acquisitions Challenges

Across the U.S. military, it takes an average of 10 to 15 years to field a new capability.⁷⁹ Yet in the cyber domain, tools are frequently updated and rendered obsolete within a year or two of development (if not sooner). Nevertheless, the services continue to enjoy a preponderant share of the budget and acquisitions authority for cyberspace even though they have not adapted to meet CYBERCOM’s timeline for tool acquisition. Thus, CYBERCOM is stuck with out-of-date capabilities and is forced to borrow the NSA’s tools, explaining why assessments continue to conclude that severing CYBERCOM from the NSA would have detrimental effects.

“Across the U.S. military, it takes an average of 10 to 15 years to field a new capability. Yet in the cyber domain, tools are frequently updated and rendered obsolete within a year or two of development (if not sooner).”

Recognizing this problem, Congress has intervened several times to grant CYBERCOM greater control over the acquisition of capabilities, resulting in incremental

78. Samuel Souvannason, “Navy Cyber Mission Force Teams Achieve Full Operational Capacity,” *U.S. Department of Defense*, November 2, 2017. (<https://www.defense.gov/News/News-Stories/Article/Article/1361059/navy-cyber-mission-force-teams-achieve-full-operational-capability>)

79. Jen Judson, “US Army looks to cut typical acquisition timeline in half,” *DefenseNews*, December 7, 2017. (<https://www.defensenews.com/land/2017/12/07/army-looks-to-cut-typical-acquisition-timeline-in-half>)

changes to ameliorate this issue. However, this solution runs contrary to civilian oversight of acquisition, which services have and CYBERCOM does not.

In the FY 2016 NDAA, Congress granted CYBERCOM authority for the development, acquisition, and sustainment of cyber-specific equipment and capabilities.⁸⁰ The following year, Congress amended DoD's special emergency procurement authority to facilitate defense against and recovery from a cyberattack.⁸¹ As a result of more recent congressional direction, CYBERCOM in 2027 will assume "service-like acquisition decision authority" over platforms that the command uses to conduct cyber operations.⁸²

Since the passage of the FY 2016 NDAA, CYBERCOM has been able to hire some acquisition professionals, but it continues to outsource most contracting, as the services make the large purchases on its behalf.⁸³ The director of CYBERCOM's acquisitions directorate said that since Congress granted the command EBC, he hoped to hire 40 people in 2023 and up to another 50 in 2024. But this is still a fraction of the personnel required to manage a \$3 billion budget. In comparison, the Army boasts that its acquisition workforce "is composed of approximately 32,000 civilian and military professionals,"⁸⁴ or about one person for every \$6 million of discretionary budget.

Despite CYBERCOM's acquisition authorities and EBC, the lion's share of funding for cyberspace activities remains with the services. The services, however, lack a unified process for spending money on cyber-related capabilities, equipment, training,

and education. This leads to redundant and disparate efforts, not effective preparation for joint warfighting. As a major in the U.S. Air Force noted, "The services and the other combatant commands have taken it upon themselves to acquire their own cyber capabilities to meet their needs, resulting in vast duplication and reliance on defense contractors to provide questionable and often self-serving operational guidance."

Another Air Force major similarly shared:

I've witnessed vendors sell the same \$100M offering to two services under a different name so those services could independently lobby for resources. I've witnessed one service sabotage another's cyber operation (both under the same 'Joint' Force Headquarters) simply because that service did not receive credit. I've seen the services' acquisition communities spend over \$1B on poorly defined and duplicative cyber requirements to deliver tools that will never be used. Every effort to unify resources and address national priorities is undermined and resisted by the services who perceive no benefit to their domains.

All of this ultimately reduces force readiness. Without the correct equipment, even the best-trained cyber warrior cannot be effective in conflict. Moreover, the ongoing effort to transfer acquisition authority to CYBERCOM, while borne out of a legitimate frustration with the status quo, will result in the removal of traditional civilian oversight of acquisition, which only the services can provide.

80. National Defense Authorization Act for Fiscal Year 2016, Pub. L. 114-92, 129 Stat. 886, §807. (<https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf>)

81. National Defense Authorization Act for Fiscal Year 2017, Pub. L. 114-328, 130 Stat. 2600, §1641. (<https://www.congress.gov/bill/114th-congress/senate-bill/2943>)

82. Paul M. Nakasone, "2023 Posture Statement of General Paul M. Nakasone," *U.S. Cyber Command*, March 7, 2023. (<https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone>)

83. Mark Pomerleau, "Cyber Command looking to bolster acquisition office as it prepares to handle \$3B annually," *FedScoop*, July 27, 2022. (<https://fedscoop.com/cyber-command-looking-to-bolster-acquisition-office-as-it-prepares-to-handle-3b-annually>)

84. "Officers in the Army Acquisition Workforce," *United States Army Acquisition Support Center*, accessed March 9, 2024. (<https://asc.army.mil/web/career-development/military-officer/information>)

Counterarguments to Establishing a U.S. Cyber Force

Some experts who acknowledge the force-generation challenges facing CYBERCOM nevertheless oppose the creation of a Cyber Force.⁸⁵ They offer four main arguments against creating an independent, uniformed cyber service.

Counterargument 1: A Cyber Force will negatively impact readiness in the short term and create budgeting and personnel problems for the other services.

This critique posits that creating a Cyber Force would deprive the services of critical personnel. Transferring capable IT and cybersecurity professionals now focused on network architecture and the defense of internal service systems to the Cyber Force would leave the services bereft of skilled personnel. However, shifting only CMF billets, which do not include the services' IT and cybersecurity personnel, would render this potential issue moot.

A related objection argues that transitioning personnel and budgets to the Cyber Force from multiple services would impose an insurmountable administrative burden. Prior to the establishment of the Space Force, the preponderance of space-related personnel and investments were already housed within the Department of the Air Force. But cyber-focused personnel and funding are currently much more dispersed.⁸⁶ While this is true, all services have existing methods for inter-service transfers. By

streamlining these transfers, the Space Force acquired more than 13,000 servicemembers and civilians in its first two years.⁸⁷

Counterargument 2: The Space Force should be responsible for force generation for cyberspace.

Some commentators argue that DoD should combine cyber and space operations under the control of the Space Force. Those who favor this position tend to believe a service's value is based at least in part on its size. At present, the Space Force is small but set to grow from 8,400 to 16,000 uniformed and civilian Guardians and may continue to grow based on the importance of space operations.⁸⁸ More to the point, however, this critique ignores the fact that a small number of highly skilled operatives can be effective in cyberspace.

The argument also presumes an inherent link between space and cyberspace. Space assets, such as communications satellites, indeed serve a critical function in the transmission of information. Likewise, many ground operations and weapons systems are also dependent on space assets, but this does not mean the Space Force should train personnel for ground operations. As distinct operational domains, space and cyberspace have unique "man, train, and equip" requirements.

Counterargument 3: 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

85. See, for example, Military Cyber Professionals Association, "HammerCon 2023: US Cyber Force Panel (Schafer, Cleary, Franz, and Montgomery)," June 13, 2023. (<https://www.youtube.com/watch?v=CUYfjnXGDk>)

86. Sandra Erwin, "U.S. Air Force to transfer 23 units to the Space Force," *SpaceNews*, March 31, 2020. (<https://spacenews.com/u-s-air-force-to-transfer-23-units-to-the-space-force/>)

87. Bryan Bender, "What the Space Force is, and isn't," *Politico*, February 3, 2021. (<https://www.politico.com/news/2021/02/03/space-force-explained-465799>)

88. David Ignatius, "The Space Force needs to get bigger," *The Washington Post*, August 22, 2023. (<https://www.washingtonpost.com/opinions/2023/08/22/us-space-force-military-pentagon-competition/>)

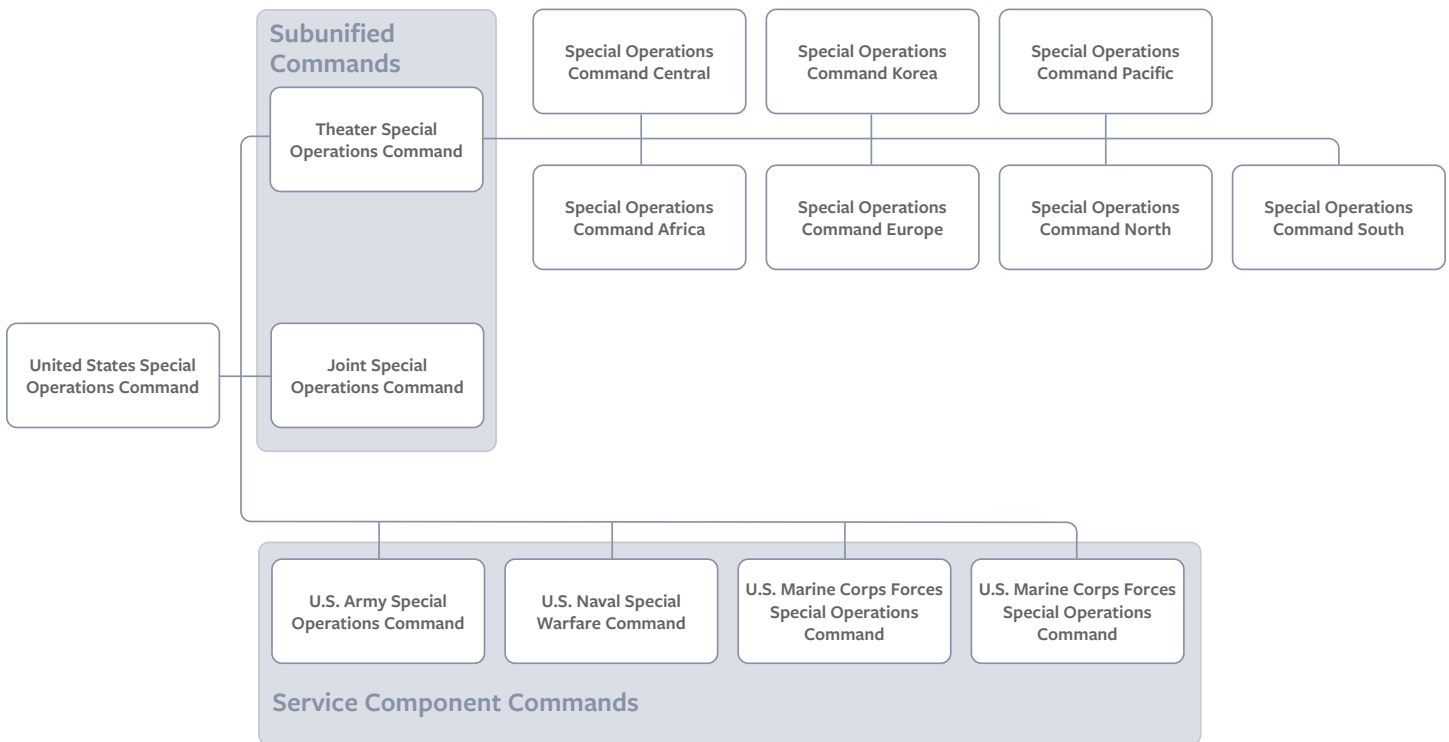
should apply the SOCOM model to cyberspace — notwithstanding SOCOM’s own growing pains over its 30-year history.⁸⁹ However, while SOCOM and CYBERCOM both possess highly skilled operators, they are otherwise very different.

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.”

A side-by-side comparison of the SOCOM and CMF structures depicts two wholly different organizational architectures, as illustrated in figures 3 and 4. SOCOM’s

Figure 3: SOCOM Structures



⁸⁹ 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>)

organization into many sub-unified commands and geographic commands does not reflect the requisite structure of CMF and its component parts.

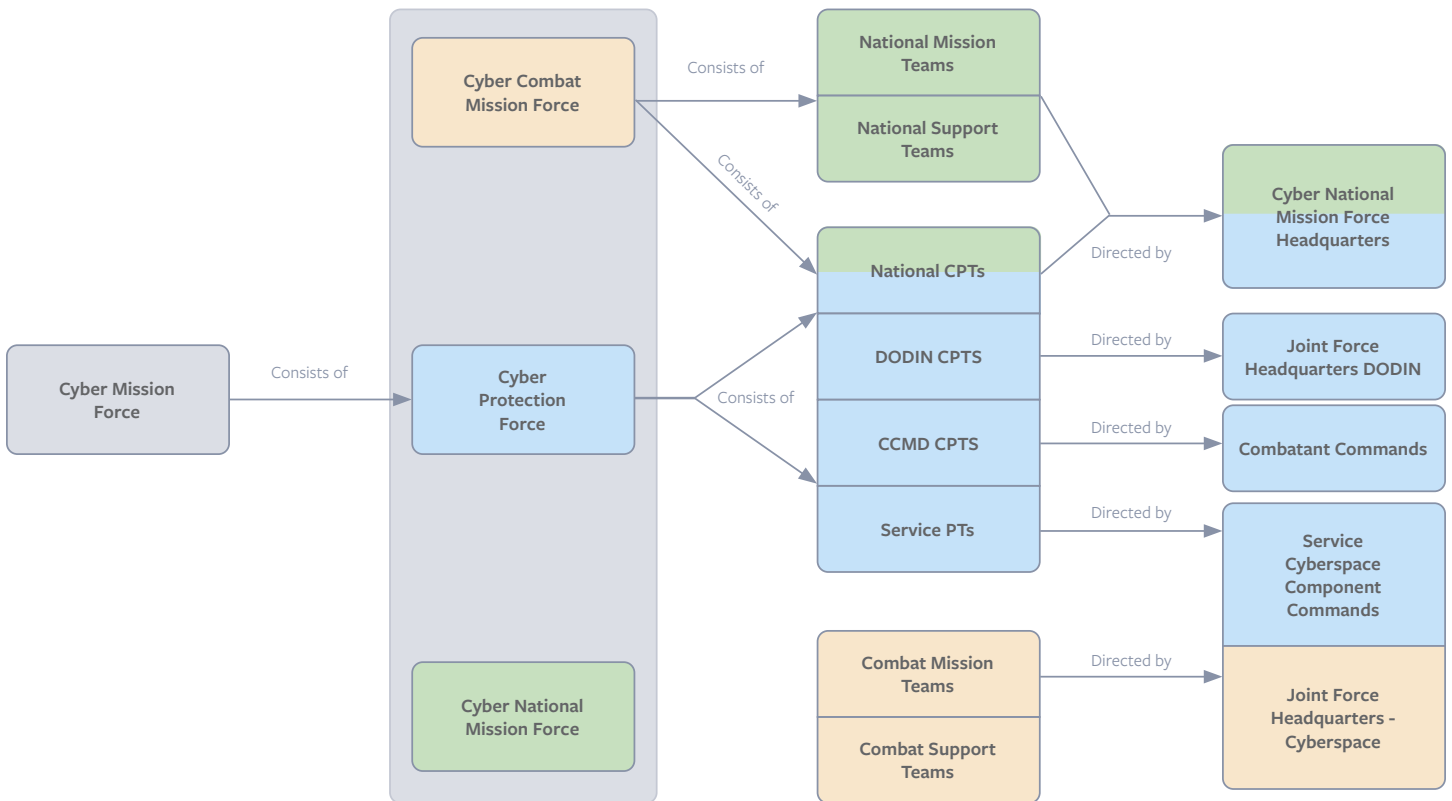
SOCOM has also faced the same challenges as CYBERCOM regarding drawing personnel from disparate services. The services' inconsistent definitions of overlapping skill sets create incompatibility. This makes interoperability challenging, particularly in dynamic, high-operational-tempo environments. Although the defense community is largely content with the way SOCOM is organized, led, and operated, a GAO report from October 2022 noted that SOCOM has its own challenges concerning oversight and command and control.⁹⁰ For SOCOM, a dependence on multiple services makes some of

these challenges unavoidable, yet the U.S. military has a better option for cyber force generation.

Counterargument 4: CYBERCOM should absorb many of the man, train, and equip responsibilities from the services.

Rather than creating a Cyber Force, some argue that 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.

Figure 4: CMF Structures



⁹⁰ Government Accountability Office, “Special Operations Forces: Better Data Necessary to Improve Oversight and Address Command and Control Challenges,” October 2022. (<https://www.gao.gov/assets/gao-23-105163.pdf>)

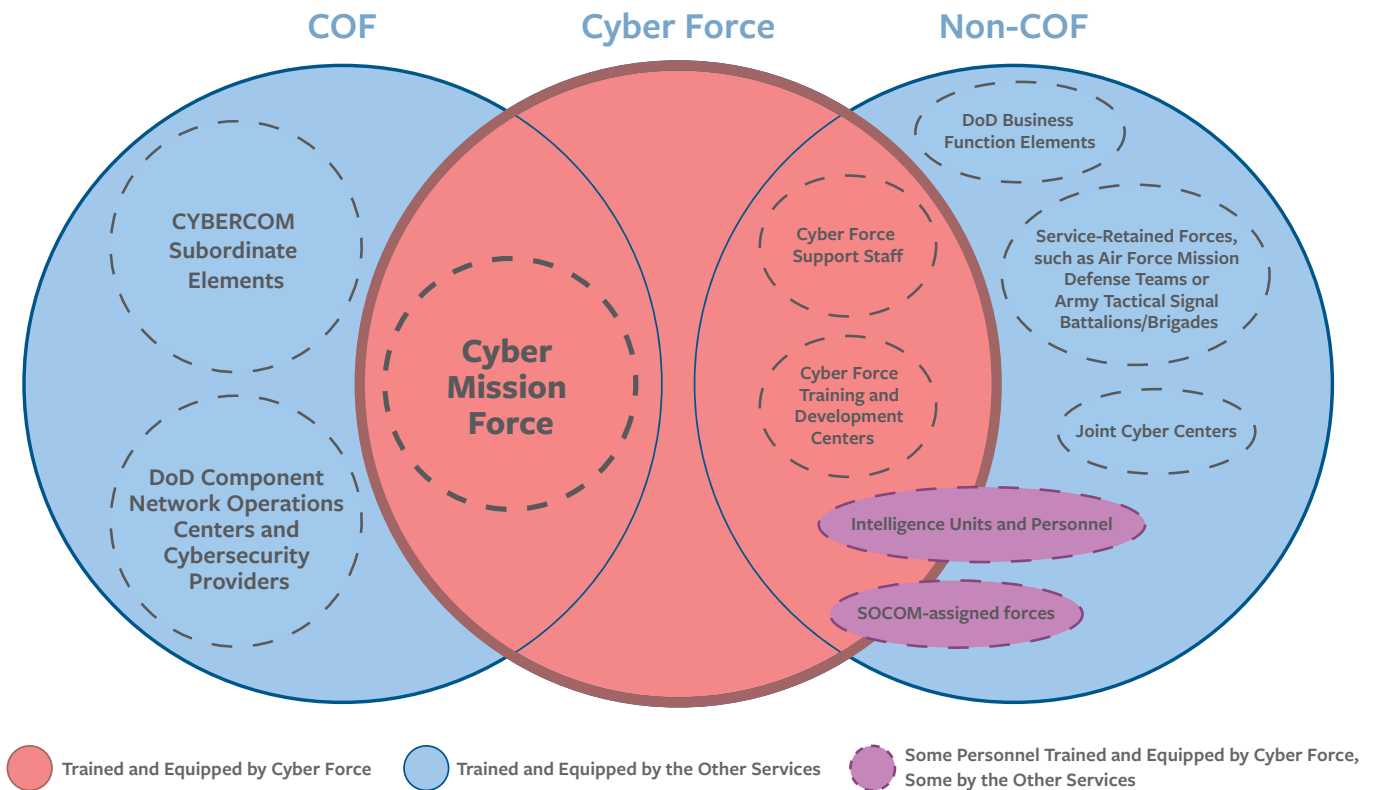
In this scenario, the commander of CYBERCOM would become responsible for military cyber force generation and force employment in addition to his or her duties as head of the NSA. While the dual-hatted structure for CYBERCOM and the NSA was initially intended to be temporary, it remains advantageous, as concluded by a December 2022 study led by General (Ret.) Joseph Dunford, former chairman of the Joint Chiefs of Staff.⁹¹ 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?

Many of the challenges outlined in the section above could only be solved or at least significantly mitigated through the creation of the Cyber Force as the force generator for the cyber domain. CYBERCOM would remain the force employer. This new Cyber Force could be located within the Department of the Army, just as the Marine Corps is housed within the Department of the Navy and the Space Force sits within the Department of the Air Force.

Standing up this new service would be relatively straightforward. Initially, the Cyber Force would

Figure 5: Initial Billets of a New Cyber Force



91. 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>)

encompass the billets that currently comprise the CMF: a 6,200-person mission group consisting of servicemembers, civilians, and contractors (see Figure 5).⁹² 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 (or addition) 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 servicemembers 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 personnel, although this number would likely 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.⁹³ At a leadership level, the Space Force’s establishment mostly required the lateral transfer of personnel from Air Force Space Command.⁹⁴ The Space Force, which currently has 8,400 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.⁹⁵ To boost recruitment, the service has also taken advantage of opportunities for the direct commissioning of civilians with requisite skills for space.⁹⁶

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. Figure 6 illustrates proposed responsibilities of the Cyber Force and the services.

An initial budget for the Cyber Force would be approximately \$16.5 billion, a fraction of the

Figure 6: Proposed Responsibilities for the Cyber Force and the Services

U.S. Cyber Force Responsibilities	Service-Retained Responsibilities
Man, train, equip for offensive cyberspace operations	
Man, train, equip for defensive cyberspace operations	Man, train, equip for defensive cyberspace operations clearly linked to traditional service warfighting competencies
Man, train, equip for the portion of the DoD Information Networks (DODIN) owned and operated by Cyber Force owned and operated	Man, train, equip for the portions of the DODIN owned and operated by the other services
Man, train, equip for the build/operation/maintenance/defense of Cyber Force IT infrastructure	Man, train, equip for the build/operation/maintenance/defense of service-retained IT infrastructure

⁹². U.S. Cyber Command Public Affairs, “Cyber 101 – Cyber Mission Force,” *U.S. Cyber Command*, November 1, 2022. (<https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force>)

⁹³. 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>)

⁹⁴. “People,” *U.S. Space Force*, accessed January 8, 2024. (<https://www.spaceforce.mil/About-Us/About-Space-Force/USSF-People>)

⁹⁵. Leo Shane III, “Space Force eyes easing enlistment rules to target high-demand skills,” *Air Force Times*, September 13, 2022. (<https://www.airforcetimes.com/news/pentagon-congress/2022/09/13/space-force-eyes-easing-enlistment-rules-to-target-high-demand-skills>)

⁹⁶. Air Force Recruiting Service, “Constructive Service Credit now offered to applicants for two Space Force career fields,” *U.S. Space Force*, October 28, 2022. (<https://www.spaceforce.mil/News/Article/3205270/constructive-service-credit-now-offered-to-applicants-for-two-space-force-caree>)

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.⁹⁷ An apt comparison is the budget for the Space Force, for which DoD requested \$30 billion for FY 2024.⁹⁸

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 thanks to 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.⁹⁹

Creating a Cyber Force would also benefit the NSA.¹⁰⁰ A quarter of the NSA's workforce comprises active-duty military units, currently provided by the services. However, these units are not held accountable for successfully serving the NSA's mission. With a Cyber Force focused on delivering well-trained cyber personnel, the NSA would, in turn, receive more, high-quality, human resources.



During a visit to Navy Information Operations Command Pensacola, then deputy commander of U.S. Cyber Command Lt. Gen. Timothy Haugh, engaged in cyber discussions with Sailors on Oct. 12, 2023. (U.S. Navy photo by Petty Officer Third Class Leonell Domingo)

A Cyber Force would also facilitate the establishment of more robust legal principles for cyberspace. Military leaders and commanders have long required legal advisors for the specific domains in which they operate. The DoD legal community, in turn, has training, education, and experience tracks to develop attorneys who deliver this legal support. 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 serves U.S. cyber operations poorly.

If done properly, the 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 acquisition processes and maximizing budgetary effectiveness.

⁹⁷. 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)

⁹⁸. 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)

⁹⁹. 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>)

¹⁰⁰. Michael Warner, "US Cyber Command's First Decade," *Hoover Institution*, 2008. (https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf); Mark Pomerleau, "Key lawmakers in favor of keeping 'dual hat' arrangement between Cybercom and NSA," *DefenseScoop*, November 17, 2022. (<https://defensescoop.com/2022/11/17/two-key-lawmakers-in-favor-of-keeping-dual-hat-arrangement-between-cybercom-and-nsa>)

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, space, electronic warfare, and psychological warfare capabilities within its Strategic Support 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,¹⁰¹ 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 CME, 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. While many experts have long called for the creation of an independent Cyber Force,¹⁰² policymakers should especially listen to the voices of those servicemembers with direct, extensive operational experience. The numerous first-hand accounts highlighted in this monograph offer a compelling testament to the need for an independent service for cyberspace.

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.

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

102. James Stavridis, “The US Military Needs to Create a Cyber Force,” *Bloomberg*, March 8, 2023. (Archived version available at https://web.archive.org/web/20230311100830/https://www.washingtonpost.com/business/2023/03/08/the-us-needs-a-seventh-branch-of-the-military-cyber-force/aa72d5dc-bdab-11ed-9350-7c5fccd598ad_story.html)

Appendix A: Select Quotations from Interviews

The following are illustrative excerpts from more than 130 pages of interviews with 76 active-duty and recently separated servicemembers and Defense Department civilians about cyber readiness, CYBERCOM, and the challenges they have encountered. These interviews were collected over the course of the past year and speak to the significant challenges discussed throughout this monograph. The authors have chosen not to disclose the full remarks to protect the individuals who agreed to share their personal experiences.

Thirty-four percent of the interviewees came from the U.S. Army, 30 percent from the U.S. Navy, and 26 percent from the U.S. Air Force. A small number of accounts also come from the Marine Corps, Space Force, and DoD civilians. Most of the accounts (61 percent) came from officers with ranks of O-4 to O-6. Another 26 percent come from officers with ranks of O-3. Notably, one interview is with a general officer (O-7).

Figure 7: The Service of Interviewees

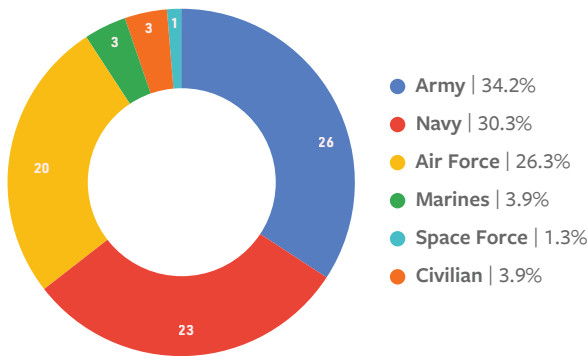
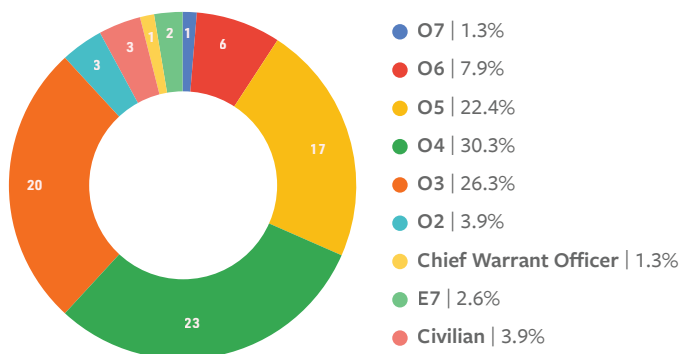


Figure 8: The Rank of Interviewees



General Officer, U.S. Military

“Our current strategy of relying on the existing Services to build the cyber expertise and capabilities required is inefficient, ineffective, and unlikely to succeed despite years of investment and the best efforts of our service members. Without a doubt, the only viable path forward for USCYBERCOM is to establish a new Service focused on organizing, training, and equipping forces required to fight — and win — in cyberspace.”

“Years of investment and training are lost when service members are moved away from the cyber mission. Complicated and inconsistently applied incentive programs result in retention issues.”

“Differences in training also impact USCYBERCOM’s ability to conduct operations.”

Colonel, United States Air Force

“In aggregate, we see a combatant command spending an inordinate amount of time executing Service-like responsibilities at the expense of its primary responsibilities to defend the [Department of Defense Information Networks], provide support to combatant commanders for execution of their missions around the world, and strengthen our nation’s ability to withstand and respond to cyber-attack. Instead, we have a Department of Defense with no single service incentivized to put cyberspace operations at the forefront.”

“If you look [at] who leads cyberspace operations in the Department of Defense, they are not typically grown from within the cyberspace operations force. Cyber leaders should lead cyberspace operations and represent cyberspace operations in joint warfighting. We need ‘cyber minded’ leaders.”

Colonel, United States Army

“Having been on both the inside and outside of the Cyber Mission Force since it was first established, the

lack of talented personnel to fill the positions on both teams has been and continues to be a severely limiting factor for the overall force.”

“In fact, it was once found that about 10% of the personnel execute as much as 80% of the operational missions.”

[On the subject of officers sitting on promotion boards] “Officers with advanced, skilled degrees in computer science from esteemed institutions are equated with those who received online degrees in information management; they are given no additional consideration for their knowledge, skills, or abilities and are disadvantaged. This is akin to equating a brain surgeon with a field medic.”

Captain (Ret.), United States Navy

“The development of service-specific cyber specialty fields without dedicated senior level commitments has yielded varying levels of fragmented support to cyber operations, lack of continuity of cyber personnel, unclear career paths, insufficient experience, wide use of noncyber personnel in cyber leadership positions, and cyber operations being treated always as a supporting entity across all services.”

“[C]yber attacks 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 cyber attacks.”

Captain, United States Navy

“[United States Special Operations Command]’s success is achieved by allowing each of the service specific commands to specialize in discrete types of warfare, technologies, and operational environments. USSOCOM picks the ‘best athlete’ depending on the operational outcome they are trying to achieve.”

“USCYBERCOM assigns the military services ... essentially requiring every team to master every aspect of cyber warfare to successfully operate against their assigned target. This methodology is completely out of sync with the way the rest of the DoD is constructed

... Applying the USCYBERCOM methodology to air warfare would be akin to requiring every service to operate the same aircraft, to accomplish every aspect of air warfare, in every operational environment.”

Captain, United States Marine Corps

“Leading in the cyberspace domain demands technical competency that cannot be taught in a twelve-month schoolhouse alone. One of my worst professional experiences involved working underneath a woefully unprepared commander with a degree in culinary arts ... Under no circumstances would a cyber officer be asked to lead a squadron of aircraft, and yet the opposite is often true.”

Major, United States Air Force

“I’ve witnessed vendors sell the same \$100M offering to two services under a different name so those services could independently lobby for resources. I’ve witnessed one service sabotage another’s cyber operation (both under the same ‘Joint’ Force Headquarters) simply because that service did not receive credit. I’ve seen the services’ acquisition communities spend over \$1B on poorly defined and duplicative cyber requirements to deliver tools that will never be used. Every effort to unify resources and address national priorities is undermined and resisted by the services who perceive no benefit to their domains.”

Colonel (Ret.), United States Army

“I’ve seen senior warfighting leaders dismissively call cyber research ‘book reports,’ cyber operators ‘nerds,’ and cyber capability development ‘science projects.’ These ... leaders who make critical cyber operational, resource allocation, and risk assessment decisions control promotions to choose people that look like themselves.”

Lieutenant Colonel, United States Marine Corps

“I can’t speak for the other services, but I perceive a lack of career progression for cyber officers in the Marine Corps. I commanded a Combat Mission

Team and am fully qualified to join the cyber field but decided not to apply for the specialty because of the limited command opportunities.”

Lieutenant Colonel, United States Air Force

“[Headquarters, Air Force] has commissioned multiple RAND studies on cyber force structure, then ignores the key recommendations.”

“Few, if any, qualified offensive cyber operators have graduated to positions of command, Colonels, and Generals. This is comparable to an Air Force in which none of the Colonels and Generals have ever been qualified pilots.”

“Coupling Goldwater-Nichols and the fact that the USAF doesn’t see ‘cyberspace operations’ as one of its core missions, [the U.S. Air Force] will likely continue to deprioritize developing and promoting leaders to achieve DoD objectives in and through cyberspace.” [USAF removed “cyber” from the Air Force Mission Statement in 2021.]

Captain, United States Air Force

“Not for more money or flexibility — I always understood the military couldn’t match industry here, but that’s not why anybody I knew joined the military. I left for the same reason as many others: when you feel your organization keeps you from making an impact on the mission and you can’t change the organization, then you either have to stop caring so much or leave. I saw two primary things holding the Air Force back that it would not fix. I believe it will require a separate cyber service to address these problems: One, organizationally the Air Force lacks understanding of the cyber domain, and, two, it has failed to take cyberspace operations seriously as a warfighting discipline.”

“During my career, I learned that making cyber operations look like the rest of the Air Force was more important than mission success. For the sake of the mission and the people, we need a separate cyber service and we must understand that lives depend on operational success in cyberspace. A general once

told me ‘Someday you can change things; when you’re a general.’ They didn’t know what that really communicated to me.”

Commander, United States Navy

“The core of the issue facing the broader [Cyberspace Operations Forces] is the lack of a single service designed to man, train, equip, and manage the careers of a full cadre of Cyber Operations professionals. The current construct of the military services is not conducive to developing, retaining, and advancing a highly trained Cyber Force. Each service is focused on being proficient in and advancing those servicemembers who excel in their respective warfighting domains (sea, air, and land).”

Captain, United States Army

“It is important to highlight the issues in Cyber are not solely because of problems within the Army. A lack of joint command vision regarding the separation of roles and responsibilities between USCC and the NSA, for example, has led to significant confusion and constantly changing direction regarding what problems the command is required to solve.”

Major, United States Air Force

“In short, the Air Force values breadth over technical depth and meeting requirements on paper versus building and enabling true technical talent. When I arrived at Keesler AFB for my initial skills training as a cyber warfare officer, I was ecstatic. I was finally going to be a part of the force responsible for the slogan ‘it’s not science fiction, it’s what we do every day.’ I expected training and equipment that would enable me to contribute to homeland defense or project power in current conflicts around the globe. The reality was very basic training which was worse than most industry offerings and equipment worse than what I had purchased for myself to use at home. Additionally, the training itself was disjointed and lacked focus - covering everything from space-based platforms to loading pallets with only a few weeks of actual offensive or defensive cyber training.”

Appendix B: Historical Case Studies: The Air Force and Space Force

In the past, when the DoD has faced force-generation or force-employment challenges, the U.S. military has undergone significant reorganization.

World War I firmly demonstrated the ability of aircraft to “impact an enemy beyond a depth that could be readily imagined by those operating in [land and sea].”¹⁰³ After the war, the War Department (the predecessor to DoD) and congressional leaders began to evaluate the implications of flying for future military operations and subsequently renamed the Air Service the U.S. Army Air Corps. While the Corps was not an independent service, it “strengthen[ed] the conception of military aviation as an offensive, striking arm rather than an auxiliary Service.”¹⁰⁴ Each service began investing in its own aviation capabilities.

During the interwar period, multiple boards examined the country’s readiness for, and resources dedicated to, military flying missions. Most notably, the 1919 Menoher Board found the “best way to take advantage of the new technology in aviation was to create a new military organization.”¹⁰⁵

By the end of World War II, air power had emerged as a pivotal force, affirming the wisdom of the Menoher

Board’s recommendation. The National Security Act of 1947 established the U.S. Air Force as an independent, uniformed service, 30 years after Congress began documenting officers raising that the domain could not be effectively handled by the compartmentalized efforts of the U.S. Army and U.S. Navy.

In 1982, the Air Force established the first Air Force Space Command. In 1985, the United States established a unified U.S. Space Command,¹⁰⁶ tasked with coordinating Army, Naval, and Air Force space forces and providing “space-based missile warning, communications, navigation, weather, and imagery capabilities.”¹⁰⁷ The 2001 Rumsfeld Commission first proposed the establishment of a Space Force.¹⁰⁸ But a year later, DoD disbanded the U.S. Space Command and gave its responsibilities to U.S. Strategic Command.¹⁰⁹

Over the next 16 years, however, DoD leaders began to recognize that no one military entity was placing sufficient emphasis on space security. China’s demonstration of its anti-satellite capabilities, along with other threats, ignited conversations among policymakers that mirrored those prior to the establishment of the Air Force.¹¹⁰ DoD leaders also began realizing that U.S. Strategic

103. John Venable, “How the Air Force Got Its Start 72 Years Ago,” *Heritage Foundation*, September 18, 2019. (<https://www.heritage.org/defense/commentary/how-the-air-force-got-its-start-72-years-ago>)

104. “1926 – The US Army Air Corps Act,” *Air Force Historical Support Division*, accessed March 9, 2024. (<https://www.afhistory.af.mil/FAQs/Fact-Sheets/Article/459017/1926-the-us-army-air-corps-act>)

105. Dr. James P. Tate, “The Army and Its Air Corps: Army Policy Toward Aviation 1919-1941,” *Air University Press*, June 1998. (https://media.defense.gov/2017/Apr/07/2001728467/-1/-1/0/B_0062_TATE_ARMY_AIR_CORPS.PDF)

106. Benjamin S. Lambeth, “A Short History of Military Space,” *Air & Space Forces Magazine*, December 1, 2004. (<https://www.airandspaceforces.com/article/1204space>)

107. Frank A. Rose, “Re-establishing US Space Command is a great idea,” *Brookings Institution*, January 7, 2019. (<https://www.brookings.edu/blog/order-from-chaos/2019/01/07/re-establishing-u-s-space-command-is-a-great-idea>)

108. Marcia S. Smith, “Military Space Activities: Highlights of the Rumsfeld Commission Report and Key Organization and Management Issues,” *Congressional Research Service*, February 21, 2001. (https://digital.library.unt.edu/ark:/67531/metadc806331/m2/1/high_res_d/RS20824_2001Feb21.pdf)

109. Frank A. Rose, “Re-establishing US Space Command is a great idea,” *Brookings Institution*, January 7, 2019. (<https://www.brookings.edu/blog/order-from-chaos/2019/01/07/re-establishing-u-s-space-command-is-a-great-idea>)

110. Everett Carl Dolman, “New Frontiers, Old Realities,” *Strategic Studies Quarterly*, Spring 2012. (https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-1/dolman.pdf); Terri Moon Cronk, “Space-Based Capabilities Critical to US National Security, DOD Officials Say,” *DOD News*, May 24, 2021. (<https://www.defense.gov/News/News-Stories/Article/Article/2629675/space-based-capabilities-critical-to-us-national-security-dod-officials-say>); Tom Roeder and Tony Peck, “Space Force: A timeline of change,” *The Gazette*, July 26, 2018. (https://gazette.com/military/space-force-a-timeline-of-change/article_44285b42-7573-11e8-b983-e3bc886964a1.html)

Command’s responsibilities were becoming “too big for one combatant commander to manage.”¹¹¹



In 2008, Congress commissioned the Institute for Defense Analyses to write a report on “Leadership, Management, and Organization for National Security Space.” It highlighted the need for a greater number of operators who are “steeped in space.”¹¹² Over the next decade, the U.S. military increased its capabilities in space and focused on specializing organizational, acquisitions, and personnel training structures.

In December 2018, President Donald Trump signed an executive order authorizing DoD to reinstate U.S. Space Command as a unified combatant command responsible

for force employment in space. In the FY 2020 NDAA, Congress then established an independent U.S. Space Force to man, train, and equip personnel for U.S. Space Command. Articulating the connection between these two entities, then commander of U.S. Space Command Air Force Gen. John “Jay” Raymond noted, “U.S. Space Command will only be as strong as the capabilities it is provided by the United States Space Force.”¹¹³

Ultimately, it took congressional intervention to establish independent uniformed services for air and space. Congressional intervention is again needed to address the significant readiness challenges stemming from the current organization and structure of U.S. cyber forces.

Figure 9: The Space Force vs. Space Command

		What It Is	What It Does	Composition
	SPACE FORCE	A military service that trains members and acquires systems for specific warfighting areas.	Provides the people and technology that protect the space-enabled advantages (GPS, communications, etc.) on which America and its allies rely.	Only Space Force members
	SPACE COMMAND	A combat command that uses the military services’ people and technology to conduct worldwide operations in times of war and peace.	Plans, operates, and directs the forces for space warfighting.	Members from all service branches

111. Frank A. Rose, “Re-establishing US Space Command is a great idea,” *Brookings Institution*, January 7, 2019. (<https://www.brookings.edu/blog/order-from-chaos/2019/01/07/re-establishing-u-s-space-command-is-a-great-idea>)

112. A. Thomas Young, Edward Anderson, Lyle Bien, Ronald R. Fogleman, Keith Hall, Lester Lyles, and Dr. Hans Mark, “Leadership, Management, and Organization for National Security Space,” *Institute for Defense Analyses*, July 2008. (<https://aerospace.csis.org/wp-content/uploads/2018/09/AllardCommission.pdf>)

113. Jim Garamone, “Trump Signs Law Establishing US Space Force,” *DoD News*, December 20, 2019. (<https://www.defense.gov/News/News-Stories/Article/Article/2046035/trump-signs-law-establishing-us-space-force>)

Appendix C: The History of U.S. Information Operations and the Creation of CYBERCOM

The concept of “cyber” in the military lexicon did not appear until well after the military established doctrinal concepts for information operations, psychological operations, and computer network operations (both offensive and defensive).¹¹⁴ Information and psychological operations have been around for centuries, long predating wired and wireless communications. The notion that computer networks could multiply the effects of these operations, however, began to take hold in the late 1980s and early 1990s. As DoD became more dependent on information systems for command and control, it created the Joint Task Force-Computer Network Defense in 1988. After the Gulf War, during which the U.S. military exploited technological advantages to ensure fast, efficient battlefield victories,¹¹⁵ the task force evolved into the Joint Task Force-Computer Network Operations (JTF-CNO).¹¹⁶

The U.S. military began developing cyber doctrine in earnest in 2003 following the discovery of “Moonlight Maze,” a multi-year Russian cyber espionage operation against U.S. systems. This campaign, which stole sensitive documents from U.S. government agencies,

marked the “first large-scale cyberespionage attack by a well-funded and well-organized state actor.”¹¹⁷ The next year, the Joint Chiefs of Staff defined cyberspace as a warfighting domain.¹¹⁸ DoD released its first National Military Strategy for Cyberspace Operations in 2006.¹¹⁹

Two years prior to that strategy’s release, DoD reorganized JTF-CNO under U.S. Strategic Command. The Joint Task Force-Global Network Operations (JTF-GNO) handled cyber defense, and the Joint Functional Component Command-Network Warfare (JFCC-NW) handled offensive missions. However, after additional significant cyber espionage campaigns by U.S. adversaries, DoD combined the two and established CYBERCOM as a sub-unified combatant command under U.S. Strategic Command in 2010, led by a commander dual hatted as the director of NSA. CYBERCOM was tasked with “direct[ing], synchroniz[ing], and coordinat[ing] cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners” as well as

114. U.S. Cyber Command, Public Affairs, “Cyber 101 - US Cyber Command History,” *U.S. Cyber Command*, October 4, 2022. (Archived version available at <https://web.archive.org/web/20221011152417/https://www.cybercom.mil/Media/News/Article/3179270/cyber-101-us-cyber-command-history>); For a history of information operations in the U.S. Army, see: Sarah P. White, “The Organizational Determinants of Military Doctrine: A History of Army Information Operations,” *Texas National Security Review*, Winter 2022/2023.

(<https://tnsr.org/2023/01/the-organizational-determinants-of-military-doctrine-a-history-of-army-information-operations>); For cyber, see, Sarah P. White, “Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine,” Doctoral dissertation, Harvard University, Graduate School of Arts & Sciences, 2019. (<https://dash.harvard.edu/handle/1/42013038>)

115. Joshua Rovner, “Warfighting in Cyberspace,” *War on the Rocks*, March 17, 2021. (<https://warontherocks.com/2021/03/warfighting-in-cyberspace>)

116. U.S. Cyber Command, Public Affairs, “Cyber 101 - US Cyber Command History,” *U.S. Cyber Command*, October 4, 2022. (Archived version available at <https://web.archive.org/web/20221011152417/https://www.cybercom.mil/Media/News/Article/3179270/cyber-101-us-cyber-command-history>)

117. Omry Haizler, “The United States’ Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking,” *Cyber, Intelligence, and Security*, January 2017. (<https://www.inss.org.il/wp-content/uploads/2017/03/The-United-States%E2%80%99-Cyber-Warfare-History-Implications-on.pdf>)

118. The Joint Chiefs of Staff, “The National Military Strategy of the United States of America,” 2004. (<https://nssarchive.us/wp-content/uploads/library/nms/nms2004>); Michael Warner, “US Cyber Command’s First Decade,” *Hoover Institution*, 2008. (https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf)

119. U.S. Department of Defense, “National Military Strategy for Cyberspace Operations (NMS-CO),” December 11, 2005. (<https://nssarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf>)

defending DoD information systems and the nation from significant cyberattacks.¹²⁰

CYBERCOM inherited the missions of defending DoD information systems, supporting joint force commanders in cyberspace, and advancing national interests in and through cyberspace. The services became responsible for force generation and force development. They also developed their own components responsible for information and cyber operations in support of operations in their respective warfighting domains.

In 2018, the president ordered the elevation of CYBERCOM to a unified combatant command. Compared to a sub-unified command, each unified combatant command has additional support mechanisms, a direct line of communication to the secretary of defense through a four-star general, greater authority to request budgetary resources, and a distinct geographical or functional responsibility.¹²¹ CYBERCOM also has dedicated combatant command staff, mirroring the organizational structure of the Joint Staff at the Pentagon.

In parallel, CYBERCOM gained additional authorities to conduct military cyberspace operations short of armed conflict to persistently engage and contest adversaries outside of DoD-controlled cyberspace. In FY 2012, the NDAA affirmed that DoD can conduct

offensive operations in cyberspace “subject to the ... legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and the War Powers Resolution.”¹²²

The FY 2019 NDAA stated that clandestine cyber operations may be launched short of hostilities. The law also gave DoD the authority “to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter” in response to “an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes.” The law further authorized CYBERCOM to disrupt and respond to attacks in cyberspace, redefining cyber as a “traditional military activity.”¹²³

These new authorities largely aligned with the Trump administration’s National Security Presidential Memorandum-13, which officials say streamlined the process for authorizing military cyber operations.¹²⁴ These changes also coincided with CYBERCOM’s publication of its first command vision, “Achieve and Maintain Cyberspace Superiority,” as well as DoD’s release of the 2018 DoD Cyber Strategy.¹²⁵

Finally, in the FY 2022 NDAA, Congress granted CYBERCOM Enhanced Budgetary Control (EBC). These authorities will take full effect in 2024, allowing

120. U.S. Cyber Command, Public Affairs, “Cyber 101 - US Cyber Command History,” *U.S. Cyber Command*, October 4, 2022. (Archived version available at <https://web.archive.org/web/20221011152417/https://www.cybercom.mil/Media/News/Article/3179270/cyber-101-us-cyber-command-history>)

121. Andrew Feickert, “The Unified Command Plan and Combatant Commands: Background and Issues for Congress,” *Congressional Research Service*, updated January 3, 2013. (<https://crsreports.congress.gov/product/pdf/R/R42077/11>)

122. National Defense Authorization Act for Fiscal Year 2012, Pub. L. 112-81, 125 Stat. 1551, §954. (<https://www.congress.gov/bill/112th-congress/house-bill/1540>)

123. Catherine A. Theohary, “Defense Primer: Cyberspace Operations,” *Congressional Research Service*, updated December 14, 2022. (<https://sgp.fas.org/crs/natsec/IF10537.pdf>); Robert Chesney, “The Law of Military Cyber Operations and the New NDAA,” *Lawfare*, July 26, 2018. (<https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa>)

124. Mark Pomerleau, “What good are ‘exceptional’ cyber capabilities without authority?” *C4ISRNET*, July 16, 2019. (<https://www.c4isrnet.com/dod/2019/07/16/what-good-are-exceptional-cyber-capabilities-without-authority>)

125. U.S. Cyber Command, “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command,” April 2018. (<https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf>); U.S. Department of Defense, “Cyber Strategy: Summary,” September 18, 2018. (https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF)

CYBERCOM to directly control resources for equipping the Cyber Mission Force.¹²⁶ As General Paul Nakasone testified to Congress in March 2023, the objective is to better harmonize CYBERCOM's responsibilities and cyberspace operations by providing the command with control over funding for major acquisition programs that the services were previously directing. In anticipation of these responsibilities, CYBERCOM has stood up a joint cyber weapons program management office.¹²⁷

In 2022, the secretary of defense elevated the CNMF (within CYBERCOM) to a sub-unified combatant command, providing it with additional authorities and responsibilities. After more than a decade, CYBERCOM now has the Traditional Military Activities authority to conduct overt and clandestine action in support of U.S. armed conflict.¹²⁸ CYBERCOM also has acquisition authority and statutory responsibility for managing its personnel.

126. Paul M. Nakasone, "2023 Posture Statement of General Paul M. Nakasone," *U.S. Cyber Command*, March 7, 2023. (<https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone>)

127. Mark Pomerleau, "Cyber Command prepares to gain significant budget control," *FedScoop*, March 14, 2022. (<https://fedscoop.com/cyber-command-budget-control-preparations-pom>); Alexandra Lohr, "CYBERCOM Acquisition has the money, now it needs the manpower," *Federal News Network*, May 8, 2023. (<https://federalnewsnetwork.com/acquisition/2023/05/cybercom-acquisition-has-the-money-now-it-needs-the-manpower>)

128. Robert Chesney, "Traditional Military Activities in Cyberspace: Clarifying DOD's Authority and the Line Between T10 and T50 Activities?" *Lawfare*, May 9, 2011. (<https://www.lawfaremedia.org/article/traditional-military-activities-cyberspace-clarifying-dods-authority-and-line-between-t10-and-t50>); Paul C. Ney Jr., "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference," *U.S. Department of Defense*, March 2, 2020. (<https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference>)

Acknowledgements

The authors would like to thank Logan Weber, who served as the principal researcher on this study while he was a research analyst at FDD’s Center on Cyber and Technology Innovation. His spadework was critical to the analysis and recommendations in this paper. Additionally, the authors would like to thank Mike Klipstein, Michael McLaughlin, Derek Bernsen, Casey Miller, Alexei Bulazel, Rebecca Lively, Todd Arnold, Shawn Lonergan, and the “operationally brilliant maverick” Navy lieutenant commander for sharing their insights and expertise. The authors also wish to express their deepest gratitude to the men and women, both in and out of uniform, who courageously offered their perspectives, views, and choice words to this report. The nation is indebted to these warfighters trying daily to hold the country’s adversaries at risk and keep us safe in cyberspace. While many experts helped refine the conclusions, any errors in fact or judgment are the authors’ alone. The authors are also grateful to Annie Fixler and John Hardie for their careful edits to the draft and to Erin Blumenthal and Daniel Ackerman for the design and production of this monograph.

About the Authors

Dr. Erica Lonergan (née Borghard) is 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 Departments of Social Science and Electrical Engineering and Computer Science, fellow at the Army Cyber Institute, and executive director of the Rupert H. Johnson Grand Strategy Program. Beyond her academic and research appointments, Erica has an extensive background in strategy and policy. Previously, she was a lead writer of the 2023 U.S. Department of Defense Cyber Strategy and the congressionally mandated Department of Defense Cyber Posture Review. Prior to that, Erica served as a senior director on the Cyberspace Solarium Commission and continues to serve as a senior advisor to CSC 2.0.



RADM (Ret.) Mark Montgomery serves as senior director of FDD’s Center on Cyber and Technology Innovation and as an FDD senior fellow. He also directs CSC 2.0, an initiative that works to implement the recommendations of the congressionally mandated Cyberspace Solarium Commission, where he served as 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. His flag officer assignments included director of operations (J3) at U.S. Pacific Command; commander of Carrier Strike Group 5, embarked on the USS George Washington, stationed in Japan; and deputy director for plans, policy, and strategy (J5) at U.S. European Command.



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)

FDD’s Center on Military and Political Power 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.



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