VOLUME 10 ✧ NUMBER 3 2025

THE CYBER DEFENSE REVIEW

Special Issue USCYBERCOM.Next? The Future of U.S. Cyber Forces

Answer This Before Changing U.S. Cyber Command or Adding a Cyber Service

Vice Adm. (Ret.) Timothy J. White

A New Cyber Service is Not the Answer

Lt. Gen. (Ret.) Charlie Moore

Beyond the Uniform: Reconnecting the Nation's Cyber Force

Cmdr. (Ret.) Christopher Cleary

Reform

Dr. Michael Warner; Maj. Bradley Kramer, Jason Vogt, & Dan Grobarcik;
Dr. Michael Warner & Dr. Emily Goldman; Jason Vogt; Lt. Col. Giancarlo Moats;
Dr. Greg Rattray & Michelle J. Lee

Replace

Maj. Nick Starck & Col. Todd Arnold; Emily Otto;
Dr. Erica D. Lonergan & Maj. Alexander Master;
Maj. Skyler Onken & Dr. Margaret Webber; Dr. Chris Demchak; Dr. Sam J. Tangredi

Guest Editors: Dr. Frank Smith III, Dr. Chris Demchak, Dr. Michael Poznansky

INTRODUCTION
What Comes Next? Alternative Futures for U.S. Cyber Forces

CONCLUSION
Reform or Replace: The Strategic Dilemma of U.S. Cyber Forces

ARMY CYBER INSTITUTE ⋄ WEST POINT PRESS

The Cyber Defense Review

✧ VOLUME 10, NUMBER 3 ✧

Aims and Scope

The Cyber Defense Review is an open-access, peer-reviewed, scholarly journal that serves as a forum for current and emerging research on cyber operations. Its focus is on strategy, operations, tactics, history, ethics, law, and policy in the cyber domain. The Cyber Defense Review positions itself as a leading venue for interdisciplinary work at the intersection of cyber and defense, welcoming contributions from the military, industry, professional, and academic communities.

The journal is committed to publishing original, previously unpublished, and intellectually rigorous research that advances the body of knowledge in this rapidly evolving field. We invite timely and relevant submissions that reflect both theoretical insight and practical application, with the goal of informing cyber-related decision-making, operations, and scholarship. As cyberspace is global, The Cyber Defense Review welcomes and encourages international participation. All submissions must contain unclassified material suitable for unrestricted distribution.

The Cyber Defense Review (ISSN 2474-2120) is published quarterly by West Point Press (westpointpress.com) and hosted by the Army Cyber Institute at West Point (cyber.army.mil).

Submitting to The Cyber Defense Review
For more information about the journal and guidance on how to submit, please see **cyberdefensereview.army.mil**

CONTACT
West Point Press
Taylor Hall, Building 600
West Point, NY 10996
TheCyberDefenseReview@westpoint.edu

Disclaimer: The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute endorsement by United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

This publication of The Cyber Defense Review was designed by Carine Lallemand and Joshua J. Dawson. The Cyber Defense Review is printed by McDonald & Eudy Printers, Inc. Printed on Acid Free paper.

INTRODUCTION

SENIOR LEADER PERSPECTIVES

REFORM

REPLACE

CONCLUSION

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 1-6
https://doi.org/10.55682/cdr/0x37-4mge

EDITORIAL

What Comes Next? Alternative Futures for U.S. Cyber Forces

Introduction to Volume 10 Issue 3

Frank L. Smith III*, Chris C. Demchak, Michael Poznansky

U.S. Naval War College, Newport, RI, USA

U.S. Cyber Command was born to fix a failure. In 2008, the U.S. military failed to detect Buckshot Yankee, a breach of its classified network. In response, Secretary of Defense Robert Gates tasked General Keith Alexander at the National Security Agency to establish and lead USCYBERCOM (Gates 2009). Since then, the Command has grown in size, authority, and autonomy. Its Cyber Mission Force achieved full operational capacity in 2018 and, shortly thereafter, the president delegated additional authorities to USCYBERCOM through the Secretary of Defense (CRS 2025). Congress has also increased its resources, given it greater control over budget and acquisitions, and expanded its freedom of action to conduct offensive and defensive cyberspace operations.

Despite this growth—or perhaps because of it—USCYBERCOM has become an awkward adolescent. Now, more than at any time since its creation, serious questions have been raised about the form, function, and future of this Command. Are its current authorities and capabilities sufficient considering the threat environment and the persistent challenges of recruiting and retaining technical talent? Or is its approach to cyber force generation and employment fundamentally broken? Do the Command and the armed services that provide its forces require only incremental reform? Or is far more radical change required?

These questions are not merely internal or esoteric debates among specialists. From Fort Meade to the Pentagon and Capitol Hill, military leaders and civilian policymakers are seeking

* Corresponding author: frank.smith@usnwc.edu

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Naval War College, the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

rigorous analysis and credible solutions to longstanding problems with the generation and use of cyber forces. From the armed services to the Joint Force, these problems range from persistent shortfalls in training and readiness to the seemingly convoluted command and control of cyber operations.

The recent approval and implementation of "CYBERCOM 2.0"—a revised force generation model—appear to have proceeded in fits and starts (Department of War 2025). Unexpected turnover in the senior ranks has also increased uncertainty. Yet calls for change remain. CYBERCOM 2.0 aims to reform how cyber talent is recruited, trained, and retained. Recent National Defense Authorization Acts likewise mandate changes to both the Command and the services that organize, train, and equip its cyber forces. Behind all of this sits a president who has demonstrated a willingness to change the military in significant ways, as evidenced by the creation of the Space Force during the first Trump administration in 2019.

This special issue of *The Cyber Defense Review* brings together a wide range of research and analytical perspectives to advance the state of debate. Arguments about how to reform or replace USCYBERCOM circulate widely among policy, academic, and practitioner communities. For instance, the Center for Strategic and International Studies recently convened a prominent Commission on U.S. Cyber Force Generation; it treats current shortcomings as a given and examines how best to implement a new service (CSIS 2025). Additional proposals and critiques appear in defense journals and think tank reports (Magee 2025; Couillard 2024; Hodgson and Gates 2025), as well as in the mainstream media (The Washington Post 2025; Winokur Murk 2024). This debate is not limited to the United States. Different countries organize their cyber forces in different ways (Blessing 2021), but some partners and allies grapple with similar challenges (UK Government 2025).

The research articles and professional commentaries in this curated collection examine the most likely paths forward, along with alternative options that merit serious consideration. Several of these contributions draw on research presented during the 2025 Cyber & Innovation Policy Institute Summer Workshop at the U.S. Naval War College, which addressed the question of "CYBERCOM.Next?" Additional contributions are provided by other experts and senior leaders. Some of these contributions are controversial. Taken together, this special issue provides insight and evidence to help you understand—and hopefully answer—pressing questions about what changes are and are not warranted for the future of U.S. cyber forces.

Senior Leader Perspectives

The stakes of this debate are underscored by senior leaders. Drawing on extensive experience, Vice Admiral (Ret.) Timothy J. White examines unresolved questions in his contribution, *Answer This Before Changing U.S. Cyber Command or Adding a Cyber Service*. For Lieutenant General (Ret.) Charlie Moore, there may be problems with USCYBERCOM but, by his account, *A New Cyber Service Is Not the Answer*. Neither the problems nor solutions are confined to the military. To leverage the private sector, Commander (Ret.) Christopher Cleary calls for looking *Beyond the Uniform: Reconnecting the Nation's Cyber Force.*

Status Quo Plus: Slow and Steady Reform?

USCYBERCOM is coming of age in an increasingly mature domain. Military cyberspace has existed for half a century. Even the largely commercial and private Internet that emerged during the early 1990s is now more than 30 years old. It is hard to argue that the U.S. military has not had time to create effective institutions on the grounds that cyberspace is still emerging or too new. Despite their differences, all the authors in this special issue agree that the current status quo for cyber forces can be improved in meaningful ways.

Several authors highlight notable progress in recent years. Dr. Michael Warner points to a positive trajectory in *Evolution of U.S. Cyber Command since 2018*. For instance, while USCYBERCOM draws heavily on infrastructure and expertise at the National Security Agency, the dual-hatted leadership of these organizations facilitates unity of effort between intelligence and warfighting. New authorities and greater autonomy have also made the Command more capable, as evidenced by its performance during crises such as Russia's invasion of Ukraine in 2022. Challenges remain, but organizational progress is real.

One relatively straightforward reform would be to grow the size of available forces. In their article, *"Go Big": Cyber Force Large*, Maj. Brad Kramer, Jason Vogt, and Dan Grobarcik argue that USCYBERCOM is too small for the threat environment. A larger pool of military cyber personnel could mitigate challenges with workforce management and force employment, regardless of whether such growth is accompanied by more radical reorganization.

In *Military Function, Form, and History's Lessons for Cyber Forces*, Dr. Michael Warner and Dr. Emily Goldman underscore the risks of radical reorganization to create a new service or department. They argue that form should follow function, noting that combatant commands do not perform the same function as the armed services. Drawing on historical examples—including the U.S. Air Force and U.S. Special Operations Command—Warner and Goldman question whether sweeping changes to force design would actually address the core purpose of USCYBERCOM.

Wargames, auxiliaries, and exercises offer additional avenues for incremental improvement. In *Gaming Campaigning in Cyberspace*, Jason Vogt demonstrates the utility of operational-level cyber wargames for better decision-making about force structure and resource allocation. Moreover, in his professional commentary, *Support and Leverage Auxiliaries for Stronger Cyber Defense*, Lt. Col. Giancarlo Moats highlights how useful National Guard, Reserve, and other auxiliary units could be, particularly when integrated into exercises that involve foreign and domestic partners.

There is also room for improvement through engagement with the industry. In their commentary, *U.S. Cyber Command Evolution and the Increasing Role of the Private Sector*, Dr. Greg Rattray and Michelle Lee emphasize how much cyber defenses at home and abroad are dominated by commercial industry rather than the military. As a result, USCYBERCOM could address several shortcomings by fostering deeper collaboration with the private sector.

Radical Change Required?

Other contributors find that a patchwork fix is insufficient. From the U.S. Public Health Service to the private sector, Maj. Nick Starck and Col. Todd Arnold open the aperture on different options in their article, *Evaluating Alternative Models for Organizing U.S. Cyber Forces*. As for the military itself, Emily Otto argues that the existing services are structurally misaligned with cyberspace in *Built for Land, Not Cyber*. Doctrine is also misconceived, according to Maj. Skyler Onken and Dr. Margaret Webber in *Reclaiming the Cyber Domain: Revising U.S. Doctrine to Treat Cyberspace as Battlespace and Not a Function*. Not only are cyberspace operations conflated with electronic warfare and information operations, but they are also incorrectly assumed to merely support kinetic force. One potential solution is to create a separate cyber service or military department, similar to the creation of Space Force in 2019 or the Air Force in 1947. That said, creating a new organization will accomplish little if the ethos and ideas that underlie it are still flawed, as argued by the authors of *Why Culture Matters: Organizational Culture and Force Generation for the Cyber Domain*.

Arguments in favor of a separate service or department typically assume that the cyber forces it generates will still be employed by USCYBERCOM. However, in *Breaking the 'Cyber' Cage: Reinventing Cyber Command for Great Systems Conflict*, Dr. Chris Demchak calls for changing the Command to include artificial intelligence, robotic systems, and quantum technologies. Alternatively, in *Bring Cyber to the Tactical Edge: The Case for Decommissioning USCYBERCOM*, Dr. Sam Tangredi explains why preserving this Command could hurt rather than help the services and geographic combatant commands during high-end warfare.

Reform or Replace: The Strategic Dilemma

The range of potential futures for cyber force generation and use is broad—far broader than often assumed. Granted, given organizational inertia, the best predictor of where USCYBERCOM will be tomorrow is where it's at today (Allison and Zelikow 1999). Yet the future of war and emerging technologies are uncertain and indeterminate. Choices remain. The choices made now will shape whether USCYBERCOM matures or struggles for years to come.

To help navigate this decision space, our conclusion identifies the key points of debate and enduring challenges raised in this special issue. We also note how analysts may agree on the diagnosis but differ on the remedy. These tensions and tradeoffs point to productive directions for further research.

ABOUT THE GUEST EDITORS

Dr. Frank L. Smith III is a Professor and Director of the Cyber and Innovation Policy Institute at the U.S. Naval War College. His interdisciplinary research and teaching examine the relationship between emerging technology and international security. Previous work includes his book, *American Biodefense*, the edited volume, *Cyber Wargaming*, and articles published in *Security Studies*, *Social Studies of Science*, *Security Dialogue*, *Health Security*, and *The Lancet*, among others. He has a Ph.D. in political science and a B.S. in biological chemistry, both from the University of Chicago.

Dr. Chris C. Demchak is Grace Hopper Chair of Cyber Security and Senior Cyber Scholar, CIPI, U.S. Naval War College, with degrees in engineering, economics, and comparative complex organization systems /political science. Her long-term expertise focuses on digital surprises disrupting today's complex "socio-technical-economic systems (STES)". She has written on emerging technologies, adversaries' cyber/AI/ML campaigns, virtual wargaming for strategic/organizational learning, and national/enterprise resilience against complex systems surprise. Books of note include: *Wars of Disruption and Resilience* (cybered conflict); *Designing Resilience*; and *Cyber Warfare and Navies (2025*). Articles of note include "China's Maxim (BGP Hijacking, 2018 and update 2021)", "Four Horsemen of AI" (2019), " 'Sea-hacking' Sun Tsu: Deception in Global AI/Cybered Conflict" (2021), and "Achieving Systemic Resilience in a Great Systems Conflict Era" (2022). Works in progress include *Great Systems Conflict: Cyber Westphalia, Warfare, and Collective Operational Resilience*, "Rise of China and Great Systems Conflict", and "Quantum AI Cyber Dancing with Thorns".

Dr. Michael Poznansky is an Associate Professor in the Strategic and Operational Research Department and a core faculty member in the Cyber and Innovation Policy Institute at the U.S. Naval War College. He is the author of *Great Power, Great Responsibility: How the Liberal International Order Shapes US Foreign Policy* (Oxford University Press, 2025) and *In the Shadow of International Law: Secrecy and Regime Change in the Postwar World* (Oxford University Press, 2020). Dr. Poznansky has held fellowships with the Belfer Center at Harvard Kennedy School, the Dickey Center at Dartmouth College, and the Modern War Institute at West Point. He holds a Ph.D. from the University of Virginia.

ACKNOWLEDGMENTS

The authors thank the U.S. Naval War College Foundation for its support of research, education, and engagement through the Cyber & Innovation Policy Institute Summer Workshop series. The authors also thank Todd Arnold, Bob Butler, Patrick Davis, and Carine Lallemand for making this special issue possible.

REFERENCES

Allison, Graham, and Philip Zelikow. 1999. *Essence of Decision: Explaining the Cuban Missile Crisis.* 2nd ed. Reading, MA: Addison-Wesley.

Blessing, Jason. 2021. "The Global Spread of Cyber Forces, 2000–2018." In *Proceedings of the 13th International Conference on Cyber Conflict.* NATO Cooperative Cyber Defence Centre of Excellence. https://www.ccdcoe.org/uploads/2021/05/CyCon_2021_Blessing.pdf.

Couillard, Jeffrey. 2024. "Beyond USCYBERCOM: The Need to Establish a Dedicated U.S. Cyber Military Force." *The Cyber Defense Review* 9 (1). https://cyberdefensereview.army.mil/Portals/6/Documents/2024_Spring/Couillard_CDRV9N1-Spring-2024.pdf.

CRS (Congressional Research Service). 2025. *Defense Primer: U.S. Cyber Command (USCYBERCOM).* June 25, 2025. https://www.congress.gov/crs_external_products/IF/PDF/IF13042/IF13042.1.pdf.

CSIS (Center for Strategic and International Studies). 2025. *CSIS Launches Commission on Cyber Force Generation.* Press release, August 4, 2025. https://www.csis.org/news/csis-launches-commission-cyber-force-generation.

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

Gates, Robert M. 2009. *Memorandum to Secretaries of the Military Departments: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations.* Memorandum, June 23, 2009. https://nsarchive.gwu.edu/document/21425-document-29.

Hodgson, Quentin E., and Susan M. Gates. 2025. *Getting the Fundamentals of Cyberspace Force Readiness Right.* RAND Corporation, August 26, 2025. https://www.rand.org/pubs/perspectives/PEA2761-1.html.

Magee, Aden. 2025. "The Sad and Sorry Tale of Cyber Command's Seven-Year Failure." *War on the Rocks* (September 4, 2025). https://warontherocks.com/2025/09/the-sad-and-sorry-tale-of-cyber-commands-seven-year-failure/.

The Washington Post. 2025. "Trump Makes Pick to Lead NSA Spy Agency after Months of Leadership Limbo." *The Washington Post* (December 16, 2025). https://www.washingtonpost.com/national-security/2025/12/16/nsa-cybercom-joshua-rudd-china/.

UK Government. 2025. *Cyber & Specialist Operations Command—Established to Tackle the Threats of Today and Tomorrow,* September 1, 2025. https://www.gov.uk/government/news/cyber-specialist-operations-command-established-to-tackle-the-threats-of-today-and-tomorrow.

Winokur Murk, Cheryl. 2024. "The Case for and Against Creating a Military Cyber Force." *The Wall Street Journal* (November 29, 2024). https://www.wsj.com/tech/cybersecurity/creating-military-cyber-force-75844bf5.

Senior Leader Perspectives

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 9-14
https://doi.org/10.55682/cdr/jt4h-mvcw

SENIOR LEADER PERSPECTIVE

Answer This Before Changing U.S. Cyber Command or Adding a Cyber Service

Vice Adm. (Ret.) Timothy J. White

As debate intensifies over reorganizing U.S. Cyber Command (USCYBERCOM) or establishing a separate military cyber service, this senior leader perspective argues that structural change should not precede rigorous problem definition and analysis. Drawing on extensive experience commanding joint cyber and intelligence organizations, the author contends that current discussions risk focusing on organizational form rather than mission clarity, readiness baselines, and resource alignment. The article examines unresolved questions about what constitutes "cyber" within the Joint Force, how cyber capabilities are integrated across domains, and how readiness should be measured in a force engaged in continuous competition. It highlights gaps in data regarding manning, training pipelines, and force-generation overhead, cautioning against reorganization without evidence-based assessment. The piece proposes a disciplined, data-driven framework to evaluate mission requirements, readiness, and force design before pursuing major institutional change. It concludes that meaningful improvement in U.S. cyber operational effectiveness depends on answering fundamental questions first—rather than accepting years of disruption from premature structural reform.

Keywords: U.S. Cyber Command, USCYBERCOM, cyber force readiness, military cyber organization, joint force integration, cyber strategy and force design

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

Vice Adm. (Ret.) Timothy J. White is a national security practitioner with over 30 years of experience as a strategist and cyber operations expert leading joint military formations and combined intelligence community organizations. Before retiring as a Vice Admiral, he commanded at all levels within the Navy and Joint Service, most recently as the Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet/U.S. Navy Space Command and previously as the Commander, U.S. Cyber National Mission Force (CNMF) at USCYBERCOM. He is the former Director of Intelligence for U.S. Indo-Pacific Command (USINDOPACOM) and has served globally in various combat zones and conflict areas supporting competition dynamics. A 1989 commander-in-chief, U.S. Pacific Fleet (CINCPACFLT) Shiphandler-of-the-Year, he misses his days driving a battleship. He is currently a Professor of the Practice, Naval Warfare Studies Institute, at the Naval Postgraduate School.

I've spent three-plus decades as a warfighter and cyber operations commander, leading organizations from tactical teams to major service and joint commands. Before retiring as a Vice Admiral, I commanded at all levels within the Navy and Joint Service—most recently as Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet/U.S. Navy Space Command/Joint Force Headquarters – Cyber (Navy), and previously as Commander, U.S. Cyber National Mission Force (CNMF) at U.S. Cyber Command (USCYBERCOM). I served as Director of Intelligence for U.S. Indo-Pacific Command (USINDOPACOM) and operated globally in various combat zones and conflict areas, supporting competition dynamics. I say this not to wave my resume, but because what follows comes from the deckplates up—from someone who's had to make the systems run on time, with what we had, while adversaries were actively working against us.

There is much argumentation about the military's cyber readiness posture that is welcome in principle. I would posit that effective organizations regularly question assumptions and effectively ask questions. The current debate about reorganizing USCYBERCOM or establishing a separate cyber service isn't wrong-headed or narrow-minded. The concerns are legitimate. But we're (likely) putting the cart before the horse. I've commanded enough organizations to know that reorganization without understanding your actual problem or having organizational buy-in is a recipe for years of turmoil with nothing to show for it. Before we start moving organizational boxes around or standing up a new military service, we need to address some fundamental questions—questions that, frankly, should have been asked and answered already. Namely, what are the agreed gaps across mission definition, readiness baseline directly linked to combatant commander operational plans, and comprehensive resource allocations informing the already-underway conversation?

WHAT DOES "CYBER" ACTUALLY MEAN?

We need agreement on what "cyber" means for U.S. military because the reality is, we don't have a comprehensive audit of cyber resources across the Department. In its four conventional operational domains – land, sea, air, and space – there is a clear linkage between resources[1] and joint warfighting capacity and capability associated with the structured planning and organized campaigning of operations in said domains. Infantry assault rifles and boots. Ships and submarines. Planes. Satellites. All accounts for terrain. All have defined objectives, basically summed as getting to, and off, the "x." This is not so in cyberspace.

Cyberspace operations – are those offensive actions in and through networks? Network defense and cybersecurity? Cyber-enabled effects integrated with kinetic operations? Information operations? All of the above or an unspecified subset?

This isn't academic. The definition drives everything – structure, training, authorities, resources, and ultimately mission success. An organization optimized for persistent engagement in adversary networks looks different from one solely focused on securing, protecting, and defending the military's infrastructure. Integrating cyber effects into joint operations requires different command relationships than maintaining cyber as a separate stovepipe. Get the mission definition wrong, and everything downstream suffers.

How much cyber capability is embedded in an airborne division, a carrier strike group or submarine ballistic nuclear (SSBN), an expeditionary or global strike wing, and a global positioning system (GPS) or sensor constellation? How dependent are our global logistics networks on cyber-enabled systems? And the strategic question: can we directly link cyber resource allocation to combatant commander campaign objectives and measurable outcomes?

Until we understand the full scope of cyber integration (dependency and vulnerability) across the Joint Force, we're making decisions in the dark (which is what the adversary wants us to do). We are not ready for a serious conversation about organizational structure and the force design and requirements needed to fully sustain the continuum of conflict across all operational phases. There is no getting on or off the conventional "x" without cyberspace.

WHAT IS THE READINESS BASELINE?

USCYBERCOM executes offensive operations, defensive operations, and information operations across the board. The mission set includes defending military networks, supporting the combatant commands, and contributing to national cyber defense. The Cyber Mission Force (CMF) has approximately 6,200 authorized billets organized into about 140 teams across sub-unified commands and service components.

The challenge? Commonly referenced in the public domain over the last several years are a range of numbers that seem to normalize as follows: we're manned at roughly 75 percent—about 4,650 personnel. Only about 30 percent of those assigned are fully trained and certified across all required work roles. That's roughly 1,395 people who are truly ready.

[1] Generally understood to be dollars, people, training pipelines, and acquisition programs

The gap between authorized strength and mission-capable personnel is significant when the operational tempo remains so high and continuous.[2]

Is this gap a structural problem, a resourcing problem, a training problem? Is it the normal friction of building a highly technical force in an emerging domain? How long do 'we' continue to claim "emerging?" Before we can think about providing answers, we ought to ensure context into what the nation needs and clarity about the expectation of mission outcomes and resource commitment.

When I started my career as a surface warfare officer on USS Missouri (BB63), building qualified watch officers, engineering plant technicians, and combat systems operators took time and had washout rates. What was not clear to an ENS was clear to the service: this was part of the conventional force design. In order to generate combat capacity in peacetime, the Joint Force has long recognized and paid the overhead required in training billets, pipeline (ranges and instructors), and time that delivers combat capability on demand. How does USCYBERCOM's "fully-trained" rate compare to conventional forces? Take a Special Operations unit. Take a submarine squadron. Take a B-2 wing. What's their percentage of bodies in seats (fill) vs. qualified bodies in seats (fit) rate? What's the average for the entire Joint Force?

Every community faces similarly unique manning and training challenges. Special operators have attrition rates that would shock people. Aviation and nuclear qualified career fields also have recruit, train, and retain overhead. Cryptologic operations—which I moved into in 1992—had its own pipeline challenges with technical clearances and specialized training that could take years. Is USCYBERCOM's situation demonstrably worse than these communities, or has the force not recognized nor paid for the overhead required to deliver USCYBERCOM capability in the moment?

Granular data should drive assessment and decision. Break down personnel by skill level—apprentice, journeyman, master—across all work roles and team types. Where are the gaps concentrated? This level of detail drives targeted solutions (more quickly achievable) instead of wholesale organizational upheaval (replete with uncertainty and latency).

WHAT SHOULD THE FORCE DESIGN STRUCTURE BE?

Although I am aware this is already being discussed, it is only after we have clarity on mission definition, readiness baselines, and resource allocations that we can assess whether structural change is warranted. Should it be warranted, advocates for a separate cyber service ought to specify precisely what functions that service would fulfill that USCYBERCOM can't accomplish now. Do we need a separate service to achieve standardization, or can existing Title 10 authorities and joint processes get us there?

[2] These numbers are estimates, dated, and worst-case. In all likelihood, present values are improved.

A lesson we have observed and learned repeatedly is that success in cyberspace does not come alone or in isolation. We must account for the deeply interconnected operational and intelligence deconfliction requirement. Inter-service coordination mechanisms deserve attention. Common standards across type commanders, resource sponsors, and systems commands would improve integration regardless of organizational structure. Unique among other Article II federal departments and agencies, the military Department can actually impose common, standard, and uniform force generation policies across the traditional services.

Is the sticking point force generation? Operational command relationships? Acquisition authorities? Career management? Reorganization is expensive – time, resources, organizational energy, operational focus – and disruptive. The joint nature of cyberspace operations complicates this. Unlike traditional domains where services present forces to joint commanders, cyber operations often require synchronized action across geographic boundaries, organizational seams, and multiple authority structures simultaneously. USCYBERCOM is fully engaged in the present; there is no luxury of future demand.

WHAT SHOULD GUIDE THIS ANALYSIS

First, it must be data-driven. I've sat through too many flag-level discussions where strong opinions substituted for hard evidence. Show me the numbers. Show me the comparative analysis. Show me where the specific failures are and the subsequent root-cause assessment as if this were an aviation mishap investigation; not about blame, all about explanation.

Deliver on the following fundamental and baseline tasks:

- Affirm commitment to the current Five-pillar National Cybersecurity Strategy, and the supporting strategy of persistent engagement, defend forward, and resilience.
- Establish expectations for sustained, continuous engagement across all operational phases[3] with a recognized overwhelming majority level and weight of effort occurring in Phase Zero. Generally, this means that while the overwhelming majority of the military's maneuver forces are "in garrison," the cyber forces are continuously engaged in maneuver operations and continuous campaigning.
- Codify and clarify a host of present and parallel topics related to the employment of the military's cyber forces and its traditional armed forces' activities. For example, these may include the mission of critical infrastructure defense in the homeland, constrained or expanded rules of engagement, development and authorization of 'cyber' letters of marque and reprisal in support of either hack back or hack ahead operations, etc.
- Ensure the Pentagon identifies all: (i) resources (billets and programs), (ii) organizations with specified cyber work roles and associated MF&T, (iii) affiliated, specified, or implied training infrastructure and pipeline, and (iv) the assigned, apportioned, allocated, or

[3] Generally understood to be the "war college" definition: Phase 0: Shape, Phase I: Deter, Phase II: Seize Initiative, Phase III: Dominate, Phase IV: Stabilize, and Phase V: Enable Civil Authority

aligned budget from within the annual approximate $1 trillion military budget. These four elements – as a minimum – should map to the Guidance for Employment of the Force (GEF), the Global Force Management Implementation Guidance (GFMIG), the Joint Strategic Capabilities Plan (JSCP), and the Unified Command Plan (UCP). There may be better or more current governing guidance; use that.

Second, any organizational change must demonstrably improve mission accomplishment. Administrative efficiency is nice, but operational effectiveness is what matters and results from a standard campaign analysis and assessment.

Third, account for implementation costs and transition risk. Standing up a new service is a multi-year evolution that consumes enormous institutional energy. What missions aren't getting attention while we reorganize? What adversary opportunities are we creating by being inwardly focused?

Fourth, solutions must be adaptable. The threat is accelerating. Technology is disrupting. Our tactics and techniques are necessarily and dynamically evolving. Any organizational structure we create needs to accommodate change rather than ossifying around current conditions and service structures. While ossification shouldn't result in organizational change for organizational change's sake, astute readers will recognize that my writing on this topic is an implicit endorsement of the exercise at large.

BOTTOM LINE

I've commanded organizations in contact with adversaries who probe us continuously. I've watched cyber operators perform brilliantly under pressure and deliver effects that matter. I've also watched organizational turbulence degrade readiness and distract from mission. Among the worst things we could do is initiate a major reorganization absent a clearly identified problem, with no specified objective(s), based on incomplete analysis, just to create years of disruption that detract from operational readiness and mission outcomes. USCYBERCOM's challenges are real. Resource constraints, manning shortfalls, and readiness gaps demand attention and solutions. I'm not recommending against change—I'm arguing for disciplined analysis to inform full speed ahead.

This is the data required to begin the analysis that delivers the evidence necessary to improve operational capacity and capability. We have an opportunity to close gaps between where our military forces are and where the nation needs them to be. Whether achieving the mission requires a separate service and its own department, a separate service within an existing department (and not necessarily the Department of the Army), or better resourcing within current frameworks is an open question.

My recommendation remains: ask and answer the fundamental questions first.

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 15-19
https://doi.org/10.55682/cdr/ve1a-bp2c

SENIOR LEADER PERSPECTIVE

A New Cyber Service is Not the Answer

Lt. Gen. (Ret.) Charlie Moore

Debate over establishing a separate U.S. military Cyber Service has intensified as cyber threats grow in scale, speed, and strategic impact. Drawing on decades of senior leadership experience and recent operational reforms, this Senior Leader Perspective argues that creating a new Cyber Service would be costly, slow, and counterproductive. Instead, it contends that U.S. Cyber Command (USCYBERCOM) already possesses—and is now expanding—the authorities necessary to organize, train, equip, and employ cyber forces effectively. The article explains why cyberspace differs fundamentally from traditional warfighting domains, requiring joint integration across all services rather than separation into a standalone bureaucracy. It assesses recent gains in manning, training authority, acquisition flexibility, and operational readiness, and warns that a new Service would duplicate functions, disrupt momentum, and divert scarce talent and resources. The piece concludes that empowering USCYBERCOM to fully execute its existing authorities is the fastest, least risky, and most effective path to maintaining cyber superiority in an era of persistent conflict.

Keywords: U.S. Cyber Command, USCYBERCOM, cyber force development, military cyber organization, joint cyber operations, defense cyber strategy

***Disclaimer:** The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

Lt. Gen. (Ret.) Charlie Moore is a retired U.S. Air Force Lieutenant General and one of the nation's most influential cyber leaders and aviators. Prior to retiring after a 33-year career, he served as Deputy Commander, U.S. Cyber Command, where he and the Commander reported directly to the President and Secretary of Defense on the planning and execution of global cyberspace operations. He also commanded two Fighter Wings, a combat operations group, and a fighter squadron. General Moore has more than 3,000 flight hours in 13 aircraft, including 640 combat hours in the F-16, and participated in Operations Southern Watch, Joint Forge, Iraqi Freedom, Inherent Resolve, and Enduring Freedom. His cyber leadership spanned the defense of the 2018 and 2020 U.S. elections, the responses to the SolarWinds, Colonial Pipeline, and Log4j compromises, and DoD's cyber support to Ukraine and other international crises. He is a graduate of the U.S. Air Force Academy, holds advanced degrees from Troy State University and Air University, and was a National Defense Fellow at Harvard University's Weatherhead Center for International Affairs. He currently serves as a Distinguished Visiting Professor at Vanderbilt University and as an advisor on cyber and national defense issues.

Cyber threats and capabilities are increasing in frequency and complexity at an unprecedented rate. To counter and prevail over current and future threats to our nation, the U.S. military must continue to improve the design, development, and deployment of the most capable cyber force in the shortest time possible. While some believe establishing a cyber service is the answer, the threats to our nation are too great, the costs are too high, and the results can be achieved more quickly by using the authorities U.S. Cyber Command (USCYBERCOM) already possesses.

Influence operations, ransomware attacks, and intrusions into critical infrastructure represent recent examples of the increasing threat malicious cyber actors pose to our national security. USCYBERCOM has responded to these threats by conducting operations continuously and building closer partnerships across the public and private sectors. Recognizing the capacity and capabilities that military cyber forces bring to continuous campaigning against our adversaries, the Command was granted new authorities. These include the power to establish training and certification standards for all of the military's cyber operations forces and broader acquisition and budgeting powers allowing USCYBERCOM to manage and execute its own budget and run acquisition programs tailored to developing cyber capabilities in a rapidly changing environment. Despite these successes and improvements, concerns remain about the Command's ability to field enough ready forces to meet the nation's requirements. Simply put, in the past, some of the military services have not kept pace with providing USCYBERCOM with the trained personnel required for sustained mission success.

One option to address this shortfall is the creation of a new cyber service, force, or department to organize, man, train, and equip forces for USCYBERCOM. This approach fits comfortably within the Pentagon's traditional processes and, over time, may improve staffing levels by creating an organization focused solely on recruitment, career development, and retention of cyber personnel. Cyber service cadre would also become the cyber experts inside the Pentagon, advocating for the military's cyber needs. But the proposal to create a new cyber service or cyber force—while well-intentioned—is not the most effective, efficient, or lowest-risk approach. To be blunt, this solution lacks imagination. Falling back on traditional Department of War structures without fully understanding the unique nature of the domain, the distinctive aspects of cyber warfighting, the latest changes in authorities, and the organizational constructs within the military leads us to improper conclusions and misguided solutions. Ultimately, meeting the demands of modern cyber conflict will require collaboration with private-sector talent; however, that collaboration will only succeed if the Department organizes its corps of cyber warriors properly.

First and foremost, we must recognize that the cyber environment is unlike any warfighting domain the U.S. military has ever seen. Cyberspace has become ubiquitous, and cyber operations are fundamental to the success of all military operations. Cyber superiority is not a "nice to have" feature or simply a way to enhance air, land, sea, and space operations—it is required for success in any of those domains, especially against sophisticated adversaries like China. We must stop thinking about cyber as something distinct and separable from the other warfighting domains and instead understand that it is inherently and inextricably linked to success across all of them. This requires a Department-wide cyber culture—not a new, individual service one.

Additionally, USCYBERCOM requires cyber warriors from each of the services who understand the unique aspects of their respective domains and can provide offensive and defensive capabilities to support those specific warfighting requirements. At the same time, we need cyber warriors filling joint cyber positions who can execute the missions assigned to this functional command by the President and the Secretary and in support of other combatant commands. These efforts must all occur under the broad oversight of the USCYBERCOM Commander, who is responsible for defending the Department's information networks and synchronizing full-spectrum cyber operations. Where would a new cyber service fit in this model?

Proponents of a new cyber service claim it could serve an administrative function—improving organizing, training, and equipping of the cyber forces that would be employed across the Department. But in doing so, it would supersede the new responsibilities that USCYBERCOM has just begun to implement. With the passage of the defense appropriation for FY2024, the Command gained broader acquisition and budgeting authorities. These new powers allow USCYBERCOM to fully manage and execute its budget, develop cyber-specific tools/weapons, and quickly procure necessary technologies. Congress and the Department granted these authorities to provide the Command greater agility and responsiveness in the rapidly evolving cyber domain.

Moreover, we cannot just consider budgeting and acquisition issues—we must also look at organization and personnel. Within the military, "organizing" refers to arranging units into formations with defined command structures and tasks. The services organize their "retained" cyber forces to meet their needs, but the forces presented to USCYBERCOM are organized into mission teams or task forces by the combatant commander, based on operational requirements. Furthermore, unlike the other domains and their respective personnel, these teams and task forces do not return to their services for reconstitution or training. Because cyberspace is a domain of persistent conflict, USCYBERCOM already manages traditional service functions. Once forces are assigned to the Command, the commander trains, commands, and reconstitutes them. In this operational model, a cyber service would have no retained forces—hence, no meaningful organizing duties.

While it is true that manning levels at USCYBERCOM have historically failed to meet mission requirements, no one has accepted that status quo. Thanks to focused leadership from the Command and its service partners, manning levels have reached new highs: Army 84%, Navy 85%, Marine Corps 91%, and Air Force 85% as of July 2025. These improvements did not happen by accident. Working with the services, USCYBERCOM has driven significant changes in recruitment, career development, and retention. This includes increased enlistment and re-enlistment bonuses, the establishment of warrant officer positions, and reforms in career progression and assignments. The result has been significant improvements in staffing levels over the last several years.

However, even with all that success, challenges have continued in training. Fortunately, as of July 24, 2025, USCYBERCOM has finally been granted full training authority over an expanded definition of the military's cyber operations forces (COF). This expanded authority, granted by the Secretary, includes but is not limited to all USCYBERCOM assigned forces, service-retained cyber forces, Department business and assessment elements, cyber operations intelligence units, joint cyber centers, and other combatant command assigned cyber operations forces. With this expanded authority, the Commander of USCYBERCOM can finally execute joint cyber training responsibilities as originally intended and granted by the President. This means that the Command will dictate the baseline training and certification standards for all military cyber operational forces, bringing about the foundational standardization and interoperability necessary in this ubiquitous domain.

Historically, the biggest bottleneck in training was at the "2000 level"—the intermediate level training received after initial service instruction. Fortunately, that problem has largely been solved. Today, the primary training challenge lies in completing joint qualification requirements (JQRs), which include hands-on evaluations and job-specific training tasks. Previously, JQRs had to be completed during real-world missions, leading to delays and backlogs. However, the maturation of the Persistent Cyber Training Environment (PCTE) now allows much of this training to occur continuously, dramatically accelerating achievement of training readiness requirements.

When looked at holistically, the improvements in manning, training, and acquisition capabilities give USCYBERCOM unprecedented ability to organize, train, and equip the force. These gains are measurable and supported by data. But the question remains, "Could a new cyber service do this better?" Maybe—but we must ask: at what cost, and compared to what alternatives?

Establishing a new cyber service will take years, with no guarantee of success. It would require significant bureaucratic overhead, divert expert personnel from current operations, and consume valuable time and funding—resources we cannot afford to divert. It would also disrupt USCYBERCOM's execution of its new authorities. Further, deciding which responsibilities stay with the Command and which transfer to a new service would invite internal competition and confusion, just as USCYBERCOM is gaining momentum. There are also strategic risks. Funding a new service means either cutting from existing warfighting efforts or seeking substantial budget increases—an unlikely outcome, considering that the Pentagon is already facing tight budgets and Department of Government Efficiency (DOGE) efforts to find ways to save money. Standing up a new service now would create friction, slow operational progress, and dilute focus at the worst possible time. Instead, we need our entire security establishment focused on preparing for strategic conflict with powerful and sophisticated adversaries, not on resolving administrative disputes and building a new bureaucracy.

In summary, a new cyber service risks doing more harm than good. It could exacerbate personnel issues by pulling talent from the field to staff a new headquarters. It could duplicate functions already performed by USCYBERCOM and the services. It could confuse chains of command, delay capability development, and reduce the Department's ability to respond quickly to fast-emerging threats. The development and operational employment of our cyber forces must continue and must keep pace with the capabilities of our adversaries. The fastest, least risky, and most cost-effective way to do this—without disrupting our nation's current cybersecurity posture—is to empower USCYBERCOM to fully execute the authorities it already possesses. The stakes in cybersecurity are too high, and the timeline too urgent, to gamble on structural experiments. A new cyber service is not the answer.

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 21-27
https://doi.org/10.55682/cdr/7zwk-aznp

SENIOR LEADER PERSPECTIVE

Beyond the Uniform: Reconnecting the Nation's Cyber Force

Cmdr. (Ret.) Christopher Cleary

ManTech International, Herndon, VA, USA

The United States faces a structural cyber manpower challenge that cannot be solved through traditional military or Department of War (DoW) force-generation models alone. Drawing on his experience as the Department of the Navy's Principal Cyber Advisor (PCA), CDR (Retired) Christopher Cleary contends that while the nation trains exceptional military cyber operators, it employs only a fraction of its available cyber talent. The article proposes a Cyber Mission Support Framework (CMSF) to reconnect uniformed forces with trusted, highly skilled cyber professionals in the private sector. CMSF enables scalable mission augmentation and, potentially, regulated cyber proxy operations under clear legal and operational oversight. The essay examines why cyber operators leave uniformed service despite continued commitment to national defense, how industry has become a latent reserve of operational expertise, and why existing models are insufficient for future conflict—particularly in high-demand theaters. Ultimately, it argues that reconnecting national government and industry cyber talent is essential to sustaining U.S. cyber readiness and strategic advantage.

Keywords: cyber workforce, mission augmentation, cyber force structure, public–private integration, national cyber readiness, force generation

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

Cmdr. (Ret.) Christopher Cleary is Vice President of the Global Cyber Practice at ManTech International, where he leads strategy and execution across cyber operations, cybersecurity, and national security missions. He brings extensive experience spanning senior government service, military operations, and executive leadership in the commercial cyber sector. Prior to returning to industry, Cleary served as Principal Cyber Advisor to the Secretary of the Navy, advising senior Navy and Marine Corps leadership on cyberspace operations and leading implementation of the Department of Defense Cyber Strategy within the Department of the Navy. He previously served as the Department of the Navy Chief Information Security Officer, overseeing enterprise cybersecurity policy, risk management, and cyber defense. A retired Naval Reserve Officer, Cleary served 24 years in operational and leadership roles, including assignments with U.S. Cyber Command. He is a graduate of the U.S. Naval Academy and the Naval War College, and currently serves as President of the Military Cyber Professionals Association.

During my time as the Principal Cyber Advisor (PCA) for the Department of the Navy, I came to the conclusion that the Navy and Marine Corps were trying to fight a 21st-century cyber fight with a 20th-century manpower model. Our most pressing cyber problem was structural; we had built a force that could not scale at the rate the evolution of the cyber threat environment demanded. The gap between expanding operational demand and the number of trained operators serving in the military was widening, not narrowing.

Out of my experience came the ideas for a Cyber Mission Support Framework (CMSF), a structure to orchestrate the scaling up of the U.S. military cyber force. The CMSF would enable two practical paths to mobilizing the full national cyber workforce: “mission augmentation” by bringing in external industry cyber personnel, and modern “cyber proxies” permitted with guidance to conduct the equivalent of modern cyber privateering. The rationale is that the U.S. already has the cyber talent it needs to meet its mission demands, it just does not have all of that talent inside the military.

Mission augmentation is the more immediate and conservative option, using vetted, cleared, highly experienced industry teams and capabilities to reinforce government cyber operations at the points where existing forces are saturated or outpaced. Modern cyber proxies is the more ambitious and yet historically grounded idea, enabling authorized private teams to conduct narrowly defined cyber operations in support of national objectives with government control or oversight. When I left the Navy, it was clear to me that without approaches like these, we risked entering the next major conflict at an operational disadvantage, not because our forces lacked skill, but because we lacked enough of them.

Mission augmentation and cyber proxies should be viewed today as necessary instruments of national power. The underlying argument is simply that we must build the mechanisms to reconnect the full spectrum talent we already have in government and industry, or we will continue to fight with only a fraction of the trained force available. This essay explains why Sailors and Marines continue to leave cyber roles despite believing in the mission; how the private sector has inadvertently become a reservoir of trusted, trained cyber operators; why organizations like the Military Cyber Professionals Association are indicators of national potential rather than evidence of loss; and why commands in theaters like the Indo-Pacific cannot rely solely on existing force generation models to withstand the opening cyber pressures of a future conflict.

Working in the Department of the Navy, I learned quickly that every readiness discussion circled back to the same uncomfortable truth: we simply did not have enough trained operators to meet the missions we were already executing, let alone new ones that were coming. The Navy and Marine Corps were committed to growing the force, and we spent years attempting to modernize career paths that were designed for a different era. Creating cyber designators, building a path that could retain technical talent, convincing promotion boards that operational value did not always look like traditional sea-shore rotation - all of it was necessary and all of it was progress. Yet none of it moved fast or far enough to close the gap.

I watched Sailors and Marines who loved the mission come to a crossroads where the institution simply failed to show them a professionally rewarding future. Their departure was not always about the personnel system in a bureaucratic sense; it was often about identity, purpose, and the overarching service's inconsistent articulation of what these operators were supposed to become. We were asking recruits to master an entirely new operational discipline, but we struggled to show them why their work was important or where that discipline fit inside the larger warfighting construct. But even with reforms, the broader service still struggles to fully integrate cyber operators into its self-conception. This disconnect matters. When cyber operators cannot see how their capabilities are valued or when the path from operator to leader feels uncertain, they look elsewhere. The irony is that these individuals still believe deeply in the mission. They do not drift from national service; they drift from an organizational structure that has not always made room for them.

The problem is not a simple readiness shortfall; it is a structural blind spot. We train an exceptional workforce, but we are only willing to use part of it. The rest, the majority of it, is thriving in industry, often with access to better tools, broader experience, and greater technical depth than when they wore the uniform. I spent years, working within the system, to build a sustainable workforce for the Navy before fully appreciating that the broader workforce already existed outside it. We simply had no mechanism to reconnect those people to national missions when the need arose. If we could not grow enough cyber operators inside the building, perhaps the answer was to recognize that the force available extended beyond the building.

The United States has now reached a point where ignoring that reality has real strategic consequences. We continue to train cyber operators as if time is on our side, as if adversaries will wait patiently for us to produce the workforce required to match them. They will not.

China recruits cyber talent at a scale we cannot replicate inside government pipelines. Russia pulls from a criminal ecosystem that functions as an auxiliary force whenever it needs one. Iran and North Korea mobilize technically literate citizens by compulsion when necessary. The U.S., bound by higher standards and a slower personnel system, cannot simply “catch up” by building more schoolhouses or creating more billets.

And yet, unlike our adversaries, we have something they do not, a large population of trusted cyber operators working in the private sector. They did not stop being who they were when they left. In many cases, they improved. They learned new technologies, worked on problems unavailable inside government, matured technically and operationally, and became part of an ecosystem that oftentimes moves faster than federal programs. Our mistake has been treating those people as a loss rather than as available national depth accessible with the proper structural innovations.

Organizations like the Military Cyber Professionals Association present a view of the real opportunities to maximize the skills and abilities of the total military cyber population - in and out of uniform. This association brings together former operators, instructors, analysts, planners, reservists, and technical specialists who helped build the Cyber Mission Force (CMF) and the service cyber components. These individuals remain deeply connected to the mission and maintain operational mindsets long after leaving government service. They volunteer to train others, swap tradecraft, and sustain the community’s culture. This is not a dispersed, unreachable diaspora. It is a latent national cyber reserve—self-identified, self-motivated, and structurally untouched by existing government mechanisms. The talent problem is not a lack of talent. It is the absence of a bridge to that surrounding community.

It is important to acknowledge that these ideas are being explored at the same time as an active debate over the creation of an independent cyber service. That discussion reflects a shared recognition that existing structures are insufficient for the demands of the domain, and it is both necessary and overdue. The concepts outlined here are not a substitute for that effort, but a parallel path, one that addresses immediate operational scale and readiness challenges regardless of how the long-term service-level question is ultimately resolved.

CYBER MISSION SUPPORT FRAMEWORK (CMSF): THE MISSING LAYER OF U.S. CYBER FORCE STRUCTURE

A practical mechanism for harnessing this broader workforce is the Cyber Mission Support Framework (CMSF). CMSF is the structured model that defines how the government can lawfully, predictably, and rapidly integrate civilian cyber expertise into federal missions. It is not contracting as usual, and it is not ad hoc surge support. CMSF provides a force generation model that integrates uniformed forces, government civilians, and the tens of thousands of highly trained cyber professionals working in the private sector. It recognizes that national cyber power is distributed, not centralized, and that the U.S. must build a repeatable way to mobilize that power when required. CMSF, properly implemented, becomes the missing layer of U.S. cyber force structure, the mechanism that transforms a talented but untapped civilian workforce into a coherent national asset.

Operationally, CMSF establishes a standing pool of pre-cleared, continuously vetted cyber professionals whose skills align with government mission sets, defensive operations, threat hunting, operational technology security, exploit development, or target analysis. These individuals remain in the private sector but maintain readiness standards appropriate to their role, similar in spirit to the reserve components supporting other warfighting domains. They can be activated rapidly because they never lose their operational currency.

Legally, CMSF provides the defined authorities, oversight structures, and reporting mechanisms needed to integrate civilian teams into military or federal cyber operations. It clarifies their status under U.S. law and international norms, specifying when they are acting in support of national defense, what boundaries govern their actions, and how liability and accountability are enforced. CMSF ensures the government does not improvise legal authorities under crisis; it builds them in advance, in peacetime, with transparency and discipline.

Strategically, CMSF provides the scalability that traditional training pipelines cannot achieve. Because the framework is built around an expandable pool of civilian talent, the government can grow capacity without expanding billets or building new organizations. CMSF creates a ladder of responsibility: at the lowest tier, embedded support to existing government teams; at a middle tier, outcome-based mission execution; and at the highest tier, fully authorized auxiliary "proxy" operations, a step short of modern cyber privateering. It is the bridge that makes privateering viable, legal, and governable.

If the U.S. is going to present mission augmentation, or ultimately auxiliary/proxy constructs, as credible instruments of national power, the organizations involved must demonstrate more than technical skill. They must prove they can function as operational entities. They must be able to plan coherent cyber operations that align effects with the commander’s intent, understand intelligence gain/loss, and frame risk in ways senior leaders can act on. They must be able to coordinate, synchronize, and deconflict with government forces, working within established authorities, participating in joint targeting cycles, and ensuring that their operations don’t collide with existing activity. They must show measurable performance, mission impact expressed through clear measures of effectiveness, measures of performance, response timelines, recovery outcomes, access persistence, cost avoidance, or any other metric that demonstrates operational value. And they must show how this scales. Demonstrating how a cadre becomes a reserve, how a reserve becomes a network, and how that network maintains readiness will determine whether augmentation becomes policy or remains a thought experiment. A single successful team is interesting; a repeatable, expandable model is transformative.

To make augmentation viable, the Pentagon must embrace a proactive, continuous vetting model. The key to immediate integration is continuous program access and trust. This continuity requires creating a new personnel status, perhaps akin to a cyber equivalent of the Individual Mobilization Augmentee (IMA) program for cleared industry personnel. The government must be willing to sponsor and sustain existing security clearances for these teams. In turn, they must fully participate in mandatory, no-notice operational readiness drills and maintain strict compliance with defined security protocols.

This model shifts the burden from relying solely on government-owned billets to leveraging industry-held capacity. The government must establish secure mechanisms, such as designated and pre-approved sensitive compartmented information facilities (SCIFs) within partner industry locations or dedicated deployable tactical SCIFs, allowing these vetted teams to integrate classified operations without sacrificing security integrity. Augmentation isn't just contracting for staff; it is establishing a trusted, standing reserve of capability that can be activated on an accelerated timeline.

As the CMSF matures, it can extend naturally into a more ambitious construct rooted in American history: modern cyber privateering as proxy forces. As a practical mechanism, it means delegating tightly bound mission authority to private entities staffed largely by former government operators. The U.S. Constitution explicitly empowers Congress to issue letters of marque. The Geneva Conventions and the Tallinn Manual outline conditions under which civilians may lawfully participate in conflict under state authorization. The U.S. has relied on auxiliaries many times: privateers, civilian pilots in World War II, and state-approved maritime security. Only the domain has changed.

Cyber proxies in the form of privateers or active auxiliaries would allow certain operations, against sanctioned-state infrastructure, cybercrime networks, or other pre-authorized adversary systems, to be executed by independent but regulated teams operating under government oversight. Unlike traditional contracting, these teams could shoulder part of the readiness burden themselves, offsetting cost through seized assets or repurposed infrastructure. A cryptocurrency wallet used to finance hostile operations could be seized and split under statutory direction. A botnet attacking U.S. ports could be dismantled, with its infrastructure repurposed for training. The financial model encourages readiness without requiring constant government funding while preserving accountability and lawful control.

For this concept to move from theory to national instrument, the legal and policy framework must be robust and transparent. This will require new legislation or a highly defined Executive Order to accomplish three key objectives.

First, authority and scope must be defined with clear policies. The government must specify the precise nature of permissible actions, disruption, collection, asset seizure, and the adversary or geographical boundaries in which they may be applied. A review body, perhaps a cyber marque commission, must be empowered to issue, evaluate, and revoke these authorities.

Second, strict rules of engagement must govern operations. Privateering teams cannot operate as free agents. Their actions must be bound by auditable reporting mechanisms and real-time government oversight to ensure they remain aligned with national strategy and do not unintentionally escalate conflict.

Third, liability and accountability must be unambiguous. Operators acting within authorized bounds must receive appropriate legal protection, while actions beyond those limits must result in immediate revocation and legal consequences. This balance of protection and accountability ensures discipline, predictability, and professionalism.

Critics warn about escalation or unpredictability, but those concerns misunderstand the framework. These teams would not be freelancers or vigilantes. They would be authorized, monitored, held to defined boundaries, required to report, and aligned to national strategy. Their freedom of maneuver would not come from ambiguity but from carefully constructed authority—just enough autonomy to act at the speed the domain demands, but not enough to jeopardize stability or national objectives.

The reality is simple: the U.S. will never have enough cyber operators inside government to meet every mission demand. That is not a critique; it is a condition of the domain. But the U.S. already has enough cyber operators when it considers the full national workforce. The talent does not need to be recreated. It needs to be reconnected. What I saw at the Department of the Navy convinced me that the military can no longer rely solely on internal force-generation models. The people we need are already out there—trained by us, trusted by us, still committed to the mission. Industry is not a separate ecosystem. It is the second half of our cyber workforce. Recognizing that fact, and building the mechanisms to act on it, may be the determining factor in whether the United States enters the next conflict prepared or outmatched.

✧ Reform ✧

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 31-39
https://doi.org/10.55682/cdr/yxsr-e85e

RESEARCH ARTICLE

Evolution of U.S. Cyber Command since 2018

Michael Warner

U.S. Cyber Command, Fort Meade, MD, USA

Much has changed at United States Cyber Command (USCYBERCOM) since it became a unified combatant command in 2018. Created in 2010 and elevated to full unified status eight years later, the command underwent substantial evolution from the outset in the ways it designed, developed, and employed its forces. Those changes came at the dictation of operational experience, with leaders learning what worked—and did not—from mission outcomes, while learning how to sustain success and mitigate negative results. Although USCYBERCOM is not fully built out, the command is more capable, more ready, and more often sought as a partner by domestic and allied operational entities. Today it does everything it could do in 2018, and many things it could not do then. These changes occurred as a result of several factors, including leadership continuity, tactical innovation, and operational flexibility. That flexibility, however, bespeaks larger constraints—or competitions for resources and focus—that may one day limit the command's potential capacity. As the nation considers the organization of cyber forces, USCYBERCOM's successful functions would have to be employed—or re-created—in whatever organizational construct performs military functions in cyberspace for the United States.

Keywords: U.S. Cyber Command, USCYBERCOM, cyber conflict, cyber operations, force evolution

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

U.S. Cyber Command (USCYBERCOM) came of age in May 2018, with its elevation to be the Joint Force's tenth unified Combatant Command. Much has changed since then, but much has remained constant as well.

USCYBERCOM's development unfolded according to the prompting of operational experience. Lessons learned by operators on keyboards (and the leaders standing behind them) not only shaped the command's development, but also the progress of cyberspace policy, strategy, and doctrine for the Department, the nation, and its allies.

The Command thus represents an ongoing experiment in not only force employment but also in force generation and force design. As with cyberspace itself, USCYBERCOM's evolution is not yet complete – even if no major conflict in cyberspace intervenes over the next few years to drive more rapid and sweeping changes. As the nation considers the organization of cyber forces, USCYBERCOM's successful functions would have to be employed—or re-created—in whatever organizational construct performs military functions in cyberspace for the United States.

The history to follow seeks to inform any such reconsideration of how the U.S. military organizes its cyberspace capabilities. Current debates over such topics sometimes proceed without reference to the basic facts and chronology. This is not a "case study" to verify some academic theory of military innovation, or an advocacy brief for some other organization altogether; its methodology follows the art and science of history to establish what has been occurring since 2018 and interpret, where possible, why it did so. Readers are free to cite its findings as they like – but they should be able to agree on the factual outline it presents.

ORIGINS AND CONSTANTS

USCYBERCOM came into existence as a sub-unified command of U.S. Strategic Command (USSTRATCOM) in 2010. Then as now, USSTRATCOM housed the Joint Force's global strike "functions," and cyber capabilities had been within its remit since 2002. The newly created command for cyber functions assembled pre-existing USSTRATCOM joint cyber elements (one offensive, and one defensive) into a four-star component. The new command worked at Fort Meade, Maryland, and so USSTRATCOM headquarters in Nebraska afforded it considerable autonomy. While USCYBERCOM never received the full package of resources validated at its inception, this cloud held a proverbial silver lining for the command. USCYBERCOM leaders building the new component had to improvise and find creative ways to employ the command's modest forces and staff (Warner 2020)

The Command has always operated under several constants. These both enabled and channeled its operational development, and hence its evolution, both before and after 2018.

Foremost among those constants has been the “dual-hat” command arrangement with the National Security Agency (NSA), whose director serves as USCYBERCOM’s commander. The brand new USCYBERCOM in 2010 inherited this relationship between the nation’s military cyberspace operational capacity and its primary signals intelligence and cybersecurity provider—a relationship dating back to 2003 (Warner 2015). The dual-hat proved crucial to the construction of the new command’s capability. For offensive mission support at least, the Command remains dependent on NSA (which now receives real assistance from USCYBERCOM as well), and the unity of effort synergized by the dual-hat arrangement has benefited both organizations – and the nation itself.[1]

Two other, built-in policy and legal constants still affect the Command’s evolution. The U.S. Constitution rightly erected walls to protect the civil liberties and privacy of U.S. persons. Military operations, again rightly, must respect those boundaries, which in effect separate military from law enforcement and administrative functions. This affects cyber operations in foreign space—where it is quite possible to touch the data of U.S. persons or allies—and even on military networks in domestic space. Adversaries in cyberspace, however, care not for our constitutional order. Indeed, they exploit the temporary sanctuary they can gain from American military and law enforcement measures by hopping back and forth across the boundaries of U.S. legal jurisdiction.[2] Such behavior is rarely effective for long in physical space, but in cyberspace a bad actor might require only seconds to accomplish his mission and move on safe from U.S. responses. Even a day or two of operational freedom can allow an adversary to harm national interests. USCYBERCOM, like the rest of the U.S. government, has not solved this problem.

Civil liberties and privacy protections combine with programmatic considerations to complicate the defense of the military’s own networks. The Command directs the operation and defense of the Department’s systems, but not their construction or administration. Individual armed services purchase much of the information technology (IT) of the entire organization, and Pentagon officials program, plan, budget, and authorize the use of that equipment. That means that the officer most accountable for defending the military’s systems—the Commander of USCYBERCOM—sometimes has little say in decisions that embed new risks in those same systems.

[1] The Secretary of Defense and the Director of National Intelligence sponsored a joint study of the dual hat relationship in 2022. The Senior Steering Group’s findings are not public, but have been publicly summarized by various leaders. For instance, Lt. Gen. John D. Caine (U.S. Air Force, retired) cited them in his written answers to confirmation questions from the Senate in March 2025: “The 2022 Joint Study on the Dual-Hat” recommended the dual-hat arrangement not only be maintained but strengthened. I continue to agree with the findings of that study. The dual-hat arrangement provides the ability to look across both organizations and has empowered both USCYBERCOM and NSA to fulfill their missions better than each could do alone. It promotes agility and enables intelligence to be operationalized rapidly. It also facilitates relationships with key foreign allies and partners.” (U.S. Department of Defense 2025)

[2] The Federal Bureau of Investigation (FBI) and U.S. Secret Service handle many of the law enforcement functions in domestic cyberspace, while the Department of Homeland Security (DHS) protects critical infrastructure.

Finally, expertise has always been short. Top cyber talent demands high premiums—which even the U.S. government cannot afford at the scale it requires. This shortage affects the military, the government, industry, and the nation as a whole. Every agency and industry needs a bigger slice of the talent pie, and the pie is growing only slowly. In one regard, however, USCYBERCOM has proved an exception to this rule. It has seen a remarkable continuity in leadership, with many of its leaders having had prior experience overseeing cyberspace missions, and a growing cadre of personnel with fluency in the relevant issues, capabilities, and teams they direct.

EVOLUTION

Having noted what has not changed in USCYBERCOM's institutional environment, we can survey other aspects of the Command that look very different from 2018. In listing the changes, it is important to note why these changes occurred. The causes of change varied, of course, but many stemmed from larger changes in what planners like to call the "threat environment." Leaders in Washington, the Pentagon, and the Joint Force called for increased cyber defenses against increasingly sophisticated hostile actors across a series of international crises. At the same time, they also grew more comfortable employing cyber operations as planners and operators demonstrated competence and delivered results.

To begin with, USCYBERCOM is bigger. In Fiscal Year 2018, it spent $600 million and employed roughly 6,100 military and civilian personnel in its Cyber Mission Force (CMF) and headquarters. Seven fiscal years later, the comparable numbers were almost $3 billion and more than 6,300 people, with the higher budget due primarily to the Command's increased influence over military cyber spending.

The growth in resources paralleled a boost in the Command's administrative authorities. In 2024, USCYBERCOM began exercising "enhanced budget control" over the funds that the services expended to sustain the respective formations that they presented to CMF (Hartman 2025). The Command is hiring staff and building offices to implement these functions. This suite of new powers collectively gives USCYBERCOM a closer resemblance to U.S. Special Operations Command (USSOCOM)—the combatant command that Congress built up into a quasi-service with unique authorities for manning, training, and equipping the nation's special operations forces. USSOCOM was indeed the model for adding comparable (though less extensive) program and budget clout to USCYBERCOM's portfolio.

The Command has also fashioned a fuller organizational structure. In a sign of the confidence that the Department has placed in USCYBERCOM, it now has two sub-unified commands—the Cyber National Mission Force (CNMF) and the Department of Defense Cyberspace Defense Command (DCDC)—which catalyze each other's missions. It also owns a reporting component, Joint Task Force (JTF) Ares.[3] Command components also work with broader operational authorities. These are not so much new as better understood and increasingly synergized; offensive cyberspace missions have been governed by White House guidance issued in 2018, and defensive orders issued by the Command are now standard practice (as opposed to the novelties they once seemed to the Pentagon and the Joint Force (Norton 2020)). It is also building the infrastructure essential to support operations in, through, and across cyberspace (GAO 2020).

A pair of catalytic events drove the acceptance of USCYBERCOM as a preferred partner for cyberspace operations. First came the effort to defend the 2018 mid-term elections from foreign influence and interference. General Paul Nakasone (U.S. Army) had just arrived as commander when he received this task, and he directed that the Command's effort would proceed in concert with NSA's. This arrangement—personified in the NSA and USCYBERCOM co-leads of the Russia Small Group (RSG) that General Nakasone established to defend the elections—set a precedent followed ever since in cyberspace campaigns. USCYBERCOM would act only when and where doing so did not imperil NSA's foreign intelligence mission; and NSA would facilitate the Command's success. The two organizations quickly learned that synchronized efforts produced operational synergy, especially in defending friendly networks. RSG's leaders also found that their combined insights were invaluable to inter-agency, allied, and industry partners, who were pleased to take such cues and act under their own authorities to frustrate pernicious cyber actors (Nakasone 2019b).

The defense of the 2018 mid-terms provided further benefits for the nation. It helped to calm political acrimony over foreign influence in U.S. elections, which is one reason why members of Congress publicly applauded RSG's contributions (Nakashima 2019). Second, the election defense success in 2018 validated the Command's concept for impairing malicious cyber actors and other online adversaries before they penetrated friendly networks or harmed their targets (an approach General Nakasone referred to as "persistent engagement" or "defend forward" (Nakasone 2019a)). This denial of sanctuary in cyberspace for foreign military and intelligence actors helped convince other U.S. government agencies, as well as allies and partners, that sustained operations and collaboration with the Command could boost their own security and would not escalate to armed conflict.

The war in Ukraine marked another learning moment for USCYBERCOM. Russia's mobilization and threats in 2021 prompted concerted actions to harden military information systems (especially in Europe), as well as concerns that a conflict could spread to the North Atlantic Treaty Organization (NATO). The war that followed in 2022 taught the Command and its

[3] CNMF is the commander's Joint Force element; it was created in 2014. DCDC was formerly Joint Force Headquarters-DoD Information Network (JFHQ-DoDIN) until May 2025. In its new, Congressionally mandated form, DCDC "directs cyberspace operations to achieve unified action in the security, operation, and defense of the DoDIN to assure DoD priorities and freedom of maneuver across the competition continuum." JTF-Ares dates to 2016, but has been repurposed from its original, counter-terrorism mission.

partners sobering lessons about the pervasiveness and impact of cyberspace operations—and the importance of collaboration with allies and industry. Command personnel worked to contain the conflict and present options to decision makers; they would re-double such efforts when Israel was attacked by Hamas in October 2023 (Haugh 2024). The cyber "fronts" in both conflicts can be compared with the intensifying drone war over Ukraine. Neither cyber missions nor unmanned vehicles have determined the outcome of these struggles. But they nonetheless demand leadership attention and significant resources – not to mention better intelligence, higher bandwidth, secure systems, electronic agility, and faster innovation and acquisition cycles.

Operational success in these events depended in part on readiness. USCYBERCOM has largely solved this problem (at least the aspects of it more easily measured), which dogged it for several years. CMF teams measure readiness according to criteria analogous to those employed to appraise fighter squadrons and infantry battalions. While the metrics naturally differ, the principle is the same: a commander needs to know whether the force elements assigned to him or her are mission capable (Stanton and Tilton 2020). CMF teams long suffered from the general dearth of talent required to perform DoD's expanding cyber missions, but the services and the Command collaborated over time to expand training opportunities, boost recruitment, and enhance retention rates. As a result, CMF attained foundational (C2) readiness in 2024, and should be able to sustain that level even while expanding the force by the 14 new teams slated to be operating by FY 2028 (Hartman 2025).[4]

WHERE IS USCYBERCOM NOW?

The prospect of a regional conflict precipitating U.S. military intervention recently became real in the Twelve-Day War between Israel and Iran. The Chairman of the Joint Chiefs of Staff publicly commended USCYBERCOM's support to the Joint Force in this affair (Brown, Blakely, and Dawber 2025). A future such contingency, especially in the Pacific, could be more costly and drawn out. This possibility underscores the imperative to balance competing resource demands between planning for contingencies versus engaging current threats that are exploiting U.S. and allied systems today, all while sustaining a reserve for unexpected events—like the Twelve Day War. There is no easy solution to this conundrum for Command leaders. A good answer, therefore, is less a matter of striking the "right" balance, but rather teaching the right people to ask the right questions—and ensuring they hear clear answers—when the next crisis breaks.

USCYBERCOM might enjoy a measure of patience as it navigates the above dilemma. It has successfully defended the military's topline networks from penetration—no mean feat, given the skills of adversaries (witness comparatively recent intrusions in other sensitive

[4] Note that even CMF teams that are not deemed fully ready can and have detailed capable mission elements to reinforce cyber operations led by other teams.

networks, such as the Russian exploitation of several U.S. government systems via SolarWinds software (Nakasone 2021; Konkel 2025)). The Command also played a role in negating the online presence and appeal of terror groups such as al-Qaeda and ISIS—which ran a slick, multi-national media empire only a decade ago (Nakasone 2020).

The long counter-terror fight in cyberspace illustrated a key aspect of USCYBERCOM's operations. The Command has a comparatively light footprint in absolute terms. As a presence in cyberspace, it is dwarfed by other U.S. government entities that perform communications and security functions—and they in turn consume only a fraction of the data and bandwidth used by the corporate search, IT, and social media giants (some of which sponsor activities that more than resemble USCYBERCOM's). The Command's missions must therefore hit the right targets in the right way. USCYBERCOM often has more impact by showing government, industry, and allied partners where they can affect matters in cyberspace. The Command became a locus for other people's counter-terrorism actions, and has continued this operational pattern, where appropriate, in other missions. While it can act, it often enables by prompting others, thus building collaboration and amplifying effects that partners have more authority to deliver. Adversary malicious activity is hampered either way—which is the point of persistent engagement.

USCYBERCOM is also working to grow the capacity of foreign allies and partners. This effort proceeds on three levels. As noted, the Command's persistent engagement approach has garnered attention on several continents and is informing the ways in which various allies build and task their own cyber forces (Pegram and Tinker 2025). Second, USCYBERCOM hosts a growing allied presence in its operational discussions and exercises, learning from partners as they learn from the Command, and practicing the sort of collaboration that could be crucial in a future contingency (U.S. Cyber Command Public Affairs 2024). Finally, USCYBERCOM's cooperative "hunt forward" missions alongside host-nation teams on their national networks contribute to their security while enabling the Command to capture new malware samples and observe adversary tradecraft in the wild (Nakasone and Sulmeyer 2020). All three of these examples of cooperation encourage and prompt a growing range of partners to work more effectively to suppress common adversaries.

WHERE IS USCYBERCOM GOING?

USCYBERCOM is more capable than in 2018. It performs more missions faster, sustains its pace longer, and more often makes opponents respond to its initiatives (rather than only responding to theirs). Today it does everything it could do in 2018, and many things it couldn't do then. These changes occurred as a result of several factors, including leadership continuity, tactical innovation, and operational flexibility. That innovation and flexibility should be viewed not only as causes but as outcomes of the Command's increased organizational maturity. They also, however, bespeak larger constraints—or competitions for resources and focus—that may one day limit the Command's potential capacity (Pomerleau 2025). The fact that the Command has continually had to improvise suggests that cyberspace operations have long been seen as exotic and risky—not to mention have consistently been under-resourced (by the calculations of the Department's own programming officials).

USCYBERCOM's future remains hazy. If the Command is radically altered or even retired, its functions will almost certainly have to be continued in different arrangements. Indeed, there is no likely future in which the U.S. does not require military elements to sustain operations in defense of Joint Force systems and U.S. interests in cyberspace.

If USCYBERCOM has a long future, it will continue to evolve with the dynamics of cyberspace and changing threat pictures. Institutions can live longer if they adapt to their changing environments and continue to demonstrate their value. USCYBERCOM's effective capabilities and successful functions will have to be employed—or re-created—in whatever organizational construct performs military functions in cyberspace for the United States.

ABOUT THE AUTHOR

Dr. Michael Warner serves as the Command Historian at USCYBERCOM. Before arriving at the Command in 2010, he served as an analyst, staff officer, and historian in several agencies of the US Intelligence Community. Dr. Warner has written and lectured widely on intelligence and cyber history, theory, and strategy. He is co-author, with John Childress, of The Use of Force for State Power: History and Future (2020). He also wrote The Rise and Fall of Intelligence: An International Security History (2014). Other writings include: "The Military Instrument in Cyber Strategy" (with Emily Goldman), SAIS Review of International Affairs 41:2 (Summer-Fall 2021); "A Brief History of Cyber Conflict," in Ten Years In: Implementing Strategic Approaches to Cyberspace, an anthology he co-edited with Emily Goldman and Jacqueline Schneider (Naval War College Newport Paper 44, 2021); and "US Cyber Command's First Decade," (Stanford/Hoover Aegis Series, 2020).

REFERENCES

Brown, Larisa, Rhys Blakely, and Alistair Dawber. 2025. *Iran Feels Might of US After Operation Midnight Hammer.* The Times (June 23, 2025).

GAO (Government Accountability Office). 2020. *Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance (GAO-21-68),* November 19, 2020. https://www.gao.gov/products/gao-21-68.

Hartman, William J. 2025. *Posture Statement Delivered to the Senate Committee on Armed Services (Subcommittee on Cybersecurity).* Testimony to the U.S. Senate (April 9, 2025). https://www.armed-services.senate.gov/imo/media/doc/united_states_cyber_command_posture_statement_ltg_william_jhartman.pdf.

Haugh, Timothy D. 2024. *Posture Statement Delivered to the Senate Committee on Armed Services.* Testimony to the U.S. Senate (April 12, 2024). https://www.cybercom.mil/Media/News/Article/3739700/posture-statement-of-general-timothy-d-haugh-2024/.

Konkel, Frank. 2025. "Pentagon Not Impacted by Microsoft SharePoint Hack, Tech Chief Says," July 24, 2025. https://www.nextgov.com/cybersecurity/2025/07/pentagon-not-impacted-microsoft-sharepoint-hack-tech-chief-says/406968/.

Nakashima, Ellen. 2019. "Cyber Force is Credited with Helping Stop Russia from Undermining Midterms." *Washington Post* (February 14, 2019). https://www.washingtonpost.com/world/national-security/us-cyber-force-credited-with-helping-stop-russia-from-undermining-midterms/2019/02/14/ceef46ae-3086-11e9-813a-0ab2f17e305b_story.html.

Nakasone, Paul M. 2019a. "A Cyber Force for Persistent Operations." *Joint Forces Quarterly* 92 (1).

Nakasone, Paul M. 2019b. *Posture Statement Delivered to the Senate Committee on Armed Services.* Testimony to the U.S. Senate, February 14, 2019. https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.

Nakasone, Paul M. 2020. *Posture Statement Delivered to the House Committee on Armed Services (Subcommittee on Intelligence and Emerging Threats and Capabilities).* Testimony to the U.S. House of Representatives (March 4, 2020).

Nakasone, Paul M. 2021. *Posture Statement Delivered to the House Committee on Armed Services (Subcommittee on Cyber, Innovative Technologies and Information Systems).* Testimony to the U.S. House of Representatives (May 14, 2021).

Nakasone, Paul M., and Michael Sulmeyer. 2020. *How to Compete in Cyberspace: Cyber Command's New Approach.* Foreign Affairs online (August 25, 2020).

Norton, Nancy A. 2020. "Advances in Defense." In *Ten Years In: Implementing Strategic Approaches to Cyberspace,* edited by Emily O. Goldman, Jacqueline Schneider, and Michael Warner. Newport, RI: Naval War College, Newport Papers 45.

Pegram, Aaron, and Emily Tinker. 2025. *Recognising a Year of Defence to the Nation.* Australian Defence Forces website, April 3, 2025. https://www.defence.gov.au/news-events/news/2025-04-03/recognising-year-defence-nation.

Pomerleau, Mark. 2025. *Congress Pushing Joint Task Force-Cyber, Shaking Up How DOD Employs Digital Capabilities.* Defense Scoop, July 24, 2025. https://defensescoop.com/2025/07/24/ndaa-fy26-joint-task-force-cyber-shake-up-how-dod-employs-digital-capabilities/.

Stanton, Paul, and Michael Tilton. 2020. "Defining and Measuring Cyber Readiness." In *Ten Years In: Implementing Strategic Approaches to Cyberspace,* edited by Emily O. Goldman, Jacqueline Schneider, and Michael Warner. Newport, RI: Naval War College, Newport Papers 45.

U.S. Cyber Command Public Affairs. 2024. *U.S. Cyber Command Hosts First Offensive Cyber Flag 2024 Exercise.* Cybercom.mil (September 3, 2024). https://www.cybercom.mil.

U.S. Department of Defense. 2025. *Advance Policy Questions for Lieutenant General John Daniel Caine (USAF), Retired, Nominee for Appointment to Grade of General and to the Position of Chairman of the Joint Chiefs of Staff.* Senate Committee on Armed Services. https://www.armed-services.senate.gov/imo/media/doc/caine_apq_responses.pdf.

Warner, Michael. 2015. "US Cyber Command's Road to Full Operational Capability." In *Stand Up and Fight: The Creation of US Security Organizations, 1942–2005,* edited by Ty Seidule and Jacqueline E. Whitt. Carlisle: U.S. Army War College Press.

Warner, Michael. 2020. *US Cyber Command's First Decade.* Stanford/Hoover Institution, Aegis Series Paper No. 2008. https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf.

Received 25 July 2025; Revised 3 November 2025; Accepted 9 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 41-52
https://doi.org/10.55682/cdr/70kp-vbpd

PROFESSIONAL COMMENTARY

“Go Big”: Cyber Force Large

Brad Kramer[1], Jason Vogt*[2], Dan Grobarcik[2]

[1]United States Marine Corps, CITY, STATE, USA
[2]U.S. Naval War College, Newport, RI, USA

The United States faces a volume and sophistication of malicious cyber activity that far exceeds the capacity of its current military cyber forces. U.S. Cyber Command (USCYBERCOM) must conduct continuous defensive and offensive operations against thousands of state and non-state actors while sustaining a small, high-skill Cyber Mission Force that is already stretched by persistent engagement requirements. This article argues that debates over whether to grant USCYBERCOM SOCOM-like authorities or to establish a separate cyber service miss the central problem: the force is simply too small. Drawing on threat reporting, congressional testimony, and workforce studies, it demonstrates how chronic shortfalls in personnel, misalignment of talent to task, and limited training throughput undermine readiness and constrain strategic options. The article makes the case for significantly expanding the active-duty cyber workforce and pairing this growth with targeted reforms in force management, training standardization, and career progression. It then assesses two primary pathways for scaling the force—growing under a SOCOM-like model or consolidating into an independent cyber service—and evaluates their respective advantages and risks. The article concludes that “going big” on cyber force size, coupled with management modernization, is a necessary precondition for sustaining large-scale cyberspace operations and providing policymakers with credible, scalable options to defend the nation in and through cyberspace.

Keywords: cyber, force generation, cyber training, cyber organization, U.S. Cyber Command, USCYBERCOM

* Corresponding author: jason.vogt@usnwc.edu

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

The U.S. is plagued by cyberthreats. In late 2024, cyber actors associated with the People's Republic of China (PRC), called Salt Typhoon, compromised major portions of U.S. telecommunications infrastructure, only one in a longstanding series of staggering compromises. That same year, another PRC group called Volt Typhoon was discovered on critical power and water systems in the U.S., possibly preparing to target these systems in the event of a conflict (Congressional Research Service 2025).

China is far from the only threat. In 2020, the U.S. government declared that Russian government hackers had compromised as many as many as 18,000 customers of Microsoft products, including multiple U.S. government agencies, critical infrastructure entities, and private sector organizations, in what is known as the Solar Winds compromise (Vijayan 2020). In 2021, a Russian criminal ransomware gang held hostage the IT networks of the largest fuel pipeline operator in the U.S., causing the company to halt its operations, driving panic and fuel shortages across the eastern states (CISA 2023). Vendors such as CrowdStrike and public security organizations like the European Union Agency for Cybersecurity consistently publish annual threat reports showing that cyber threats continue to grow in both sophistication and scale over time (CrowdStrike 2024). Despite a clear and present danger, the United States has struggled to keep pace. Nearly half of all ransomware attacks in the world were conducted against U.S. targets, as its lucrative private sector attracts significant attention from criminal actors. Meanwhile, its public networks face persistent attacks on critical infrastructure from state-sponsored or hacktivist groups displeased with U.S. foreign policy (CrowdStrike 2024).

All the while, USCYBERCOM has been hampered by readiness issues, driven in part by a shortage of qualified personnel (Cobb 2025). Some advocates for reform have called for the creation of an independent cyber service based around USCYBERCOM's current organizational structure (Lonergan and Montgomery 2024). Others advocate for a more incrementalist approach, increasing USCYBERCOM's authorities to make it more like U.S. Special Operations Command (USSOCOM), giving it greater control over its budget and the personnel assigned to its missions (Haugh 2024).

While each has merit, the problem with both of these options is that they do not fundamentally alter the United States' posture to defend against cyber threats or counter adversaries abroad. For example, in April 2024, General Timothy Haugh, Commander of USCYBERCOM, acknowledged that sustaining large-scale cyberspace operations against capable adversaries "was a requirement not fully projected" when the command was established (Haugh 2024). This shortfall reflects an enduring mismatch between operational demand and force capacity.

Congressional testimony and multiple oversight reports identify similar concerns. The Senate Armed Services Subcommittee on Cybersecurity reported that current personnel levels have forced USCYBERCOM to "prioritize near-term missions over force readiness and development," resulting in operational strain and deferred training cycles (Inhofe 2022). Likewise, the Government Accountability Office found that persistent shortfalls in qualified operators have limited USCYBERCOM's ability to meet validated mission requirements across defensive and offensive cyber operations (GAO 2019).

These findings indicate that existing forces are already stretched to meet day-to-day operational demands. They would likely be overextended in any sustained or large-scale conflict. While improving the efficiency and readiness of existing units is essential, such measures alone are insufficient to close the structural gap between mission demand and available manpower. Expanding force capacity is therefore not merely additive—it is necessary to ensure that USCYBERCOM can maintain persistent operations without compromising training, retention, or readiness. Expansion will, of course, require the military to grow the number of active-duty cyber personnel. We recommend this because the threats from malicious cyber actors far outstrip the capacity of the current force. Additionally, empirical studies show that defense workforce expansion can improve readiness only when accompanied by deliberate changes in leadership practices, workload distribution, and institutional incentives. A larger cyber workforce would also allow the military to better align personnel development with mission-critical skill sets and long-term service goals. It also creates redundancy in key roles, enhancing mission continuity and providing opportunities to pair junior apprentices with more experienced mentors, accelerating skill development and institutional knowledge transfer. An expansion could occur under USCYBERCOM's existing force generation model, or through the creation of an independent cyber service. Either way, greater scale stands to provide greater strength.

A SMALL FORCE WITH LARGE PROBLEMS

The military's traditional cyber force generation model relies on teams of highly trained cyber operators that operate closely with intelligence services to conduct cyber operations. Modeled after the National Security Agency at Ft. Meade, USCYBERCOM has shown itself to be adept at conducting sensitive operations aimed at disrupting terrorist groups, countering disinformation campaigns and supporting law enforcement efforts against cyber criminals. However, like most elite forces, these units face challenges when trying to operate at the larger scale posed by the multitudes of adversaries and attacks.

USCYBERCOM is currently organized into 147 mission teams and associated headquarters, numbering approximately 8,000 personnel. Collectively known as the Cyber Mission Force, these units are responsible for three missions that define USCYBERCOM's subordinate force structure: defensive cyber operations, offensive cyber operations, and building, securing, and operating the Department of War Information Network (DoWIN) (USCYBERCOM 2022). Nearly half of these forces are aligned to cyber protection missions. They are managed by the Joint Force Headquarters (JFHQ)-DoWIN, the organization responsible for securing the

DoW’s sprawling IT infrastructure (DoD 2014). For their part, the four service-led JFHQs (Army, Air Force, Navy, and Marine Corps) develop offensive capabilities and options in support of other Combatant Commands. Lastly, the Cyber National Mission Force (CNMF) defends the nation from malicious cyberspace actors who threaten the United States and its interests (Congressional Research Service 2025).

Some estimates place the broader U.S. defense cyber workforce at over 225,000 personnel, including military, civilians, and contractors. Further, the U.S. retains a distinct advantage in its commercial cybersecurity workforce, which serves as a reservoir for talent and innovation. "The strength of U.S. digital services lies largely in their culture of technical expertise and innovation-led investment. The U.S. is home to 59 universities on the *Times Higher Education* list of the global top 200. Its tech and entrepreneurship ecosystem has no equal" (International Institute for Strategic Studies 2023). Current assessments place the active U.S. cybersecurity workforce at approximately 1.3 million professionals. Despite this depth, a persistent talent gap remains, with over 500,000 job openings across the public and private sectors (U.S. House of Representatives, 2024).

Some would argue that protecting the nation from malicious actors is a “team sport” (Nakasone 2021), requiring coordination across the broader cyber ecosystem rather than exclusive dependence on military cyber forces alone. Private sector actors are the dominant players in cyberspace because they develop and operate the bulk of the networks that make up the internet. These organizations are often the best postured to patch and defend networks. But they are unable to take actions that directly impact those attempting to hack them, a process otherwise known as "hackback" and is specifically illegal according to the Computer Fraud and Abuse Act of 1986.

The FBI, State Department, and Department of Homeland Security (DHS) also play important roles in combating cyber threats. Hacking and foreign influence operations are illegal. This allows the FBI and other law enforcement entities to conduct investigations, issue arrest warrants, and compel companies to delete malicious accounts when supported by a court order. The State Department can sanction individuals, organizations, and governments engaged in hacking. DHS’ Cybersecurity and Infrastructure Security Agency can help share information with the private sector and organize the government’s response.

While these actions may be effective in some cases, they are slow-moving and often do little to dissuade malicious behavior, particularly when a hacker is backed by a foreign government. As a result, military cyber operations are often the only direct way to disrupt the malicious activities of foreign actors. The military provides policymakers with unique tools that allow for direct action against hostile actors without the risks associated with conventional military operations. Expanding the size of the force available would give the President additional options to be used against a wider set of threat actors, many of which cannot be effectively disrupted by other means.

ADVERSARY CYBER FORCES

On the other end of this equation sits the nation's adversaries. In 2024, Microsoft observed over 600 million cyberattacks per day. Cybersecurity experts are now tracking over 1,500 unique cyber threat groups, including over 600 nation-state groups, 200 influence groups, and over 300 groups engaged in cybercrime. This activity is overwhelmingly focused on the U.S., along with key allies and partners, including Israel, Ukraine, and Taiwan (Microsoft 2024). Even though USCYBERCOM's operators possess higher levels of technical sophistication than the average hacker, it is simply implausible for the CNMF—which numbers approximately 1,500 personnel—to effectively counter malicious cyber groups that number in the tens of thousands.

The Strategic Pacing Threat: China

China's cyber power is defined by sheer scale and the seamless legal integration of civilian talent into military operations. Following the dissolution of the Strategic Support Force in April 2024, the PRC consolidated cyber operations into the PLA Cyberspace Force. While official personnel counts are classified, credible estimates place the direct military operator cadre between 30,000 and 50,000 personnel (Center for Strategic and International Studies 2024). This force is augmented by the Ministry of State Security and a tiered "cyber militia" system that potentially numbers in the millions, though most are low-capability actors focused on information operations rather than on technical network exploitation (International Institute for Strategic Studies 2024).

The most significant long-term strategic threat posed by the PRC is its human capital pipeline. China now produces approximately 3.57 million STEM graduates annually, nearly four times the U.S. output of approximately 820,000 (Center for Security and Emerging Technology 2024). Under the PRC's National Intelligence Law, this civilian workforce is legally compelled to support state intelligence objectives, effectively serving as a latent auxiliary force.

The Force Multipliers: Specialized State Threats

If China represents the hurricane of the threat landscape, Russia, North Korea, and Iran function as destructive tornadoes: smaller in numerical footprint, but generating strategic effects vastly disproportionate to their size. These nations do not rely on mass; instead, they punch above their weight through elite sophistication, existential dedication, and specialized asymmetry.

Russia trades scale for high-end tradecraft and aggression. Despite a smaller elite operator count—estimated at 1,000 to 3,000 elite personnel in specialized units like Sandworm (Unit 74455)—Russian forces possess extensive combat experience and a willingness to conduct disruptive infrastructure attacks that fall outside the norm . North Korea compensates for its isolation with sheer desperation, mobilizing a 6,800-person cyber warfare personnel (Ministry of National Defense, Republic of Korea 2023) that functions less like a military unit and more like a regime-survival mechanism, responsible for generating up to 50% of the nation's foreign currency (UN Security Council 2024). Iran exerts disproportionate influence through fragmentation, leveraging specialized proxies (such as "MuddyWater") that are positioned to provide stolen data and access to the Iranian government and other malicious cyber actors (CISA 2022). The danger lies in the aggregate. While the U.S. might be able to manage these distinct, high-impact threats in isolation, it must do so while simultaneously holding back the overwhelming tide of Chinese scale.

The Industrialized Criminal Threat

Compounding these state threats further is the industrialization of the non-state cyber ecosystem. The 2024 Europol IOCTA characterizes this landscape as a tiered, resilient economy of Ransomware-as-a-Service (RaaS) affiliates and Initial Access Brokers (IABs). This service-based model lowers the barrier to entry, creating a mass-volume threat that overwhelms traditional defensive sizing models. The FBI's 2024 Internet Crime Report cites a record $16.6 billion in losses, demonstrating that these actors now function as a strategic economic attrition force. Consequently, proper force disposition requires not just point defense, but Hunt Forward teams capable of projecting power into the extraterritorial safe havens where these syndicates operate with impunity (Europol 2024).

The Coming Turbulence: Autonomous AI

The convergence of these threats signals the onset of massive turbulence approaching the U.S. cyber defense apparatus. Chinese, Russian, Iranian, North Korean, and criminal groups are actively incorporating autonomous AI agents into their campaigns. This technological evolution increases the threat by allowing adversaries to execute complex operations at machine speed and scale. This shift creates a tsunami-tempoed threat environment where human operators alone will be overwhelmed by the velocity of attacks. To survive, the U.S. requires a force structure that is not only larger but fundamentally restructured to manage the hyper-accelerated violence of AI-driven warfare.

WORKFORCE AND TALENT MANAGEMENT CONSIDERATIONS FOR FORCE EXPANSION

Right-sizing the force is clearly only part of the challenge. USCYBERCOM's workforce has long faced readiness issues that are exacerbated by its small force size. Recruiting challenges and high personnel turn-over in cyber units have been a consistent challenge. Unlike conventional military units, which can train individual skills and collective tasks in cycles, cyber operations typically require 24/7 operational commitments that can easily stress a small workforce (Chappelle et al. 2013). This is particularly true given USCYBERCOM's current operating concept, called persistent engagement. This concept was implemented in 2018, and it requires near constant operations to disrupt adversary activities (Nakasone 2019). Despite the marked increase in demands placed upon it, USCYBERCOM has only grown by 10%, adding 14 additional teams (about 600 people) between 2022 to 2024 (Di Pane 2024). The additional demands of persistent operations, coupled with only modest workforce increase, has further increased stress on the force (Lonergan and Montgomery 2024). Personnel increases require a larger force than has been implemented to combat both the scale of adversary activity and workforce readiness detractors.

Critics rightly note that adding personnel alone does not automatically change organizational behavior or mitigate dysfunctional labor practices. However, empirical studies show that workforce expansion can improve readiness only when accompanied by deliberate changes in leadership practices, workload distribution, and institutional incentives. For example, RAND and GAO analyses of Air Force and intelligence community workforces have found that capacity growth yields measurable performance gains when supported by reforms in scheduling, supervisory ratios, and task specialization (GAO 2019; RAND 2019). Conversely, when new personnel are absorbed into unchanged structures, the result is often diluted productivity and sustained burnout.

To ensure that growth leads to sustainable readiness gains, Congress and the Pentagon should require that USCYBERCOM integrate workforce expansion with management reforms. These could include codifying maximum operational tempo thresholds, adopting rotational assignment models similar to those used in aviation and special operations, and creating "force health" reporting metrics that link readiness ratings to personnel workload indicators. Evidence from other high-demand technical organizations—such as NASA's mission control teams and nuclear submarine crews—demonstrates that structured rest cycles and distributed expertise significantly reduce stress-induced error and attrition (Chappelle et al. 2013). In this way, workforce expansion becomes an enabler of cultural and procedural reform rather than a substitute for it.

A larger cyber formation also creates opportunities to correct readiness shortfalls by addressing one of the core issues within current cyber forces: the misalignment of talent to task. Among the most significant benefits of a larger workforce is the ability to better match personnel to appropriate roles. This helps reduce the frequency with which individuals are overtasked or diverted from their core responsibilities. Cyber operators have cited excessive administrative overhead and frequent assignments outside their primary specialties as major detractors from readiness (RAND 2019). Expanding the workforce allows USCYBERCOM to better match technical personnel to demanding technical roles, reserving less complex tasks for less experienced or less capable individuals. This approach improves workforce utilization, ensuring operators are used to their potential while mitigating readiness erosion caused by role misalignment.

Additionally, a larger workforce enables more effective talent distribution across the force through tiering of teams and alignment of unit proficiency to mission complexity. Previously, highly skilled personnel were frequently shifted between teams to cover readiness gaps, undermining team continuity and cohesion (GAO 2019). Increasing the size of cyber formations alleviates this by allowing USCYBERCOM to fill shortfalls from readiness pools (e.g. groups of people who are training complete but not assigned to a team) instead of constantly drawing from other operational teams. This stabilizes teams, reduces internal cannibalization of talent, and promotes more predictable readiness cycles.

More people would allow each of the services to better align personnel development with mission-critical skill sets and long-term service goals. Current incentive systems often target broad MOS categories rather than key roles. This leads to uneven retention of talent where it is most needed (GAO 2022; RAND 2019). Likewise, with more personnel, USCYBERCOM could better spread-load demanding schedules across a larger workforce. Having less burdened schedules creates time for continuous development, allowing for tiered development models, pairing junior members with experienced mentors and managing upskilling across career stages. Force structure increases also support workforce maturity management practices, enabling long-range planning to cultivate and retain talent essential to sustained readiness.

The size of the force also directly impacts USCYBERCOM's ability to manage its critical, low-density specialists, such as specialized offensive operators or application developers. A larger force ensures that no team relies on single "one deep" operators. It creates redundancy in key roles, enhancing mission continuity and providing opportunities to pair junior apprentices with more experienced mentors, accelerating skill development and institutional knowledge transfer. Furthermore, a larger formation allows for the development of tiered team structures, where mission complexity is matched to experience, skill, and seniority of a team versus the current one-size-fits-all approach. This flexibility not only improves alignment between workforce capability and mission demand, but also helps prevent burnout, reduce turnover, and close persistent skill gaps (Demus et al. 2024). Ultimately, a more robust force provides the depth and agility needed to meet the scale and sophistication of adversary operations, especially in high-demand operations.

FORCE EXPANSION OPTIONS: A SOCOM-LIKE MODEL OR A SEPARATE CYBER SERVICE

The DoW's cyber force generation is modeled after USSOCOM's approach and relies on the services to provide cyber personnel and units to USCYBERCOM, which maintains operational control of the cyber mission. Others have argued that this force generation model is insufficient and that an independent cyber service should be established. There are positives and negatives to both approaches. Expanding the force under the existing force generation model is possible, but it would be helpful to realign training under USCYBERCOM to help create a more unified approach. Creating a new cyber service would help with overall career management but would also create upheaval that may be undesirable.

The SOCOM Model

As within the special operations community, the services currently recruit and train cyber personnel according to their own departmental requirements before assigning them to USCYBERCOM. These types of highly skilled personnel and units are more difficult to build than conventional forces. Nevertheless, USSOCOM currently has 70,000 personnel, which suggests that growing the size of the cyber force under the existing model is achievable (U.S. Special Operations Command 2022). It will require Congress to allocate additional funding but also requires the DoW to harmonize its special pay, bonus and incentive programs across the services to help bolster recruitment and retention of cyber personnel.

To support a larger cyber workforce, the military must increase training throughput by eliminating training fragmentation across services and adopting scalable training models. Current entry-level pipelines vary widely across services, leading to inconsistent skill development and inefficiencies. Soldiers and Marines complete up to 36 weeks (about 8 and a half months) of sequential training at multiple locations (U.S. Army, 2025). Sailors and airmen undergo shorter or single-site programs (Navy Recruiting Command 2025; Department of the Air Force 2023). Some of these programs prepare service members for expensive follow-on training better than others, all of which contribute to uneven performance across the Joint Force. To resolve this, and prepare the Command for growth, USCYBERCOM should be responsible for setting and auditing the training standards of all services that provide its forces. This would help make quality more consistent and help build a force based on USCYBERCOM's operational needs rather than service-specific determinations. A unified model would also enable scalable force growth, progression beyond basic certification, and enable joint team composition.

Expanding the size of the force under the existing model is possible and it could be done with modest administrative growth based within existing organizations. However, there are limitations to this approach. For instance, different levels of commitment from each of the service could continue to stymie unification at scale. Requiring the services to increase recruitment and retention of cyber personnel may also run up against other priorities. Even the consolidation of training under USCYBERCOM could create challenges, as services may be unwilling to relinquish control of training requirements, particularly if they come with increased costs.

A Separate Cyber Service

In contrast to the status quo USSOCOM-like model, another force generation model that can be used to expand the number of cyber personnel is the creation of an independent cyber service. Under this model, the forces currently supporting USCYBERCOM would be consolidated within the new service, which would gain the Title 10 authorities to man, train, and equip these forces. This approach has the potential advantage of streamlining recruitment and retention efforts. Cyber training would also be consolidated under the new service, allowing it to manage the throughput more efficiently. It would also create a cyber service chief who could advocate for additional resources.

Creating a new service would allow for a unified career progression system to aid in the development and retention of cyber personnel. Because promotion and advancement criteria differ by service, even for identical cyber roles, high-performing operators often find limited opportunities to grow in ways that align with their technical skills (Lonergan and Montgomery 2024; RAND 2019). Research across the cybersecurity industry shows that different standards in work progression for similar roles contribute to attrition, especially among mid-career professionals who lack clear pathways for growth (SANS Institute 2024). Establishing consistent, cyber-specific advancement frameworks would promote long-term development and improve retention of highly skilled workers.

There are risks, of course. Creating a new service would create bureaucratic upheaval that could hamper operations in the short term. Creating a cyber service will not eliminate the need for personnel with cyber skills within the departments, creating even greater competition for skilled personnel. It would also require the creation of new organizations that will take time to fully staff and mature.

BIGGER IS BETTER

Expanding the size of the cyber force will give policymakers more options for combating malicious cyber actors. It will also help improve the quality of USCYBERCOM's operational force. We recommend what we have called "Going Big" because the threats from malicious cyber actors far outpace the capacity of the current force and are accelerating. Additionally, empirical studies show that workforce expansion can improve readiness only when accompanied by deliberate changes in leadership practices managing cyber personnel careers, workload distribution, and institutional incentives. A larger cyber workforce would also allow the military to better align personnel development with mission-critical skill sets and long-term service goals. It also creates redundancy in key roles, enhancing mission continuity and providing opportunities to pair junior apprentices with more experienced mentors, accelerating skill development and institutional knowledge transfer.

It is possible to grow the force under the existing force generation model, although the model could be improved by giving USCYBERCOM greater control in how forces are trained by the services. Expansion could also be achieved through the creation of an independent cyber service, which would also enhance cyber career management. However, increasing the size of the force is probably a more immediate need than restructuring it. Congressional oversight should emphasize commitments from USCYBERCOM leadership to pair new personnel with management modernization, ensuring that increases in manpower are directly translated into improved force sustainability, retention, and mission continuity.

ABOUT THE AUTHORS

Major Brad Kramer is a U.S. Marine Corps communications officer. He holds a Master of Science (highest honors) in Computer Information Systems from Boston University and a Bachelor of Science (summa cum laude) in Business Administration with a minor in Economics from the University of Colorado. He is also a graduate of the U.S. Naval War College. He also holds industry-leading certifications from the International Information System Security Certification Consortium (ISC2) and the Computing Technology Industry Association (CompTIA).

Jason Vogt is an assistant professor and a core faculty member of the Cyber & Innovation Policy Institute at the U.S. Naval War College. He holds a MA in Global Security Studies from Johns Hopkins University. Vogt previously worked for the Defense Intelligence Agency and served on active duty as an Army officer. He specializes in cyber and wargaming.

Dan Grobarcik is a former research associate with the Cyber & Innovation Policy Institute at the U.S. Naval War College. He received his BA in International Relations from American University with an emphasis on U.S. Foreign Policy, and completed his MA in Intelligence and International Security from King's College London. His research focus is on information warfare, security issues in the post-Soviet states, and the Cold War.

REFERENCES

Center for Security and Emerging Technology. 2024. *China is Fast Outpacing U.S. STEM PhD Growth.* Washington, D.C.: Georgetown University.

Center for Strategic and International Studies. 2024. *Force Design for the Twenty-First Century Fight: U.S. Cyber Force Lessons from China's Strategic Support Forces.* Washington, D.C.

Chappelle, Wayne, K. McDonald, J. Christensen, L. Prince, T. Goodman, W. Thompson, and W. Hayes. 2013. *Sources of Occupational Stress and Prevalence of Burnout and Clinical Distress Among U.S. Air Force Cyber Warfare Operators.* https://apps.dtic.mil/sti/citations/ADA584653.

CISA (Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Cyber National Mission Force, National Cyber Security Centre, and National Security Agency). 2022. *Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks (AA22-055A).* Cybersecurity Advisory, February 24, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-055a.

CISA (Cybersecurity and Infrastructure Security Agency). 2023. *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years.*

Cobb, John. 2025. *An Insider's Guide to Cyber Readiness.* War on the Rocks, May 1, 2025. https://warontherocks.com/2025/05/an-insiders-guide-to-cyber-readiness/.

Congressional Research Service. 2025. *Defense Primer: U.S. Cyber Command (USCYBERCOM).*

CrowdStrike. 2024. *2024 Global Threat Report.* https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2024-global-threat-report/.

Demus, A., E. Bodine-Baron, C. McCulloch, R. Bauer, C. Paul, J. Fujiwara, and K. Beavan. 2024. *Operationalizing U.S. Air Force Information Warfare.* RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1740-1.html.

Department of the Air Force. 2023. *Cyber Warfare Operations Career Field Education and Training Plan.* https://static.e-publishing.af.mil/production/1/af_a2_6/publication/cfetp1b4x1/cfetp1b4x1.pdf.

Di Pane, J. 2024. *Cyber Warfare and U.S. Cyber Command.* The Heritage Foundation. https://www.heritage.org/sites/default/files/2024-01/2024_IndexOfUSMilitaryStrength_ASSESSMENT_POWER_CYBER.pdf.

DoD (U.S. Department of Defense). 2014. *Quadrennial Defense Review 2014.* https://www.acq.osd.mil/ncbdp/docs/2014_Quadrennial_Defense_Review.pdf.

Europol. 2024. *Internet Organised Crime Threat Assessment (IOCTA) 2024.* https://doi.org/10.2813/442713.

GAO (U.S. Government Accountability Office). 2019. *U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force.* GAO-19-362. https://www.gao.gov/products/gao-19-362.

GAO (U.S. Government Accountability Office). 2022. *Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking.* https://www.gao.gov/assets/820/814304.pdf.

Haugh, Timothy. 2024. *Posture Statement of General Timothy Haugh Commander, United States Cyber Command.* Senate Committee on Armed Services, April 10, 2024. https://www.armed-services.senate.gov/imo/media/doc/20242.pdf.

Inhofe, James M. 2022. *National Defense Authorization Act for Fiscal Year 2023.* PUBLIC LAW 117–263, 136 Stat. 2903, §1533. https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf.

International Institute for Strategic Studies. 2023. *Cyber Capabilities and National Power: A Net Assessment (Volume 2).* London: International Institute for Strategic Studies.

International Institute for Strategic Studies. 2024. *The Military Balance 2024.* London: Routledge.

Lonergan, E., and M. Montgomery. 2024. *United States Cyber Force: A Defense Imperative.* Foundation for Defense of Democracies. https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf.

Microsoft. 2024. *Microsoft Digital Defense Report 2024.* https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024.

Ministry of National Defense, Republic of Korea. 2023. *2022 Defense White Paper.* https://www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_202307280406019810.pdf.

Nakasone, Paul M. 2019. "A Cyber Force for Persistent Operations." *Joint Force Quarterly* 92 (1): 10–14. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_10-14_Nakasone.pdf.

Nakasone, Paul M. 2021. "Cybercom and NSA chief: Cybersecurity is a team sport," December 6, 2021. https://www.defensenews.com/outlook/2021/12/06/cybercom-and-nsa-chief-cybersecurity-is-a-team-sport/.

Navy Recruiting Command. 2025. *Cyber Warfare Technician.* Accessed January 11, 2025. https://www.navy.com/careers-benefits/careers/intelligence-information-cryptology/cyber-warfare-technician.

RAND. 2019. *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers.* Cyber Workforce Interview Findings. https://www.rand.org/pubs/research_reports/RR2618.html.

SANS Institute. 2024. *Attract, Hire, and Retain Mid-Level Cybersecurity Roles*, May 20, 2024. https://www.sans.org/webcasts/how-attract-hire-retain-mid-level-cybersecurity-roles-outcomes-of-giac-workforce-study/.

U.S. House of Representatives, 2024. *Finding 500,000: Addressing America's Cyber Workforce Gap.* Hearing before the 118th Congress, 2nd Session. Committee on Homeland Security. https://www.govinfo.gov/content/pkg/CHRG-118hhrg59423/pdf/CHRG-118hhrg59423.pdf.

U.S. Special Operations Command. 2022. *SOCOM Factbook 2022.* https://www.socom.mil/FactBook/2022%20Fact%20Book.pdf.

UN Security Council. 2024. *Report of the Panel of Experts established pursuant to resolution 1874 (2009).* S/2024/215. United Nations. https://undocs.org/S/2024/215.

USCYBERCOM (U.S. Cyber Command). 2022. *CYBER 101 – Cyber Mission Force.*

Vijayan, Jai. 2020. "18,000 Organizations Possibly Compromised in Massive Supply-Chain Cyberattack," December 14, 2020. https://www.darkreading.com/cyberattacks-data-breaches/18-000-organizations-possibly-compromised-in-massive-supply-chain-cyberattack.

Received 4 August 2025; Revised 5 November 2025; Accepted 15 December 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 53-64
https://doi.org/10.55682/cdr/qfdx-jhqr

RESEARCH ARTICLE

Military Function, Form, and History's Lessons for Cyber Forces

Michael Warner[1], Emily Goldman[2]

[1]U.S. Cyber Command, Fort Meade, MD, USA
[2]National Security Agency, Fort Meade, MD, USA

This article examines what kind of military cyber force the United States requires and what organizing principles should guide future force posture and structure. It argues that cyberspace's character as a domain of constant contact favors continuous, scalable campaigning rather than episodic operations. Using historical institutional analysis to survey U.S. service, functional, and geographic commands, the article derives criteria for evaluating organizational reform proposals. It foregrounds the core questions that should discipline ongoing debates: What problem, precisely, are advocates trying to solve? What do U.S. military cyber organizations need to do over the coming decades across competition, crisis, and armed conflict? How will proposed changes affect synergy versus segmentation between intelligence and operations, and between cyber and the wider Joint Force? Can adaptation occur with less disruption, expense, and risk while preserving service-organic capabilities and tight intelligence–operations integration? By centering these questions, the article offers a "form follows function" framework to judge whether disruptive organizational change would genuinely improve U.S. cyber campaigning effectiveness and long-term strategic advantage for the nation.

Keywords: U.S. Cyber Command, USCYBERCOM, cyber conflict, cyber force design, sustainment, force development

***Disclaimer:** The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

Few force design issues have been so hotly debated in the United States in recent years as the proper organization for military cyber operations. This controversy reflects not only the novelty of cyberspace but also its various divergences from the "physical" operating domains (Waterman 2025).

Fitting cyberspace and cyber operations into a traditional military framework has always been a struggle. Cyberspace is an interconnected domain of constant contact where "maneuver," if it is to happen at all, requires continuous engagement to set and reset the operational environment to one's advantage. This imperative differs significantly from episodic mass or pulsed operations characteristic of conventional warfighting on land, in the air, and at sea. Like Schrödinger's Cat, enemies in cyberspace are definitely there, or not there, all the time. Therefore, operators and cybersecurity professionals must assume they are there – until one is certain this or that enemy is not (perhaps after unplugging the potentially compromised system). And then the question is finding out where they have gone (Sullivan 2025).

This article steps back from the debates about specific solutions and more deliberately focuses on the purpose behind a military organization's design. The essential and underlying principle here is that "form should follow function." Put another way, the design of something should support its purpose. So, the first question should be, what is (are) the purpose(s) or functions of military cyber forces?

Policymakers never have the luxury of starting *ex nihilo*– with the proverbial blank slate as that question suggests. They must always consider what has already been built, and how it can be reformed or salvaged, with its pieces repurposed, to produce something else that achieves the desired objective. That constraint raises a second question about existing military organizations under consideration for reform: what problem must be solved, or rather, what have the existing forms failed to accomplish, and how do we know?

The current debates about cyber organization are therefore implicitly debates about the purposes being met (or not met) by the *form in place*, and the *functional problems* that will be solved by a solution being envisioned. Any promoters of reforms to U.S. military cyberspace forces should answer these questions about their purpose and performance before any proposed solutions are adopted. Good answers can narrow the range of helpful options and specify key criteria for selecting among different courses of action.

Across factors such as historical context, structural constraints, technological progress, and operational lessons learned, this essay combines contextual analysis, historical institutional analysis, and the extensive, combined experience of the authors in observing multiple senior commanders up to the present, to address these questions. Readers can then judge for themselves whether, and how well, advocates for significant organizational change have answered the questions posed here.

WHAT PURPOSE DRIVES ORGANIZATIONAL FORM?

U.S. Cyber Command (USCYBERCOM)'s history is discussed in more detail elsewhere in this special issue (Warner 2025), but a quick historical note is essential here. The Department of Defense (DoD) determined in the late 1990s that it could no longer fight without reliance on global networks (to oversimplify only slightly, on the Internet). That meant that its own networks and data had to be operationalized and run as a weapons platform, not managed as utilities. From this insight emerged a host of organizational, institutional, and doctrinal innovations, culminating in the creation of USCYBERCOM as a sub-unified command in 2010, and its elevation to a functional unified command in 2018 (Warner 2020).

In a 2019 *Joint Force Quarterly* essay, the then-Commander of USCYBERCOM, General Paul Nakasone (U.S. Army), raised the question of purpose directly. He reiterated a question that Samuel Huntington had posed to the U.S. Navy in 1954: "What function do you perform which obligates society to assume responsibility for your maintenance?" General Nakasone answered the question for USCYBERCOM by explaining that the Command's strategic concept was evolving from a "response force" to a "persistence force" (Nakasone 2019). In short, the Command had been established to defend the military's networks and prepare for war (in the hope that proper preparation would deter conflict). By 2019, as General Nakasone explained, the Joint Force and the nation required more. They required a cyberspace force that could not only continue performing its original defensive and warfighting functions but also play a critical role in strategic competition below the threshold of use-of-force.

General Nakasone's answer to Huntington's question makes sense today because it reflects the structural imperatives of the cyber strategic environment (Fischerkeller, Goldman, and Harknett 2022). By then, USCYBERCOM had already adapted its internal organization as it learned from operational experience in dealing with the peacetime strategic competition. Like many other formations, it had moved to task organizing and employing smaller, Service-provided elements routinely as joint teams in ways never anticipated in 2012 when its Cyber Mission Force (CMF) was first created and allocated across Cyber Mission Teams (CMTs), Cyber Protection Teams (CPTs), and the like. Although introduced to address a gap in how the Joint Force operates in and through cyberspace below the use-of-force threshold, that logic of "initiative persistence" that USCYBERCOM adopted seven years ago also underpins emerging ideas about how to set favorable conditions in and through cyberspace by "contingency campaigning" in anticipation of a crisis or armed conflict (Fischerkeller, Goldman, and Harknett 2025).

Nakasone's 2019 article focused on the Command's then-new strategic concept of persistent engagement but paid less attention to what Samuel Huntington had identified as two additional factors that determine the success in deploying a strategic concept. These are critical challenges: the resources, both human and material, required to implement the concept to support the purpose, and the organizational structure, which groups the resources allocated by society in a manner that implements the strategic concept (Nakasone 2019). The problem of how those resources and organizational structure factors flagged by Huntington (especially the Command's relationship with the Services) should be addressed today drives debates over form and purpose inside and outside the Command, alongside policy-level discussions over the dual-hatted leadership arrangement between the Command and the National Security Agency (NSA), and, in the last couple years, over the pros and cons of a separate cyber service.

WHAT PROBLEM NEEDS SOLVING?

Several important changes have occurred since General Nakasone published his *Joint Forces Quarterly* article in 2019. These raise the salience of those additional factors raised by Huntington.

First, the world has witnessed heightened campaigns of aggression and the development of full-fledged cyber fronts in wars in Europe and the Middle East. These developments are testing assumptions about the role of cyber capabilities and operations in militarized crisis and armed conflict. Although the nature of war, the contours of the cyber strategic environment, and the structural imperatives of operating in and through cyberspace have not changed, many actors in cyberspace have grown bolder and more capable as they gained operational experience and new permissions. We surmise that adversaries will continue to seek advantage over the U.S. and its partners by exploiting cyberspace outside of armed conflict–even as they posture and prepare for war. This means that any country that aims to be a great cyber power must organize cyber forces for operations in competition, crisis, and conflict. This imperative introduces a need for "concurrent campaigning," namely, working to preclude adversary gains through cyberspace outside of war while also setting conditions to prevail in armed conflict.

Second, American cyber personnel (not just in USCYBERCOM) have amassed considerable experience. They have built and sustained cyber forces, operating them below the threshold of war and, at times, employing them to enable or complement conventional operations during militarized crises and armed conflict. They have recruited, trained, and equipped the existing capacities and capabilities that, in any fiscally realistic environment, must be part of whatever solution anyone proposes for arranging U.S. military cyberspace operations forces.

Third, rapid advances in machine learning, artificial intelligence, and automation have compounded the "tyranny of scale" problem for cyberspace operations. There are more actors, operating faster and more capably, and posing more threats to the Joint Force and the nation's interests and allies.

The intensification and scale of threats, along with real-world (versus hypothetical) insights from nonstop operations in cyberspace, add new urgency to our second question: What problems are reformers attempting to solve? And, by extension, what problems do their suggested reforms risk creating, or worsening? The current Departmental cyber posture has come under criticism for an array of reasons, some more substantiated than others (see the other essays in this volume). Cyber forces (allegedly) do not meet readiness standards. They have not attained force mastery. Recruitment and retention problems persisted. The U.S. military as an enterprise is slow to acquire and field new capabilities. Acquisition processes optimized for conventional force development do not adapt at cyber-relevant speed. These are some of the problems that observers (and leaders) say they want to see solved (Defense Science Board 2024).

These issues will not be solved in a vacuum. Historical context, structural constraints, technological progress, and operational experience have all converged in different ways and at different points in time across the global environment to offer an array of organizational and operational solutions for various military problems. Below, we survey approaches from American military history to shed light on whether past solutions are relevant to address not just current shortcomings but future conditions too.

HISTORICAL EXAMPLES

The U.S. military has grappled with how to organize and fight for 250 years. We therefore see a range of historically validated solutions that have been applied in the past.

Counterintuitively, the U.S. military has historically been rather agile in some respects (Posen 1984; Rose 1994; Farrell and Terriff 2002). American policymakers, commanders, and planners have recognized over the last couple centuries that no single organizational construct uniformly meets all force generation, capability, and employment requirements. Different constructs have emerged over time. Those that have survived work together to defend the nation.

The Services regulate and perpetuate military instruments of power. They specialize in recruiting, training, equipping, and developing doctrine and capabilities. Services came into being during and after the Revolutionary War with the realization that victory in conflict demanded sustained, peacetime efforts by professionals, not ad hoc assemblies of patriotic amateurs (i.e., militias and privateers) when a crisis had already arisen. Thus, the U.S. Constitution explicitly authorized an Army, and a Navy (with its Marines), and it effectively but not exclusively aligned them to physical (land and maritime) domains.

The Constitution also permitted creation of a separate, cross-domain service for the collection of tariffs and suppression of smuggling. Secretary of the Treasury Alexander Hamilton convinced the first Congress to enact a law providing him with officials to inspect cargos in-port and to acquire up to ten “cutters.” Their crews were empowered to board every ship arriving in the U.S. (out to “four leagues” at sea) to “search and examine the same and every part thereof" (U.S. Congress 1790). Here was the origin of what would become the U.S. Coast Guard—from the beginning a military force with extensive powers for law enforcement and infrastructure protection.

The original Services operated in comparatively well-defined domains, but that historical fact is not as straightforward as it might appear. A "domain" is a set of physical realities that channel the design and employment of forces in that battlespace. The land, sea, air, and space domains all make unique technological demands that a military force and a commander must satisfy to operate effectively. The physical realities of those four domains are also "adversary agnostic," to coin a phrase. Each of the physical domains looks and acts the same for anyone operating in them. We can speak of states owning territory, but the character and principles of military operations on land hold true whether the mountains, forests, or steppes in which forces operate are located in Chile, Greece, or Mongolia. Spacecraft, aircraft, and ships basically function the same wherever they are in a physical domain, and when they do not, the differences in performance can be attributed to physical, not legal, factors (depth, altitude, temperature, sunspots, etc. – as opposed to borders drawn on maps).

Technological progress drove the creation of another service after World War II while, at the same time, it further blurred the "domain-specific" characters of the service model. The invention of airplanes led to a separate air force in 1947 to guarantee the resources, attention, doctrine, and culture advantageous in this then-newest warfighting domain. Yet the resulting Air Force, ironically, broke the "domain-specific" pattern. While the U.S. Air Force operated in the air domain and achieved a certain primacy over air operations, all the other services retained the right (and capacity) to conduct their own air operations in support of their land and maritime missions. In addition, the Air Force (despite strenuous efforts) never achieved a monopoly on operations above the air (i.e., in space), in a far more technologically demanding physical environment.

Interestingly, it is a fact that the U.S. military has never stated nor followed an imaginary principle that each operating domain requires its own dedicated service. The Republic has always had a "maritime domain" service with capable soldiers (i.e., Marines), as well as a separate quasi-navy (the Coast Guard), which worked both ashore (in ports) and at sea. In short, the Services exist to build certain forces for certain functions, even though they certainly have concentrated their respective efforts in particular domains.

The Services built forces, but they were not always good at operating them. Any study of the Union Army's war record – and the U.S. Army's performance in other contests before 1941 – reinforces this finding. The U.S. experimented with several ways of controlling forces in wartime before settling in the 1940s on the modern Department of Defense, now the Department of War (the umbrella over the Services), and Combatant Commands.

Combatant Commands emerged from World War II with the recognition that modern war requires combined arms, joint operations, and coalition campaigning. The delicacy of inter-allied relations, along with inter-service rivalry, had hampered the Services from achieving the unity of effort required to defeat the Axis powers and, hence, forced the creation of supreme, regional command of Service and coalition forces in each geographic theater of operations. The geographic Combatant Commands of today descended, in concept at least, from the "theaters" of World War II (e.g., Central Pacific, South Pacific, China-Burma-India, and so on).

Combatant Commands evolved toward more centralized entities after the experience of Vietnam, in which U.S. Pacific Command delegated the warfighting to a four-star subordinate element (Military Assistance Command-Vietnam, or MAC-V), which in turn gave its Service components wide latitude and independence in how they conducted operations. Since the Goldwater-Nichols Act in 1987, the Commands have mostly concentrated their allocated forces by domain, not service, typically creating land, maritime, and air components. The Geographic Combatant Commands have further, and often, sub-divided the conduct of combat operations by creating and tailoring temporary Joint Task Forces for specific missions or campaigns.

Functional Combatant Commands (FCC) emerged during the Cold War to perform and sustain enduring, joint functions and global missions on an operational basis. They combine military mission command and the ability to innovate training and equipment as required. Typical FCCs today are U.S. Transportation Command (USTRANSCOM), U.S. Strategic Command (USSTRATCOM), and U.S. Space Command (USSPACECOM).

U.S. Special Operations Command (USSOCOM) represents a still-more unique FCC. This requirement arose in the 1980s as Congress determined that neither the Services nor the Geographic Commands were sustaining and effectively employing the special operations forces that the nation and the Department required to execute key missions. USSOCOM is a distinct model of a FCC that executes missions while also exercising Service-like authorities for training, doctrine, equipping, and acquisition for all the Service special operations forces. The USSOCOM model tightly links support activities with operational command to keep the force proficient and agile.

USCYBERCOM is another sort of FCC. It operates high-demand and low-density assets, like USSTRATCOM. It also serves some man, train, and equip functions, like USSOCOM. These man, train, and equip functions largely flow through its Service component commanders, who are also dual-hatted as leaders of their respective "Joint Force Headquarters-Cyber" combat elements. The USCYBERCOM Commander, moreover, serves as the "dual-hatted" Director of the National Security Agency, a key element of the Intelligence Community that is the nation's premier signals intelligence and cybersecurity arm. USCYBERCOM furthermore *supports* the geographic and other Functional Combatant Commands in their missions, while being *supported* by them in its unique mission of securing, operating, and defending the Department of War Information Networks (DoWIN, formerly DoDIN), on which the entire Department and Joint Force depend for command and control, situational awareness, intelligence, logistics, and much more (Pomerleau 2025). To expand the picture even further, one of USCYBERCOM's operational components is the Cyber Defense Command (DCDC), headed by a three-star officer who also directs the Defense Information Systems Agency (the large combat support agency that builds and maintains the entire Department's networks).

Other countries have experimented with cyber forces, and they provide a wide array of possible solutions for organizing military capabilities in cyberspace. Jason Blessing (2021) identified nine different cyber force structures based on organizational model and scale of command. Some countries separated their offensive and defensive cyber forces into different organizations, while others relied on their signals intelligence organizations to conduct some cyberspace operations. None of these countries, however, operated a military with global responsibilities and presence, and none of them shared the fine but peculiar structural and legal imperatives dictated by the U.S. Constitution. Our model is not necessarily fitting for others, and vice versa.

For its part, the U.S. military has organized its cyberspace capacity in a congeries of structures and relationships with a lot of moving parts. That arrangement resulted from changes driven by hard-fought experience, lessons learned, and the emergence of new technologies. It is easy to see how each one of USCYBERCOM's duties could be performed better by a dedicated organization created for that function (or mission) and nothing else. The trick is how to ensure that the Department and the Joint Force can depend on some replacement entity or entities that will: a) do all that USCYBERCOM does now, b) do so at least as well as it is doing them now, and c) not fail in any important function.

WHAT SHOULD A SOLUTION INCLUDE?

The available space to design new cyber organizations is not unconstrained. It should acknowledge the considerations that gave rise to the various experiments and solutions described above, while it aligns to the nature of the cyber strategic environment and what is required to create security in and through cyberspace. It should also be cognizant of how adversaries are operating – especially those with a different conception of competition and conflict that ignores the Westphalian peace-war binary. Our cyber forces must be able to operate independently of the conventional force to address adversary campaigns aiming at "winning without fighting," while also being capable of operating synergistically with the conventional and nuclear forces in competition, crisis, and armed conflict.

This is a lengthy set of requirements. Yet any solution to them should not just solve the challenges of today. It should also anticipate and build in flexibility to meet future requirements. There are long-running debates about how to optimize for cyber, signals intelligence (SIGINT), information operations (IO), electromagnetic spectrum operations (EMSO), and electronic warfare (EW). Many of our most capable adversaries seem to be integrating EW, Cyber, SIGINT, and IO capabilities in real-world operations. Other debates ask whether military cyber forces have a role in enhancing "cognitive security" and targeting adversary cognitive vulnerabilities; or whether they should become a highly technical force to lead the Department in automation, data orchestration, and data management.

Another debate must be addressed simultaneously. The current, dual-hatted relationship between the Command and NSA was created in 2003 to be the Department's locus of expertise on operationalizing data and analytics. Its success in this mission seems clear, but if that dual-hatted relationship is altered, whatever arrangement succeeds it must avoid stove piping intelligence and operations – a point that even critics of the "dual-hat" acknowledge.

Above all, any solution must enable unity of effort. Advantage in cyberspace goes to the actor postured to understand, anticipate, act, and adapt to changes in that environment. Understanding, anticipation, action, and adaptation in our modern world involve a lot of players with differing authorities, incentives, and capabilities. They must work together. The U.S. military lost any chance of gaining a monopoly on operating in what was not yet called cyberspace decades ago when it relinquished its lead in developing computers and software. But the military still needs to be involved in any comprehensive solution to the national security issues posed in cyberspace. What the nation needs is an alert and agile web of military, federal, allied, industry, and partner capabilities. Its military arm in cyberspace should have tightly linked intelligence and operational capacities to act when needed, and to enable others to act.

"Sometimes the Remedy is Worse than the Disease" –Francis Bacon

We conclude by returning to one of our original questions, and add another that seems obvious: what is the problem that people are trying to solve; and what do we need our military cyber organization(s) to do in the next several decades? We have tried to place current debates into the perspective of both history and the future. A survey of how the American military has addressed previous technological and organizational challenges raises questions that advocates of any solution [or remedy] must address based on credible evidence. These are issues that engender emotion as well as logic, and this is to be expected. They relate to military culture, operational experience that has cost the nation much in blood and treasure, competing theories about the future security environment, and how best to prepare for it. Such debates should therefore begin with foundational questions.

Different organizational solutions reflect functional prioritization. Working from function to form, we offer that any proposals for organizing a future U.S. military cyberspace operations function should consider the following:

- A cyber "military" element must operate with speed, agility, persistence, and scale. It must understand the rest of the Joint Force and be integrated with forces in the physical domains, and with other cognitive capabilities. It must be able to do so in competition, crisis, and conflict.
- Cyber is organic to, required of, and inseparable from, what each Service must do. The Services each sustain organic intelligence and communication communities that map to the respective physical domains and operational technologies. These communities in turn depend on cyberspace.
- Military and intelligence missions in cyberspace often take place on the same networks. As a result, effective operations must be synchronized in near-real time. This necessitates seamlessness within the communications and intelligence enterprises across all cyber military force elements (and vice versa).
- Cyberspace is an interconnected strategic environment that rewards synergy and punishes segmentation. Decisions should bias toward synergy, not insularity and segmentation. How will any solution impact synergy and segmentation?
- Any significant change to current arrangements will take time and cause disruption, to include loss of operational tempo, missed opportunities, added expenditures, and personnel churn. Reorganizing takes resources, leadership, and talent away from mission. Advocates of any solution must explain not only whether but how we can adapt with less disruption, expense, and risk, and yet still improve upon the status quo. They should also explain how enduring and agile their proposed solutions will be given potential technological changes on the horizon.
- How will whatever new organization that succeeds USCYBERCOM fare, when the wider defense enterprise has thus far resisted adapting? It may be the case, for example, that USCYBERCOM has not "failed," but rather the Joint Force or Department has nonetheless fallen short of required functions in cyberspace. For instance, the Command is embedded in an industrial-era defense ecosystem with an acquisition system that privileges Service autonomy over integration and is optimized to develop solutions over years, rather than in weeks or months—as evidenced by the most recent round of reforms (U.S. Department of War 2025).

A short-term pursuit of efficiency can overpower effectiveness; likewise, the demands of today can overpower the needs of tomorrow. Any disruptive change to military organizations had best do no harm while it solves for future problems.

ABOUT THE AUTHORS

Dr. Michael Warner serves as the Command Historian at USCYBERCOM. Before arriving at the Command in 2010, he served as an analyst, staff officer, and historian in several agencies of the US Intelligence Community. Dr. Warner has written and lectured widely on intelligence and cyber history, theory, and strategy. He is co-author, with John Childress, of The Use of Force for State Power: History and Future (2020). He also wrote The Rise and Fall of Intelligence: An International Security History (2014). Other writings include: “The Military Instrument in Cyber Strategy” (with Emily Goldman), SAIS Review of International Affairs 41:2 (Summer-Fall 2021); “A Brief History of Cyber Conflict,” in Ten Years In: Implementing Strategic Approaches to Cyberspace, an anthology he co-edited with Emily Goldman and Jacqueline Schneider (Naval War College Newport Paper 44, 2021); and “US Cyber Command’s First Decade,” (Stanford/Hoover Aegis Series, 2020).

Dr. Emily O. Goldman is a cyber strategist and thought leader on cyber policy, currently working for the Office of the Assistant Secretary of War for Cyber. Previous positions include Director for Cyber Strategy at the National Security Council and cyber advisor to the Director of Policy Planning at the Department of State. As Director of the USCYBERCOM/NSA Combined Action Group, she led a team that wrote the 2018 Command vision, Achieve and Maintain Cyberspace Superiority. She was a professor of Political Science at the University of California, Davis, for two decades and has published and lectured widely on strategy, cyberspace operations, and military innovation. Publications include Cyber Persistence Theory: Redefining National Security in Cyberspace (Oxford University Press 2022) with Michael Fischerkeller and Richard Harknett and "The Importance of Analytic Superiority in a World of Big Data and AI" (Cyber Defense Review 2024) with Robert Grossman.

REFERENCES

Blessing, Jason. 2021. “The Global Spread of Cyber Forces, 2000–2018.” In *Proceedings of the 13th International Conference on Cyber Conflict,* edited by T. Jančárková, L. Lindström, G. Visky, and P. Zotz. Tallinn: NATO CCDCOE Publications.

Defense Science Board. 2024. *Future Cyber Warfighting Capabilities: Executive Summary.* Office of the Under Secretary of Defense for Research and Engineering. https://dsb.cto.mil/wp-content/uploads/2024/09/DSB_Cyber_ExecutiveSummary_2Aug24.pdf.

Farrell, Theo, and Terry Terriff, eds. 2002. *The Sources of Military Change: Culture, Politics, Technology.* Boulder, CO: Lynne Rienner.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford University Press.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2025. *Setting the Stage: Cyber Contingency Campaigning.* Lawfare, August 28, 2025. https://www.lawfaremedia.org/article/setting-the-stage--cyber-contingency-campaigning.

Nakasone, Paul M. 2019. “A Cyber Force for Persistent Operations.” *Joint Force Quarterly* 92:10–14. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950/a-cyber-force-for-persistent-operations/.

Pomerleau, Mark. 2025. *Congress Pushing Joint Task Force–Cyber, Shaking Up How DoD Employs Digital Capabilities.* DefenseScoop, July 24, 2025. https://defensescoop.com/2025/07/24/ndaa-fy26-joint-task-force-cyber-shake-up-how-dod-employs-digital-capabilities/.

Posen, Barry R. 1984. *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars.* Cornell University Press.

Rose, Stephen Peter. 1994. *Winning the Next War: Innovation and the Modern Military.* Cornell University Press.

Sullivan, Vincent. 2025. *Your Security Tools Are Lying to You: What Happens When Threats Go Unobserved—Schrödinger’s Cat Paradox within Cybersecurity.* Cyber Strategy Institute, January 29, 2025. https://cyberstrategyinstitute.com/your-security-tools-are-lying-to-you-what-happens-when-threats-go-unobserved-schrodinger-cat-paradox-within-cybersecurity/.

U.S. Congress. 1790. *Statutes at Large, 1 Stat. 175.* August 4, 1790.

U.S. Department of War. 2025. *Secretary of War Announces Acquisition Reform.* Press Release, November. https://www.war.gov/News/Releases/Release/Article/4329487/secretary-of-war-announces-acquisition-reform/.

Warner, Michael. 2020. "US Cyber Command's First Decade." *Aegis Series Paper,* no. 2008 (December). https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf.

Warner, Michael. 2025. "Evolution of U.S. Cyber Command since 2018." *The Cyber Defense Review* 10 (3). https://doi.org/10.55682/cdr/yxsr-e85e.

Waterman, Shaun. 2025. "Former CYBERCOM Commanders Urge Caution on Push for New Military Cyber Service." *Air & Space Forces Magazine* (December 9, 2025). https://www.airandspaceforces.com/former-cybercom-commanders-new-military-cyber-service/.

Received 31 July 2025; Revised 19 October 2025; Accepted 5 December 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 65-78
https://doi.org/10.55682/cdr/5td8-jw30

RESEARCH ARTICLE

Gaming Campaigning in Cyberspace

Jason Vogt*

U.S. Naval War College, Newport, RI, USA

This article introduces a new tool for gaming out military campaigns in cyberspace. Called the Persistent Engagement Wargame, this multi-sided game explores how different force designs and operational strategies interact with the kinds of missions and objectives that may be assigned to organizations such as U.S. Cyber Command (USCYBERCOM). Five iterations of the game were played at the U.S. Naval War College between 2023-2025. These games indicate that, over periods of sustained competition, sizable cyber forces are necessary, yet they can still fail if the nation's operational approach is not properly aligned. Optimal results occur when a nation has sufficient capacity and a strategy that exploits gaps in its adversary's defenses while simultaneously defending its own military networks and critical infrastructure. These games also revealed several important lessons about force design that can inform the current debates surrounding cyber force structure. Chief among these is the requirement for a greater number of "counter-cyber" forces within USCYBERCOM. Another major implication is the need for robust organizations to enable allied cooperation. Greater use of such wargames could help practitioners, planners, and policymakers understand and experiment with different effects of alternative futures for cyber forces.

Keywords: cyber, wargaming, campaign, force structure, cyber organization, persistent engagement wargame, U.S. Cyber Command, USCYBERCOM

* Corresponding author: jason.vogt@usnwc.edu

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

Wargames have long been used by militaries to examine force structures, operational plans, and new technologies. From the Prussian General Staff's planning in the mid-nineteenth century to the U.S. Navy's development of War Plan Orange and Cold War studies of nuclear escalation, wargames have proven to be invaluable tools. They enable leaders to explore interactive, high-stakes scenarios in a controlled environment, revealing potential strengths and weaknesses in doctrine, force design, and capabilities without the cost of blood and treasure in the real world.

While modern wargames have successfully integrated land, air, maritime, and even space operations, integration of cyber operations remains a persistent challenge. Conventional military wargames are poorly suited for capturing the complex dynamics of cyber conflict. Recognizing these limitations, some game designers and researchers have developed dedicated cyber wargames (Smith, Kollars, and Schechter 2024). Nevertheless, many of these efforts focus narrowly on tactical operations, higher-level strategic decision-making, or organizational preparedness. While valuable, this leaves a methodological gap at the operational level—where military leaders must wrestle with cyber force structure, resource allocation, and sustained competition.

As the Department of War considers questions about different cyber force generation models, military and civilian leaders must evaluate how potential changes could affect national security outcomes. Wargames at the operational level of cyber campaigning can help. To that end, this article introduces the *Persistent Engagement Wargame*. This multi-sided game uses abstract network topologies instead of a standard geographic map. It employs specialized cyber units instead of traditional military formations. And it uses time horizons that span months and years instead of mere hours and days. The game's core objective is to allow players to explore how different cyber force models and operational strategies perform against thinking adversaries during prolonged competition or protracted war.

Five iterations of the *Persistent Engagement Wargame* were played at the U.S. Naval War College between 2023 and 2025. These games showed that overinvesting in offensive capacity against a single adversary or objective can undermine broader national security goals. Separately, players who have sufficient cyber forces can still underperform without appropriate operational strategies. In short, these games show that force structure alone does not determine outcomes. They also reveal other important lessons, including the requirement to expand "counter-cyber" capabilities—to disrupt the activities of malicious cyber actors—in U.S. Cyber Command (USCYBERCOM). Additionally, robust organizations for cooperation and deconfliction with allies and partners are required.

Greater use of such operational cyber wargames could help practitioners, planners, and policymakers game out alternative force designs, strategies, and scenarios. In particular, they could help compare proposals for incremental reform or radical changes to USCYBERCOM. These wargames also help explore how variations in operational approach can affect outcomes independent of force design.

LIMITATIONS OF CYBER IN CONVENTIONAL WARGAMES

Wargame designers have experimented with cyber warfare since the 1990s (Schechter 2023) and the military has routinely integrated cyber operations into conventional wargames for over a decade. Unfortunately, while many of these games can help military leaders unfamiliar with cyber understand its potential utility and impact, they do so at considerable cost to the realistic representation of this domain.

Most conventional wargames lack a suitably representative cyberspace environment and the appropriate roles therein to effectively depict cyber in conflict. Many have fossilized into a standard approach that merely gives players a generic list or menu of network accesses and actions that they can execute during the game (Cancian, Cancian, and Heginbotham 2023). They tend to ignore the operationally relevant socio-technical-economic dependencies that exist between civilian and military networks. They also foreshorten consideration of the time needed to play through cyber actions and effects, since these operations involve longer time horizons than those typically represented in conventional wargames.

Most conventional wargames, not surprisingly, are built around conventional military forces. These forces are dispersed on a map or chart, prepared for armed conflict, and controlled by conventional military commanders. When included, cyberspace is usually just bolted or added on after the fact. Granted, cyberspace is built upon physical infrastructure that can be overlayed onto a geographic map. However, it also exists as a virtual space that is ‘accessed’ remotely through routers on the global internet, via networked terminals to a satellite, or using wireless radio frequency connections (Conti and Raymond 2017). This is different terrain.

Moreover, most military operations are now highly dependent on a dynamic array of multiple network connections critical to command and control (C2), intelligence gathering, information processing, and targeting. If one or more of these networks are damaged through cyberspace, the loss can degrade or disrupt all of these operations. Representing these potentially devastating system-wide cyber effects is often beyond the scope and level of detail considered in conventional wargames.

Another problem is that military cyber forces are neither the most numerous nor necessarily the most consequential actors in the peacetime or wartime cyber ecosystem. With respect to government cyber operations, intelligence rather than military agencies are the most prolific actors, since they engage in long-term cyberspace campaigns to collect information or, in some cases, to influence foreign populations (U.S. Department of Justice 2018). There is also a large community of organized criminal enterprises, many of which are state sanctioned, who are responsible for billions of dollars of theft from targeted states each year (Gold 2022).

Perhaps most importantly, large technology companies now act with the broadest global reach in this domain. They include dedicated cybersecurity firms that help defend their clients' networks and generate cyber threat intelligence that often exceeds what government agencies now produce (Google Threat Analysis Group 2023). These actors are rarely represented in military wargames that focus on kinetic firepower, in part because of the challenges of including more players, but also because most of their activities fall below the threshold of armed conflict.

Consequently, conventional wargames minimize or ignore the socio-technical-economic dependencies between militaries, civilian populations, and the commercial networks that make up the bulk of cyber infrastructure (Kollars and Schechter 2021). Civilian logistics, which rely heavily on IT for inventory control and transportation management, are particularly vulnerable to disruption (Greenberg 2018). Cyberattacks on critical infrastructure, such as power and telecommunications, are also likely to harm civilian populations and military operations (Greenberg and Newman 2023). While efforts have been made to understand these threats at the technical level, their downstream effects on military operations and conflict are rarely played out in wargames.

The last factor that indirectly influences the cyber wargame environment and the decision-making of cyber actors is time. While a well-prepared cyber operation can be executed in minutes or hours, it can take months or years to acquire the necessary network accesses and develop tools to exploit them (Conti and Raymond 2017). In many respects, the art and science of cyber warfare are not manifest in the execution of a cyberattack—they are in the planning and painstaking preparation to gain access to a system in the first place. While some conventional wargames encompass long time horizons, most do not. This limits what can realistically be achieved through cyber operations in these games, which could otherwise exceed the pro forma list of accesses and actions typically provided to players.

CYBER WARGAMES

Given these problems, some wargame designers have sought to create games specifically focused on cyber conflict. Most of these games focus on one of three areas: tactical network operations, strategic decision-making, and organizational preparedness. These games can help improve operator skills, crisis response, and inter-agency coordination. However, they do not fully account for decisions related to force structure and the operational decisions of made by cyber leaders during long-term campaigns.

It is important to note that cyber wargames represent a distinct analytical tool. Penetration testing and red teaming are both commonly used to improve network defenses and help companies improve their emergency response procedures—but they are not wargames. Cyber wargames also differ from computer-based simulations that attempt to mathematically model cyber behavior through quantitative methods (Crotty and Daniel 2022).[1] Instead, cyber wargaming focuses on human decision-making and how the choices people make interact within a complex environment (Curry 1990).

As with the earliest conventional wargames, much of the initial emphasis on developing cyber wargames focused on the tactics associated with hands-on network operations, leading to the adoption of cyber ranges for conducting tactical exercises. A cyber range is a simulation tool, capable of emulating friendly or rival information technology environments with realistic hardware and software components, which cyber professionals use to develop practical skills and evaluate the security of their networks (Sullivan et al. 2018).

While many non-governmental activities on these ranges focus on training and education, governments and military organizations are now utilizing similar simulators to conduct large scale cyber wargames—such as the annual NATO cyber defense exercise (NATO CCDCOE 2023). For instance, in 2021, the NATO exercise featured cyberattacks against the fictional island of Icebergen, where hackers attempted to steal intelligence and intellectual property, disrupt government services, and bring down the power grid. While this game focused on the cyber dimensions of the conflict, it also included players in the traditional military domains (Miller 2022). As valuable as this kind of exercise is, however, cyber ranges are tactically focused, so their utility for operational campaigns and strategies is limited.

Game designers and researchers have also built cyber wargames resembling tabletop exercises to help them understand the implications of escalation and deterrence in cyberspace. These games tend to focus on decision-making at the senior level. Players representing heads of state or other senior leaders are typically presented with a scenario in which one or more cyberattacks or vulnerabilities are revealed. The players are then asked to make decisions about how they would respond. Networks and attack capabilities tend to be highly abstracted, as the technical details are often less relevant to the player decision space. For example, the International Crisis Wargame placed players in the role of cabinet officials who were asked to make decisions related to cyber and nuclear stability (Schneider, Schechter, and Shaffer 2022). These types of games can help researchers understand how leaders may respond to a crisis. But they do not examine the decisions at lower echelons that are critical to understanding cyber campaigns.

Games focused on organizational preparedness are the third area of cyber wargaming that has seen significant growth. These games are popular in both the government and the private sector, as they allow organizations to understand how cyberattacks could impact their systems and exercise their response plans. For example, the North American Electric

[1] While there are game-theoretical approaches to understanding decision-making strategies in cyberspace, they typically focus at the tactical level and do not take overall force design into consideration (Bao et al. 2017).

Reliability Corporation and its Electricity Information Sharing and Analysis Center developed a wargame called GRIDEX, which enables utility providers and government agencies to practice their response and recovery actions in response to cyberattacks (Duncan 2023). There are countless other examples, but a key feature of these games is that they are almost always reactive and focused on organizational processes required to respond after a cyberattack. These games are rarely tied to the levels of national cyber conflict that involve the military.

The increased adoption of tactical, strategic, and preparedness cyber wargames illustrates the value of gaming methods for understanding cyber conflict. Greater use of these tools at the operational level is warranted. Building such a game requires accounting for the actions of different types of cyber forces within multiple and different kinds of networks over extended periods of time.

THE PERSISTENT ENGAGEMENT CYBER WARGAME

Campaigning in cyberspace is a complex process involving persistent operations against adversary networks to gain intelligence, develop cyber options for conventional military operations, and disrupt the activities of malicious cyber actors' intent on doing harm. In this context, cyber operations are similar to conventional military operations, defined as a series of actions targeting a specific network. Similarly, cyber campaigns are a series of coordinated cyber operations used to gain a strategic advantage over time. Much like military campaigns in major wars, cyber campaigns can last from months to years and are often conducted in concert with other elements of national power to achieve objectives (Harknett and Smeets 2022).

The critical difference is that the longer-term military campaigns are only conducted in the context of a long-running major conflict, while cyber operations and campaigns occur all along the conflict spectrum from peace to war. Cyber operations can be designed to support future military operations or as part of broader information campaigns intended to influence populations before or during conflict (Libicki 2017). Examples include Russia's efforts to erode democratic norms and elections through cyber influence campaigns, China's efforts to penetrate U.S. critical infrastructure, and the use of cyber espionage to acquire information on advanced military technologies.

To counter these operations, the former head of USCYBERCOM, General Paul Nakasone, called for a new operational approach based on maintaining near-constant pressure on adversaries in cyberspace, known as "persistent engagement" (Nakasone 2019). The idea that nations must engage in persistent operations to achieve national security goals in cyberspace is further articulated by Fisherkeller, Goldman, and Harknett in their work, *Cyber Persistence Theory*. These scholars argue that cyber conflict is defined by states that are "persistently active in sustained campaigns within cyberspace deliberately calibrated to remain below a threshold that would likely elicit an armed response, seeking instead to produce cumulative gains over time." Competition in cyberspace exists in its own strategic environment, which is not defined by state-based coercion but rather the ability for nations to exploit vulnerabilities in their adversary's digital networks to create opportunities that further their national interests (Fischerkeller, Goldman, and Harknett 2022).

The *Persistent Engagement Wargame* seeks to model this strategic environment at the operational level of campaigning. Conducting cyber campaigns requires commanders to balance the activities and timing of not only offensive and defensive cyber operators, but also intelligence analysts and software engineers. If a network is connected to the internet and using software with known vulnerabilities, it could be relatively fast and easy for a cyber operator to gain access. However, gaining access to more complex or better-protected targets such as military C2 systems, financial institutions, and electrical power grids could require cyber operators to gain access to a series of networks, taking additional time and resources (Conti and Raymond 2017).

In this game, as in reality, cyber campaigning also requires sharing information and coordinating defensive cyber forces' actions with allied governments, interagency partners, and members of the intelligence community (The White House 2023). In addition to defending military networks, cyber forces may be tasked with defending a nation's critical infrastructure from cyberattacks. This cannot be accomplished without coordination with local governments, infrastructure owners and operators, and the pervasive commercial cybersecurity industry. How a nation chooses to prioritize these activities over months and years can have significant implications for their ability to defend against malicious cyber activity. Hence, the *Persistent Engagement Wargame* incorporates all these requirements.

Game Design

This wargame involves a fictionalized scenario with three democratic nations (Blue, Gold, Green) that are under threat from three autocratic regimes (Red, Purple, Gray) (Table 1). Red, which is the largest autocratic nation with the most robust cyber forces, is conducting cyber operations in preparation for a major invasion against the smallest democratic nation, Green. At the same time, Gold is having a national election, which the autocrats are attempting to influence. Blue, the most capable democratic nation, is attempting to help both Green and Gold defend themselves against the autocratic threats. The overall purpose of the wargame is to examine how force structure, operational strategy, and allied cooperation affected the democratic nations' ability to meet their national security goals.

Five iterations of the game were played at the U.S. Naval War College between 2023-2025. Game participants included a mix of students, U.S. Naval War College faculty members, faculty members of other academic institutions, and private sector personnel. The participants had backgrounds in military cyber operations, intelligence, cybersecurity, wargaming, and political science. For each game, players were broken into six teams, typically with 2-3 players per team. They had control of all of their respective nation's cyber forces. The game required 8-12 hours to play, which were either concentrated over two days or spread over several weeks. Players submitted their actions on move cards created with PowerPoint, which were then emailed to the adjudication team at set intervals. Adjudication was conducted using a rigid probability-based rule-set (completed manually or with the aid of an Access Database tool developed specifically for the game).

Each game was broken into two phases: a force design phase and a competition phase. During the first phase, players made decisions about which types of cyber units and organizations they wanted. These included military cyber units to target foreign networks, counter-cyber units capable of disrupting the activities of their opponents' cyber forces, intelligence assets to conduct espionage, cybersecurity organizations, influence actors, and, in some cases, criminal organizations. Each of these units had specialized skills used either independently or in conjunction with other units. For example, offensive cyber units could work with intelligence units to improve their chances of gaining access to a target. Alternatively, that same intelligence unit could be used to target an adversary political party to acquire information for influence operations. These decisions represented operational trade-offs, constrained by initial decisions about force design.

During the competition phase, players made operational decisions about how to employ their forces to achieve their national objectives. In lieu of a map, the game board consisted of a graphical representation of over 700 target networks, each belonging to a nation's government, military, and commercial sectors. Players were provided with graphics displaying each nation's digital infrastructure, categorized by both its sector (military, government, critical infrastructure, or industry) and level of network accessibility (represented by a four-tier scale).

Player decisions centered around efforts to gain access to adversary networks, while simultaneously protecting their own systems from exploitation. In general, the target networks associated with a nation's military or intelligence apparatus were relatively difficult to access,

Table 1. Nation Profiles and Cyber Force Postures in the Persistent Engagement Wargame

Nation	Type	Primary Objectives	Cyber Force
Red	Autocratic- Superpower	Develop offensive cyber options to prepare for the invasion of Green; Conduct influence operations against the Gold elections	36 Units
Blue	Democratic- Superpower	Conduct cyber operations to help defend Green and Gold; Hold Red and Gray networks at risk	30 Units
Purple	Autocratic- Medium Power	Conduct influence operations against the Gold elections; Hold Gold networks at risk	25 Units
Gold	Democratic- Medium Power	Defend national elections from foreign influence operations; Hold Purple networks at risk	25 Units
Gray	Autocratic- Small Power	Conduct cybertheft operations against the other nations	18 Units + Criminal orgs
Green	Democratic- Small Power	Conduct cyber operations to defend Green networks	18 Units

while civilian logistics and local government were more permissive. Networks associated with nuclear capabilities were very difficult to access. Players could either take offensive actions that improved their chances of accessing a target network or employ defensive actions that made their own networks more difficult to access. The number of available targets far exceeded the capacity of any one nation's offensive capacity, forcing them to develop strategies to allocate their limited resources.

Each move in the game represented a two-month period; six moves total a year. This gave players the opportunity to develop an initial strategy, test it over several months of game time, and then modify it as they saw fit. As players gained access to cyber infrastructure, they gained intelligence about the activities of their adversaries. Players then modified their defensive actions or employed counter-cyber units to disrupt their enemies. Specifically, counter-cyber units could hack into adversary infrastructure and conduct offensive cyberattacks against it—effectively stopping any activities supported by that infrastructure. Players could also share information with their allies to help form a shared understanding of the threat and, when possible, work together to counter their mutual adversaries.

Underpinning the players' decisions about force structure and operational employment were a series of game mechanisms designed to represent the nature of modern cybersecurity. For instance, these included an operational risk analysis tool that evaluates each unit's activities to determine whether they were detected by cybersecurity firms. If that occurred, their activities were publicly exposed to all the other players via a public cybersecurity report. This created a dynamic environment in which some information was known to all the players, whereas other information was kept secret, known only to the players who collected it through their covert cyber operations.

At the end of the game, players were assessed based on how well they achieved their nation's objectives. They were also rewarded for maintaining access to adversary networks, conducting influence operations, and acquiring technology through industrial espionage and cybertheft.

Following the game, the players gathered as a group to discuss their force design decisions and operational strategies, providing all participants with an opportunity to learn from their experiences. All game data, including player actions and adjudication results, was captured on move cards, creating a traceable record. Over the course of each game, over 1,000 individual decisions were recorded, creating a rich data source that was used for post-game and cross-game analysis.

FINDINGS

The game's findings reveal the close linkage between force design, operational strategy, and a cyber force's ability to meet national objectives. Having sizable cyber forces was necessary for operational success, but it was insufficient if the player's operational approach wasn't properly aligned. Optimal results occur when a nation has sufficient capacity and a strategy that exploited gaps in its adversary's defenses, while simultaneously blunting the operations directed against themselves.

Post-game analysis revealed that over periods of sustained competition in cyberspace, a nation that over-invests in offense against one adversary may have insufficient forces to meet their overarching national security goals. For example, players frequently aligned significant offensive cyber capabilities against their principal adversaries, oftentimes at the expense of counter-cyber and defensive forces. This limited their ability to respond to adversary intrusions into their own networks.

Separately, nations that had sufficient units aligned to an objective could also underperform based on their operational strategy. In one case, one team got another nation to commit half of its defensive cyber forces to their mutual protection–a significant achievement–but they still underperformed on defense. This was because the team prioritized defense of its commercial and financial sectors, leaving their government and military networks open to exploitation. Players also tended to underinvest in resources needed to combat criminal activity. Force structure alone was not determinant of outcomes.

When it came to defense against election interference, all but one of the allied teams were ineffective. In several instances, players did not allocate enough counter-cyber units in their force design, again, leaving them with limited options to respond to adversary threats. In some cases, intelligence on adversary influence operations was slow to develop, which also hampered their efforts. The most successful teams acquired the intelligence they needed, had sufficient forces, and an operational approach that allowed them to update their targeting priorities and disrupt threats with speed.

In sum, the games revealed several systemic challenges that may be inherent in cyber campaigning. The ability to assess progress is difficult. Even within this relatively bounded representation of cyberspace, players struggled to understand what their adversaries were doing and how well their own forces were performing. For instance, during one iteration, players were asked to rate how well they were performing on their objectives. Most rated themselves highly when, in fact, many were failing. Players often appeared overwhelmed with the information they received, much of which was either vague or ambiguous. This was especially true for democratic nations who needed to understand what both their adversaries and allies were doing. Players also proved resistant to altering their campaign plans, even when there was ample evidence that indicated they should.

IMPLICATIONS FOR U.S. CYBER FORCES

As played, these wargames did not require players to apply USCYBERCOM's organizational structure. Still, they made decisions about the relative balance of forces committed to offense, defense, and disruption. These choices approximate those made by force planners when the Cyber Mission Force was created (U.S. Department of Defense 2014). As such, the games revealed several important lessons about cyber force design that can inform current debates surrounding cyber force structure.

Chief among these is the need for greater numbers of counter-cyber forces, currently housed in the Cyber National Mission Force (CNMF). The games indicate that at the operational level, these forces can have an outsized effect on the ability to frustrate malicious cyber activity. Defensive cyber units also contribute to this mission. However, their ability to strengthen network defenses was generally insufficient for thwarting malicious actors at scale. Currently, less than a quarter of the total U.S. force structure is dedicated to the counter-cyber mission, despite the large number of threats arrayed against the United States. (U.S. Department of Defense 2014). The *Persistent Engagement Wargame* suggests this proportion should be much higher and the U.S. should prioritize growth within the CNMF above other parts of the force.

A related finding is the need to keep counter-cyber forces closely coupled with the larger cybersecurity community. Compared to the real world, the wargame has a simplified information environment. Yet, even with this simplification, players had difficulty understanding what their adversaries were doing and who they should prioritize for counter-cyber targeting. This was less of a problem for offensive cyber units, who generally knew what they needed to target. But information management was critical for effective counter-cyber action. This suggests that the CNMF should remain tightly coupled with the intelligence community, particularly the National Security Agency, and expand partnerships with private cybersecurity companies that can help them inform their targeting priorities.

Another major implication for force design is the need to consider more robust organizations to enable allied cooperation. During the game, allies were most effective at coordinating defensive cyber operations because it was relatively easy to de-conflict which units would protect friendly networks. Players also had some success de-conflicting offensive operations against a common adversary. But synchronizing allied counter-cyber operations was far more difficult. Allies were constantly targeting the same adversary cyber units. On several occasions, multiple allies attacked the same adversary infrastructure on the same move–completely unaware of each other's actions.

This suggests that operational fratricide is a real possibility. At the very least, real allies and partners are probably wasting resources trying to gather intelligence and target the same malicious actors. The secretive nature of cyber operations makes international cooperation difficult. Organizations like the NATO Cyberspace Operation Centre[2] tend to focus on information-sharing and defense of internal networks, which are less sensitive than offensive or counter-cyber operations. However, a major conflict with Russia or China would likely require more cyber resources than any one nation can muster. It is imperative that the U.S. and its allies think through the types of combined organizations they would require, along with the operating concepts needed to synchronize and deconflict offensive and counter-cyber operations during conflict.

LIMITATIONS

While the *Persistent Engagement Wargame* can help cyber leaders understand the longer-term impact of force structure and strategy, it does have several limitations. The game lacks mechanisms to account for law enforcement and other interagency actions that are standard practice for governments. For instance, the FBI and other law enforcement agencies routinely indict foreign cyber criminals and state-sponsored hackers. The State Department can also issue sanctions for individuals or companies engaged in malicious cyber activity. While these actions rarely lead to formal prosecutions, they can disrupt the activities of those actors for at least a limited period.

Additionally, the game should not be used to inform short-term operational decision-making. The target networks were highly abstracted; for instance, gaining access to a network was based on probabilistic outcomes, not technical specifications. Without detailed knowledge of all the target networks represented in the game, it is impossible to determine which network presents the best opportunity for gaining access. Instead, the game should be used to evaluate how the strategies of different nations interact over time.

Lastly, the game does not fully consider the level of proficiency of individual units and how they could change over time. While it is simple enough to add a handicap to represent lower levels of technical expertise, the game does not include mechanisms to account for training or learning that would naturally be gained over time. For example, a cyber unit tasked with gaining access to another nation's critical infrastructure would likely acquire specific industrial control system training to enable them to conduct those operations. This kind of learning does not exist in the game but could be developed in follow-up iterations.

CONCLUSION

Current conventional wargaming practices are not adequate for cyber campaigns. Military cyber organizations should consider adopting the *Persistent Engagement Wargame*, or something similar, to help improve their cyber campaign strategies.

[2] See https://nrdc-ita.nato.int/nato-allied-reaction-force/component-commands/nato-cyber-operation-centre

The game described above can be adapted to fit many potential scenarios involving multiple countries. While this study focused on interstate cyber competition and cooperation prior to conflict, the game can be adapted to examine protracted warfare as well as the transition from competition to kinetic conflict.

The game could also be adapted to study intrastate dynamics, such as how USCYBERCOM cooperates with different government and private organizations in ways that help or hinder each other's efforts. Such applications could be used to help inform analysis of different force generation models, including those involving a separate cyber service or new government agencies. Given the complex threat environment and domestic as well as international interactions therein, operational cyber wargaming is too useful not to use.

ABOUT THE AUTHOR

Jason Vogt is an assistant professor and a core faculty member of the Cyber & Innovation Policy Institute at the U.S. Naval War College. He holds a MA in Global Security Studies from Johns Hopkins University. Vogt previously worked for the Defense Intelligence Agency and served on active duty as an Army officer. He specializes in cyber and wargaming.

REFERENCES

Bao, T., Y. Shoshitaishvili, R. Wang, C. Kruegel, G. Vigna, and D. Brumley. 2017. "How Shall We Play a Game?: A Game-Theoretical Model for Cyber-Warfare Games." In *2017 IEEE 30th Computer Security Foundations Symposium (CSF).* Santa Barbara, CA. https://doi.org/10.1109/CSF.2017.34.

Cancian, Mark F., Matthew Cancian, and Eric Heginbotham. 2023. *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan.* Center for Strategic / International Studies. https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan.

NATO CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence). 2023. *World's Largest Cyber Defense Exercise Locked Shields Kicks Off in Tallinn.* https://www.ccdcoe.org/news/2023/worlds-largest-cyber-defense-exercise-locked-shields-kicks-off-in-tallinn/.

Conti, Gregory, and David Raymond. 2017. *On Cyber: Towards an Operational Art for Cyber Conflict.* Kopidion Press.

Crotty, James, and Elizabeth Daniel. 2022. "Cyber Threat: Its Origins and Consequence and the Use of Qualitative and Quantitative Methods in Cyber Risk Assessment." *Applied Computing & Informatics,* https://doi.org/10.1108/ACI-07-2022-0178.

Curry, John. 1990. *Peter Perla's The Art of Wargaming: A Guide for Professionals and Hobbyists.* Annapolis, MD: Naval Institute Press.

Duncan, Matthew. 2023. "The Evolution of the North American Electrical Reliability Corporation's Grid Security Exercise." In *Cyber Wargaming,* edited by Frank L. Smith, Nina Kollars, and Benjamin Schechter. Washington, DC: Georgetown University Press.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory.* Oxford University Press.

Gold, Jon. 2022. *FBI: Victims Lost Nearly $7 Billion to Cybercrime in 2021.* CSO Online, March 23, 2022. https://www.csoonline.com/article/572345/fbi-victims-lost-nearly-7-billion-to-cybercrime-in-2021.html.

Google Threat Analysis Group. 2023. *Fog of War: How the Ukraine War Transformed the Cyber Threat Landscape.*

Greenberg, Andy. 2018. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History,* August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greenberg, Andy, and Lily Newman. 2023. *China Hacks US Critical Networks in Guam, Raising Cyberwar Fears.* Wired, May 24, 2023. https://www.wired.com/story/china-volt-typhoon-hack-us-critical-infrastructure/.

Harknett, Richard J., and Max Smeets. 2022. "Cyber Campaigns and Strategic Outcomes." *Journal of Strategic Studies* 45 (4): 534–567. https://doi.org/10.1080/01402390.2020.1732354.

Kollars, Nina, and Benjamin Schechter. 2021. *Pathologies of Obfuscation: Nobody Understands Cyber Operations or Wargaming.* Atlantic Council.

Libicki, Martin C. 2017. "The Convergence of Information Warfare." *Strategic Studies Quarterly* 11 (1): 49–65. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf.

Miller, Maggie. 2022. *NATO Prepares for Cyber War.* Politico, March 12, 2022. https://www.politico.com/news/2022/12/03/nato-future-cyber-war-00072060.

Nakasone, Paul M. 2019. "A Cyber Force for Persistent Operations." *Joint Force Quarterly,* no. 92, 10–22. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

Schechter, Benjamin. 2023. "Wargame Research on Cyber and Nuclear Crisis Dynamics." In *Cyber Wargaming,* edited by Frank L. Smith, Nina Kollars, and Benjamin Schechter. Washington, DC: Georgetown University Press.

Schneider, Jacquelyn, Benjamin Schechter, and Rachael Shaffer. 2022. "A Lot of Cyber Fizzle But Not a Lot of Bang." *Journal of Global Security Studies* 7 (2). https://doi.org/10.1093/jogss/ogac005.

Smith, Frank L. III, Nina A. Kollars, and Benjamin H. Schechter. 2024. *Cyber Wargaming: Research and Education for Security in a Dangerous Digital World.* Washington, DC: Georgetown University Press.

Sullivan, D. T., E. J. M. Colbert, B. E. Hoffman, and A. Kott. 2018. "Best Practices for Designing and Conducting Cyber-Physical-System War Games." *Journal of Information Warfare* 17 (3): 92–105. https://www.jstor.org/stable/26633168.

The White House. 2023. *National Cybersecurity Strategy.* Washington, DC. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

U.S. Department of Defense. 2014. *Quadrennial Defense Review 2014.* Washington, DC. https://history.defense.gov/Portals/70/Documents/quadrennial/QDR2014.pdf.

U.S. Department of Justice. 2018. *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations.* Press Release, Office of Public Affairs, October 4, 2018. https://www.justice.gov/archives/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

Received 28 July 2025; Revised 29 October 2025; Accepted 10 December 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 79-85
https://doi.org/10.55682/cdr/rz8a-ncfy

PROFESSIONAL COMMENTARY

Support and Leverage Auxiliaries for Stronger Cyber Defense

Giancarlo J. Moats

United States Air Force, Hanscom Air Force Base, MA, USA

Military auxiliary organizations offer considerable but often neglected potential for improving the U.S. military's cyber defense capabilities and growing the professional ecosystem. These auxiliaries include the Reserves, the National Guard, the Marine Corps Cyber Auxiliary (MCCA), the Civil Air Patrol (CAP), the U.S. Coast Guard (USCG) Auxiliary, and additional entities organized through state authorities. In addition, specialized exercises, such as "Cyber Yankee", enable better use of these auxiliaries and thus they deserve increased support. International initiatives such as the National Guard Bureau's State Partnership Program (SPP) and the Interallied Confederation of Reserve Officers' (CIOR) international cyber event also foster greater engagement and deliver benefits that cannot be achieved through active-duty military efforts alone. All of these capabilities, initiatives, and opportunities stand to improve the generation and use of cyber force by the armed services and U.S. Cyber Command.

Keywords: cyber defense, cyberforce, auxiliary, reserves, Marine Corps Cyber Auxiliary, Cyber Yankee exercise, U.S. Cyber Command, USCYBERCOM

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

The question of whether the U.S. military should create an independent cyber force remains complex and fiercely debated. However, one issue that rarely receives much attention is the positive potential of harnessing military auxiliaries for the cyber domain, regardless of which direction the cyber force debate goes. All the existing services have auxiliary organizations that augment the active forces' respective capacities with additional capabilities that are in short supply or lacking full-time units. These arrangements exist in all warfighting domains, including cyberspace, but they are often underappreciated for the important functions they can fulfill. This article illuminates several key organizations and associated activities to highlight some of the force-multiplying opportunities readily available in these auxiliaries, which are not usually apparent.

I will use the term "auxiliary" to refer to formally recognized organizations that support the military missions, particularly those missions connected to the defense of critical infrastructure. This broad definition helps us better understand the diverse array of entities that could work more closely with active-duty military organizations to improve cyber defense. It is also instructive to appreciate the large and growing landscape of official and semi-official organizations that are responsible for cyber defenses, a landscape that needs to be appreciated as more than just terrain.

GENERAL PURPOSE AUXILIARIES

In the United States, the best-known auxiliary is the National Guard, a state-level standing militia that falls under the authority of its respective governor when not activated to fulfill a federal mission. Similarly, each military branch has dedicated Reserve organizations that provide comparable auxiliary support to their respective military service. These National Guard and Reserve forces are trained and equipped to offer directly employable capabilities for existing active-duty military organizations. Their personnel serve in uniform for limited periods throughout the year and, when not doing so, maintain full-time civilian careers. In many cases, these people use the same skill sets in their civilian jobs that they employ in uniform, with many civilian cyber professionals working part-time in the National Guard, Reserves, or other auxiliary organizations as well. This arrangement benefits the military by having ready access to the industry's best practices that individual Guard and Reserve personnel bring with them.

While the Reserves solely augment active-duty capacities in straightforward connections between their military and civilian careers, the National Guard connects civilian professions with state resources and legal frameworks to federal service when activated. In other words, they bring expertise in state-based systems and authorities to the national defense mission, as well as federal training in cyber to state defense efforts. Also, they may be able to cooperate with state law enforcement and similar organizations below the national level to further complement federal efforts when necessary.

Deeper within the National Guard's structures, and especially relevant to cyber missions, is the West Virginia National Guard's Army Interagency Training and Education Center (AITEC). This Center has been developing new schemes for mission integration and force development with an eye towards the sacred duty of protecting the homeland in all domains, including cyber. Through ongoing initiatives to better coordinate multi-domain defenses, such as a recent critical infrastructure protection workshop that focused on "possible threats to the country's public utilities, resources and cybersecurity systems" (Bodker 2025), the AITEC is providing a crucial foundation for many partnering organizations, including auxiliaries. Together, they learn to forge stronger collaborative and combined defenses against evolving threats. The role of cyber within the overarching defense of critical infrastructure is also intertwined with the other warfighting domains. The AITEC's leadership in integrating all domains helps provide a far more effective defense through the inclusion of additional organizations.

Other auxiliary organizations are also well situated to help in the cyber defense of critical national infrastructure. The Civil Air Patrol (CAP)[1] is a civilian volunteer auxiliary that is formally linked to the U.S. Air Force and receives federal funding. It could use its nationwide membership to support cyber defense by helping with basic cyber training, public outreach on cyber hygiene, and reporting suspicious cyber activity related to aviation or emergency services. The U.S. Coast Guard (USCG) Auxiliary is a uniformed but civilian volunteer organization that is partly funded by the federal government through the Coast Guard and Department of Homeland Security (DHS). It could help protect maritime communities by assisting with training on cyber secure navigation and communications, as well as passing information about possible cyber threats to Coast Guard units that protect the maritime transportation system.[2] Both the CAP and the USCG Auxiliary can accept as members currently serving active duty personnel, enabling additional professional development and connections to critical missions by uniquely qualified military personnel.

CYBER-FOCUSED AUXILIARIES

Military auxiliary organizations specifically relevant to the cyber domain are also being established to benefit from the larger pool of civilian expertise. These auxiliaries, if appropriately integrated, are likely to play a significant role in further shaping America's cyber defense and its corresponding cyber forces.

[1] Civil Air Patrol cyber missions: https://cyber.cap.gov

[2] In a previous edition of the Cyber Defense Review, Lieutenant Colonel (Ret.) Jeffrey J. Fair provided an excellent perspective on these organizations' relevance to the cyber domain (Fair 2022).

The Marine Corps Cyber Auxiliary (MCCA)[3] was created in 2019. It represents the United States' first auxiliary organization wholly dedicated to the cyber domain. By law, this new organization is composed entirely of volunteers with skills and qualifications relevant to cyberspace that can be leveraged to support and augment the active-duty mission requirements of the Marines. MCCA can bring in private sector cyber professionals to help with exercises, training events, and advice on new threats.

To better harness the valuable cyber qualifications of the MCCA members, updated legal guidance needs to be established to allow this auxiliary to fully realize its original mandate. Due to legal restrictions that limit the government's ability to accept gifted services, the MCCA has been limited to only providing support to the Marines in certain restricted capacities instead of broadly augmenting the full mission of their parent active-duty service, as the other long-established auxiliaries are legally capable of doing. Additionally, while CAP and USCG Auxiliary permit active-duty members to serve within their respective organizations, the MCCA does not allow currently serving military personnel to join. This limitation on membership restricts professional development and insight into critical missions. Policymakers should reconsider how best to bring the MCCA into line with the other auxiliary organizations for the benefit of all.

The Coast Guard also has auxiliary cyber capabilities located in its own dedicated Cyber Flotilla.[4] Based out of Fort Meade, the Cyber Flotilla can provide national-level support and assist with the cyber defense of critical infrastructure. As part of the USCG Auxiliary, it is a uniformed civilian volunteer unit connected to Coast Guard Cyber Command through the AUXCYBER augmentation program. Its members are brought in because they already work in cybersecurity. Active duty members in military cyber are also permitted to join. In practice, these volunteers help defend Coast Guard information systems, assist with cyber incident handling and analysis, and support projects to improve the security of digital systems that support Coast Guard missions and the wider maritime transportation system.

The CAP has similar special organizations dedicated to training and developing professionals relevant to the military's cyber defense missions. Programs such as CAP Cyber Missions and the CAP National Cyber Academy provide classroom lessons, online courses, and week-long activities to teach cadets and adult volunteers practical cybersecurity, networking, and system protection skills that align with Air Force and other military needs. These efforts are closely tied to national efforts like the Air & Space Forces Association's CyberPatriot competition and its partnerships with the Cisco Networking Academy. CAP members learn to defend real-world networks, experience they can then bring into military service or other roles that support national cyber defense.

[3] Marine Corps Cyber Auxiliary: https://www.hqmc.marines.mil/Agencies/Deputy-Commandant-for-Information/Information-Maneuver-Division/Marine-Corps-Cyber-Auxiliary

[4] USCG Auxiliary Cyber Flotilla: https://wow.uscgaux.info/content.php?unit=054-22-12

National Guard organizations also have cyber-specific units that organize and participate in regional cyber exercises designed to hone critical skills. Of these exercises, *Cyber Yankee* is perhaps the best-known for practicing cyber defense and response activities against contemporary threats, such as a massive cyber-attack against the region (Lohmann and Brown 2025; Pomerleau 2022, 2025). Held in the Northeastern U.S., the participants include Guard cyber forces and cyber professionals from industry, academia, varying echelons of governments, and international partners. The participants enhance cyber defense practices and develop strategic partnerships for the real-world, beyond this exercise. Because these exercises put auxiliary organizations front-and-center with tangible impacts upon military readiness and threat awareness, they should be afforded even greater attention and resourcing. Doing so will help develop and deepen further layers in cyber defenses of critical infrastructure at home and abroad.

CIVILIAN AND INTERNATIONAL ANALOGS

Looking even further beyond military auxiliaries, cyber defense should incorporate civilian organizations that also perform auxiliary-like functions. After all, civilian organizations typically represent the first line of defense against cyber-attacks at the local level. Their defenses could benefit from and contribute to stronger connections with military cyber organizations. Examples of such civilian organizations include the Cyber Resilience Corps[5] led by University of California Berkeley's Center for Long-Term Cybersecurity and the CyberPeace Institute; the Texas Cybersecurity Clinic[6] at the University of Texas at Austin; and the Michigan Cyber Civilian Corps (MiC3).[7]

Each of these capable entities engages with community organizations to provide critical support for cyber defense and incident response. In doing so, they build resilience, enhance the professional and private ecosystem, and raise broader awareness of cybersecurity as a critical facet of national defense. Additionally, each of these organizations has official academic or governmental connections to their respective state governments, through which they can connect with capabilities and authorities that reside with their corresponding state's National Guard.

Further, it is always worth remembering that our international allies and partners face similar threats and have their own corresponding organizations to handle these matters. Here again, our auxiliaries can provide critical connective tissue, such as through the National Guard's State Partnership Program (SPP).[8] The SPP is a unique arrangement that pairs the National Guard of different American states with allied and partner nations. One of the most

[5] See https://cltc.berkeley.edu/program/cyber-resilience-corps

[6] See https://www.strausscenter.org/apply-here-cyber-clinic

[7] See https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3

[8] See https://www.nationalguard.mil/Leadership/Joint-Staff/J-5/International-Affairs-Division/State-Partnership-Program

relevant examples for cyber is the pairing between the state of Maryland and the country of Estonia. Maryland's National Guard collaborates with their Estonian counterparts, leveraging their bilateral arrangement directly. This allows them to use state, federal, and international resources to advance both their separate and combined interests. Additionally, with U.S. Cyber Command (USCYBERCOM) located in Fort Meade, Maryland, and Estonia's hosting of the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO CCDCoE), both the U.S. and Europe can leverage their respective professional ecosystems to further enhance and defend their close cyber connection.

Beyond the SPP, there are other auxiliary-centric opportunities overseas, most notably through the Interallied Confederation of Reserve Officers (*in French:* Confédération Interalliée des Officiers de Réserve or CIOR). The CIOR is a unique international organization that focuses on the professional development and partnering of reserve components of allied militaries. Among the myriad of related activities, CIOR organizes an international cyber event[9] for "advancing cyber capabilities within military reserves," as well as providing NATO leaders with expert insight. By leveraging special pathways for strategic engagement, such as those provided by the CIOR, allies can better address threats to the whole as well as individual member states. Such engagements can be conducted in addition to the corresponding active-duty military partnerships and exercises that occur within the larger NATO enterprise, thereby fostering a stronger cyber defense-in-depth throughout the Alliance.

CONCLUSION

If the contributions of auxiliaries and related organizations are properly included in planning and operational considerations, a far more capable and robust ecosystem for cyber defense is possible, force multiplying what the active-duty military alone could provide. Conversely, if an independent cyber force or Department were ever established without due regard for strengthening the relationships among existing auxiliaries and exercises such as *Cyber Yankee*, there is considerable risk of inadvertently muddling and undermining the country's capabilities and capacities in this domain. In the worst case, neglecting these auxiliaries and related organizations while creating a completely new cyber service could create more inter-organizational gaps and seams that adversaries could exploit. Thus, whatever the future of USCYBERCOM, with or without a new cyber force, it will be critical for cyber auxiliaries to be given due regard for all that they can do in this domain.

[9] See https://cior.net/activities/international-cyber-event

ABOUT THE AUTHOR

Lieutenant Colonel Giancarlo Moats is a Command Pilot and Multi-Domain Strategist in the Michigan Air National Guard. He has operational experience across five continents and four oceans, including more than 1,900 hours of combat flight time in three Air Force major weapon systems. His previous assignments include multiple operational flying squadrons, the headquarters staff for a theater special operations command, and the headquarters staff for the Joint Force Air Component Commander of USSTRATCOM. Currently, he resides in Massachusetts with his wife and four children.

ACKNOWLEDGMENTS

The author would like to provide special thanks to Professor Francesca Lockhart of the UT Austin Strauss Center, Ms. Kathryn Dura at MIT, Ms. Valorie Aguilar and Major Erik Salzman at the Marine Corps Cyber Auxiliary, Colonel Gina Nichols at the AITEC, and faculty in the U.S. Naval War College's Cyber and Innovation Policy Institute.

REFERENCES

Bodker, Erica. 2025. *West Virginia Guard Hosts Workshop to Address Potential Infrastructure Threats.* U.S. Army, April 22, 2025. https://www.army.mil/article/284834/west_virginia_guard_hosts_workshop_to_address_potential_infrastructure_threats.

Fair, Jeffrey. 2022. "America's Cyber Auxiliary: Building Capacity and Future Operators." *The Cyber Defense Review* 7 (2). https://www.jstor.org/stable/48669292.

Lohmann, Sarah, and Jason Brown. 2025. "Voices from Cyber Yankee: Lessons for Strengthening Critical Infrastructure Cyber." *The Cyber Defense Review* 10 (2): 141–158. https://www.jstor.org/stable/48849639.

Pomerleau, Mark. 2022. "Cyber Yankee Exercise Helps National Guard Mature Partnership with Cyber Command," June 30, 2022. https://defensescoop.com/2022/06/30/cyber-yankee-exercise-helps-national-guard-mature-partnership-with-cyber-command/.

Pomerleau, Mark. 2025. *National Guardsmen Receive Brief from Volt Typhoon Utility Victim at Cyber Exercise.* DefenseScoop, May 22, 2025. https://defensescoop.com/2025/05/22/volt-typhoon-utility-victim-national-guard-cyber-yankee-exercise/.

Received 1 August 2025; Revised 14 December 2025; Accepted 17 December 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 87-97
https://doi.org/10.55682/cdr/gez4-hjmv

PROFESSIONAL COMMENTARY

U.S. Cyber Command Evolution and the Increasing Role of the Private Sector

Greg Rattray*[1][2], Michelle J. Lee†[2]

[1]Cyber Defense Assistance Collaborative (CDAC), New York, NY, USA
[2]Next Peak, New York, NY, USA

The United States must effectively leverage all its capabilities to prepare for and prosecute conflicts with a cyber dimension. Both U.S. Cyber Command (USCYBERCOM) and the private sector play crucial roles. However, their efforts remain largely uncoordinated due to limits in traditional approaches to private-sector collaboration. This paper advocates establishing collaboration mechanisms to increase the effectiveness of both USCYBERCOM and the private sector, improving cyber defense at home and in support of friends and allies. Examples such as the Cyber Defense Assistance Collaborative (CDAC) illustrate how both general capacity building and targeted defense assistance are increasingly led by private companies. Key contexts in Europe and Asia highlight the need for deeper private-sector involvement. Numerous current and potential cyber conflict scenarios show where private actors can offer more effective support through intelligence, defensive capabilities, and training that can supplement or sometimes surpass military cyber operations. We conclude that USCYBERCOM should work more directly with the private sector. We propose establishing a Cyber Command Private Sector Collaboration Center (CCPSCC) to enable consistent blue-force tracking across government and private activities; coordinated threat hunting; and improved operations centers supporting cyber defense in conflict.

Keywords: U.S. Cyber Command, USCYBERCOM, Public-private collaboration, cyber defense, threat intelligence sharing, operational coordination, digital resilience

* Corresponding author: greg.rattray@nextpeak.net
† Both authors contributed equally to this research.

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

As cyberattacks increasingly target critical infrastructure, government systems, and commercial enterprises, the role of the private sector in cyber defense has expanded (Rattray and Lee 2025). The U.S. private sector has become a target, and global technology infrastructure serves as the battlefield. Consequently, companies now play a direct role in countering cyber threats by operationally and tactically influencing the digital dimension of modern conflict, not only supporting or provisioning cyber defense but also actively absorbing and responding to attacks in active geopolitical disputes.

This expanding role places private actors in close proximity to U.S. Cyber Command (USCYBERCOM). As companies become more capable and more active in their response to nation-state threats, their operations increasingly intersect with this Command's mission space. However, coordination remains fragmented, both between companies themselves and with government organizations, particularly USCYBERCOM.

Existing efforts such as the National Security Agency's Cybersecurity Collaboration Center (NSA CCC) and the Department of Homeland Security's Joint Cyber Defense Collaborative (DHS JCDC) have begun to improve public-private coordination. But they were not designed to manage cyber conflicts overseas, provide assistance to allies and friendly nations, or organize private sector support at the scale and tempo now required. The persistent separation between private and national defense operations raises critical questions around co-learning, deconfliction, and the mechanisms required to align efforts without compromising autonomy or effectiveness. USCYBERCOM's ability to adapt to this shared battlespace and leverage private sector capabilities and collaboration will shape not only the efficacy of cyber defense but also the broader resilience of U.S. and allied digital infrastructure.

This paper focuses on three key dimensions of private sector involvement. First, we examine the increasing role of private companies in defending allies and partners during cyber conflicts by assessing how firms engage in cyber defense operations. Second, we consider how the geopolitical realities of the 2020s, such as the war in Ukraine and the potential for conflict over Taiwan, have reinforced and accelerated this trend. Finally, we evaluate the implications for USCYBERCOM, particularly in defining its authority, coordination with private actors, and its evolving role in cyber operations overseas.

PRIVATE SECTOR DOMINANCE IN CYBER DEFENSE

We must understand the private sector's growing role in strengthening the cyber defenses of U.S. allies and partners at the national level. Foundational cyber defense tools and capabilities—ranging from endpoint protection to advanced threat intelligence to artificial intelligence—are predominantly developed, maintained, and operated by private industry. Because most cyber defense occurs at the enterprise level, private companies are often best positioned to engage in cyber defense. These efforts depend not just on public-sector strategies and national capabilities, but on the ability of private actors—individually and in collaboration—to take practical steps to defend themselves and assist others. Such actions can include delivering threat intelligence and situational awareness, offering licensing and training for cyber tools and tech, and developing operational procedures that enable cyber defenders to deploy tools effectively in complex threat environments (Kollars and Poznansky 2021).

Ukraine offers a clear example of this shift. As Russia launched its 2022 re-invasion, cloud service providers and cybersecurity firms rapidly mobilized to help Ukraine withstand waves of digital and kinetic attacks. Microsoft, for instance, detected and neutralized the "FoxBlade" malware within hours of the invasion (Constantinescu 2022). It then helped Ukraine migrate critical government systems to Azure—offering over $400 million in cybersecurity support (Smith 2022). Recorded Future (2022) deployed its threat intelligence platform at no cost to Ukrainian defenders, enhancing situational awareness as attacks intensified.

Other firms followed suit, reinforcing Ukraine's digital infrastructure on multiple fronts. Cloudflare expanded *Project Galileo*[1] to protect Ukrainian public and nonprofit websites from Distributed Denial of Service (DDoS) attacks and even redesigned its servers in the region to self-wipe if compromised (Tomé, Belson, and Berdan 2023). Google's *Project Shield*[2] defended Ukrainian media and government platforms from state-sponsored disinformation and phishing campaigns. In parallel, Cisco's Talos Intelligence Group launched *Project PowerUp* to counter Global Positioning System (GPS) jamming and cyberattacks on Ukraine's power grid (Marshall 2023). They developed and delivered specialized devices that maintained accurate timing without GPS—valued at $1 million each.

The speed and flexibility of private companies stand in contrast to the bureaucratic processes of government. Private companies have acted quickly—sometimes within days or even hours—while official government channels remain constrained by legal and procedural hurdles. The Cyber Defense Assistance Collaborative (CDAC)[3] offers a compelling example of a private sector-led initiative operating on the front lines of cyber defense against foreign adversaries—particularly amid the war in Ukraine (Temple-Raston 2022). CDAC is a volunteer coalition involving over 30 private technology companies and U.S. government agencies that provide intelligence, technology, training, and advisory services to Ukrainian institutions. As of January 2025 (Rattray and Lee 2025), CDAC has coordinated over $40 million in cyber defense aid, including 2,600 tools and 1,600 training credits delivered to 25 Ukrainian entities.

[1] See https://www.cloudflare.com/galileo/

[2] See https://projectshield.withgoogle.com

[3] See https://crdfglobal-cdac.org/

A leading example of CDAC's work is its centralized threat intelligence aggregator, *Voitheia* (CDAC 2024). Companies such as Threat Quotient, Recorded Future, and Google Cloud's Mandiant—alongside entities like the Cyber Threat Alliance and the U.S. Cybersecurity and Infrastructure Security Agency (CISA)—contributed to the platform, which seeks to de-duplicate and prioritize intelligence for a range of Ukrainian recipients.

CDAC's operating principles—voluntary engagement, shared threat intelligence, and mission-aligned collaboration—became a model for how private industry could respond to digital conflict. According to the Center for Security and Emerging Technology, former U.S. government officials and industry experts agree that technology companies have the freedom to move swiftly in comparison to the U.S. government with its legal processes and procurement procedures (Fox and Probasco 2023). Continuing CDAC collaboration since the spring of 2022 across all major U.S. government agencies—the National Security Council (NSC), the Office of the National Cyber Director (ONCD), and the Departments of State, Defense (now War), and Homeland Security—has continually validated the need for and effectiveness of private sector cyber defense assistance.

The structure and funding for U.S. government support for this assistance have been indeterminate. Long-term commitments have yet to materialize. Without operational channels for co-learning, both public and private sides risk working in silos during active conflict and undermining the broader effectiveness and resilience of allied defenses. In 2025, as U.S. government support for Ukraine's cyber defense has diminished, the private sector's contributions have become more critical than ever (Council on Foreign Relations 2025). Embracing a more flexible, forward-leaning posture toward private sector engagement with the U.S. government, to include USCYBERCOM, will be essential to building an integrated cyber defense posture that can meet the demands of modern geopolitical conflict.

USCYBERCOM lacks a formal mechanism to collaborate proactively and continuously with many of the technology companies that operate on the digital front lines. Its role in Ukraine is largely opaque. There is no established process for synchronizing activities, sharing insights, or learning collectively from ongoing conflicts. As a result, operational lessons—from coordination challenges to the resilience and recovery of Ukrainian networks—remain unlearned and efforts to provide cyber defense assistance to the Ukrainians are fragmented.

Relying on traditional contracting or federal funding authorities cannot solve this problem. The U.S. State Department and Department of Defense (DoD, now Department of War) were unable to move resources to companies at the speed demanded by the conflict; some efforts have been stalled for three to four years. Effective cyber defense during active aggression depends on private sector partners who can act operationally—paid or unpaid—without waiting for procurement systems to catch up. Crucially, companies are not motivated to participate in these efforts solely for profit. Across Ukraine, Albania, and other contexts, firms have stepped in voluntarily out of a sense of responsibility to assist, a broader moral commitment to maintaining a safe and stable cyberspace, and a clear self-interest in preserving the digital ecosystems and global markets on which their businesses depend. For major technology firms, the security of these environments is directly tied to the viability of their platforms and the customers who rely on them. For cybersecurity companies, instability threatens both current operations and future markets.

A move by the People's Republic of China (PRC) against Taiwan would likely prove extremely disruptive across the global technology and cyber environment. The CDAC approach described in the next section demonstrates how private sector partners can contribute to both phases: helping prepare a partner, such as Taiwan, before a crisis, and supporting active defense, as seen in Ukraine. While significant differences exist in the context of cyber defense assistance to Taiwan to resist potential PRC aggression, most U.S.-based tech and cybersecurity companies have left the PRC market. Discussions within CDAC have indicated strong support by the companies regarding exploring such assistance efforts. These examples underscore why USCYBERCOM must find ways to collaborate with private companies already operating in the battlespace.

SHAPED BY CONFLICT: PRIVATE SECTOR ROLE IN CYBER ASSISTANCE

The success of CDAC has prompted interest in adapting its model to other regions, particularly Taiwan. At the end of 2024, Chinese President Xi Jinping reaffirmed plans to reunify Taiwan with mainland China, which raised expectations of increased cyberattacks aimed at disrupting Taiwan's government, economy, and military, and deterring U.S. allied involvement (Boyle 2024).

Taiwan faced over 2.4 million cyberattack attempts daily in 2024—twice the 2023 average (Lemos 2025). In response, Taiwan has turned to private sector partnerships, as many Western cybersecurity firms—including those affiliated with CDAC—have sought to support Taiwan's cyber defenses. This activity has the potential to mirror Ukraine's private sector-driven cyber defense (Groll and Vicens 2023). These capabilities could bolster Taiwan's digital resilience amid growing cyber pressure from China (Kramer et al. 2024). To explore the viability of applying CDAC's Ukraine-tested methodologies, Greg Rattray—Executive Director of CDAC—visited Taiwan in October 2024. Following meetings with Taiwan's National Security Council, Ministry of Digital Affairs, Administration for Cyber Security, the American Institute in Taiwan, and technology firms, it was clear that interest was strong, although sustained coordination remains nascent.

Ukraine and Taiwan illustrate a broader pattern: geopolitical flashpoints are increasingly drawing private sector actors into the national security arena in the realm of cyber defense. Similar dynamics are unfolding in Europe, where countries such as Moldova, the Baltic states, and Poland are experiencing cyber campaigns that mirror early-stage Russian cyber operations against Ukraine (Antoniuk 2025; Bajarūnas 2025; Ribeiro 2025). These developments not only embed the private sector more deeply in national defense ecosystems but also emphasize the need for structured coordination across actors and regions. In this emerging landscape, USCYBERCOM is the natural leader to shape and scale these partnerships into a more cohesive operational strategy. The private sector can usefully team with this Command in potential conflicts by allowing the private sector to focus on provisioning the best possible defenses while USCYBERCOM focuses on planning and execution of offensive operations as appropriate.

THE CASE FOR STRONGER PUBLIC-PRIVATE CYBER COLLABORATION

Cyber conflicts have exposed critical structural gaps between the speed and scale of private action and the formal mechanisms available to USCYBERCOM to coordinate with these actors. As private companies take on larger roles in defending allied and partner networks during active conflicts, USCYBERCOM's current frameworks—built primarily for government-led operations—struggle to provide the visibility, synchronization, and shared situational awareness needed to operate effectively in a blended public-private battlespace.

This evolving landscape makes stronger collaboration with private industry not simply beneficial but necessary. Without deliberate integration, U.S. cyber operations risk fragmentation, duplication of effort, and missed opportunities to learn from ongoing real-world defense activities. One of the most immediate challenges is establishing a more direct and structured interface between USCYBERCOM and private sector cyber defense assistance companies and operators.

A critical area of improvement is the development of comprehensive blue force tracking mechanisms that provide visibility into the cyber defense activities and operations conducted by both government and private sector entities. Although U.S. government organizations remain interested in the limited CDAC-led blue force tracking effort in Ukraine to better understand the delivery, effectiveness, and impact of cyber defense assistance, the initiative continues to face several challenges. First, the Ukrainians lacked the bandwidth to provide feedback and assist with the tracking of efforts. Second, the blue force delivery efforts by providers were uncoordinated and completed on an ad-hoc basis. Finally, such a complex analytic undertaking requires programmatic commitment, dedicated staff, and sustained financial investment. A USCYBERCOM-sponsored blue force tracking effort conducted jointly with the private sector could prove crucial in coordinating blue force assistance delivery efforts, decreasing inefficiencies and friction in the process, and helping to identify lessons for providing effective cyber defense assistance in future similar situations.

Additionally, USCYBERCOM should explore coordinated threat-hunting operations and create Security Operations Centers (SOCs) in collaboration with private sector partners. Many of the world's most advanced cybersecurity capabilities reside within private industry, which makes it imperative for USCYBERCOM to leverage these resources in proactive defense efforts. Similarly, lessons from U.S. assistance and collaboration with Albania, Costa Rica, and Japan—where private sector entities played key roles in mitigating nation-state cyber threats—should inform the development of future collaborative frameworks. In each case, industry actors filled critical gaps in national response: Microsoft supported Albania's recovery following Iranian cyberattacks and provided mitigation assistance to Costa Rica during the 2022 Conti ransomware campaign (Microsoft Security Threat Intelligence Center 2022; Datta and Acton 2022). In Japan, firms like Nippon Telegraph and Telephone (NTT) partnered with CISA to strengthen cyber defenses against persistent regional threats (NTT Corporation 2023).

Beyond direct operational collaboration, USCYBERCOM needs to help drive U.S. national policy alignment and institutional support to ensure that private companies engaging in cyber defense assistance operate within a clear legal and regulatory framework. The experiences in Ukraine and Taiwan highlight the challenges of private sector participation in geopolitical conflicts, where companies must navigate complex legal, financial, and diplomatic risks. USCYBERCOM should work with policymakers to establish clear guidelines for private sector engagement in cyber conflicts, including frameworks for liability protection, contractual agreements, and information-sharing protocols. In the case of Taiwan, the Ministry of Digital Affairs and the Administration for Cyber Security are actively working to enhance the nation's cyber resilience. Still, further collaboration with the U.S. and the private sector is needed.

BUILDING A U.S. CYBER COMMAND PRIVATE SECTOR COLLABORATION CENTER (CCPSCC)

Current mechanisms—such as USCYBERCOM's Under Advisement (UNAD) programs and other routine collaboration efforts—were not designed for urgent circumstances involving national-security-grade threats (CYBERCOM 2023). These programs support steady-state information sharing, not the rapid and synchronized action required during crises on the scale of Russia's invasion of Ukraine or a potential conflict over Taiwan. In such scenarios, private companies are already "in the fight." Their executives have repeatedly demonstrated a willingness to engage out of necessity, responsibility, and strategic interest. What is needed is not a peacetime advisory structure but a conflict-focused collaboration construct.

To meet this challenge, we propose the creation of a *Cyber Command Private Sector Collaboration Center (CCPSCC)*. This would be a permanent, mission-driven organization that serves as the primary interface between USCYBERCOM, other government entities, and private sector partners. The CCPSCC would formalize operational collaboration by leveraging existing relationships, programs, and trust to identify key contingencies, support planning and execution of cyber defense operations, and rapidly provision critical capabilities abroad.

Essentially, USCYBERCOM must have a deep programmatic commitment to operational collaboration with the range of key private sector actors, involving ongoing identification of key contingencies, planning, and conduct of operations. Such a CCPSCC would require a dedicated staff that includes both the Command, other government organizations, and the private sector with the ability to mobilize assets for specific planning efforts and operational activities. The CCPSCC should consider adopting aspects of the British National Cyber Security Centre's approach, where much of its work is carried out in an open, unclassified environment, complemented by a deeply technical and classified side (NCSC 2025). The CCPSCC would require a senior USCYBERCOM leader as the head with the proper authority, both legally and in organizational commitment, as well as private sector leaders able to commit their organizations and people to enable timely operational decisions and oversee joint actions. Undoubtedly, complex issues to resolve—such as operational security and the use of classified material—arise regarding participation in establishing a CCPSCC and conducting activities.

The lessons learned from establishing the NSA's CCC, DHS's JCDC, the Federal Bureau of Investigation (FBI)-led botnet take downs, and other operational public-private collaborations should guide the way (NSA 2025; CISA 2025). The CCC has enabled deep threat intelligence sharing and attack surface management with the defense industry, overcoming security clearance and operational issues. The JCDC has established relationships with key critical infrastructure and technology players and has proven able to provide assistance (New York Cyber Task Force 2023). The FBI has likewise developed operational approaches to synchronize joint activities with private sector partners that focus on identifying, pursuing, and defeating adversaries, including botnets leveraged by Russia and the PRC (Edgar 2024).

Building the CCPSCC will come with real challenges that must be addressed from the outset. First, USCYBERCOM will need to clearly define the Center's mandate to lead operational collaboration in preparing for and executing cyber defense with the private sector. It will also need to formalize coordination with other agencies—such as NSA, CISA, and the combatant commands—to avoid mission overlap and interagency friction. Doing so requires assigning operational leadership and codifying supporting roles.

Second, security classification and clearances remain a structural barrier. Without fast-track clearances, shared analytic environments, or rapid sanitization processes, private companies could remain locked out of operational coordination in real time. Seeking approaches that allow for operationally relevant collaboration at the unclassified level will speed the conduct and effectiveness of joint activities.

The CCPSCC should focus on a prioritized set of contingencies for action in the Indo-Pacific, Europe, and the Middle East. Engagement with the appropriate combatant commands would be essential. The Center should convey a clear message to foreign partners regarding an engagement model, the Center's capabilities, and potential assistance. Specific operational activity will vary by contingency but the Center should seek to achieve consistency to maximize efficiency and learning over time.

The CCPSCC should have federal authority to provide funding to relevant private organizations. A funding approach that grants significant discretion to the CCPSCC—allowing it to rapidly deploy resources and enable private sector action—is critical. Situational awareness provided by the CCPSCC would include both understanding adversary activity and the status of defensive efforts. As described earlier, Ukrainian cyber centers and key government and critical infrastructure enterprises were provided with timely, ongoing attack-surface monitoring and cyber-intelligence platforms. They also received details on emerging adversary command and control (C2) structures and tactics, techniques, and procedures (TTPs). Together, these capabilities gave Ukrainian defenders essential visibility. A CCPSCC could organize and conduct such activities more effectively and at scale.

Contingency plans should seek to clarify how to link available capabilities and resources to improved defense and resiliency outcomes in a prioritized way. For example, is uplifting in-country telecommunications resiliency the most important priority? Do private sector players have lessons to share? Can resources be provided? Will the adversary seek to cut undersea fiber-optic cables? Such planning will need to involve numerous stakeholders: USCYBERCOM, other combatant commanders, Department of War (DoW), Department of State, interagency partners, and private sector players engaged in the contingency.

Additionally, the CCPSCC should orchestrate ongoing cyber defense activities and assistance. A primary focus would be enabling key hubs in an allied or partner nation, such as national or regional cyber centers, national Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs), and industry information-sharing and analysis centers. Private sector actors would likely have the availability, expertise, and scale to assist private industry and non-national security agencies, such as central banks, power, and telecommunications companies. USCYBERCOM's hunt forward teams are best positioned to support national security organizations, where missions typically require higher levels of operational security, classified tools, and access to sensitive intelligence. CCPSCC could help existing efforts by enabling the use of select private sector talent and capabilities—particularly through the creation of joint teams operating under government direction. Establishing such a system would expand the options for generating the additional forces needed to support these operations.

ONBOARD THE PRIVATE SECTOR NOW

Deep private sector involvement in cyber conflicts that also involve USCYBERCOM is already occurring. Private sector companies provide the tools and services used by cyber defenders across the globe every day. Enabling defenders to improve deterrence and digital resilience will be needed before and during any potential conflict. The knowledge and lessons learned by the private sector in Ukraine and elsewhere can be applied going forward. Although USCYBERCOM and private sector actors desire similar outcomes, surprisingly little operational collaboration currently occurs.

USCYBERCOM should build the necessary programs, operational approaches, authorities, and resources to improve. Creating a Cyber Command Private Sector Collaboration Center would be an important step in the right direction. The time to act is now.

ABOUT THE AUTHORS

Dr. Greg Rattray is partner and co-founder of Next Peak LLC, a cybersecurity and risk management firm. He is also currently the Executive Director of the Cyber Defense Assistance Collaborative (CDAC), as well as the Chief Strategy and Risk Officer for Andesite and a senior advisor to the Red Cell Partners Cyber practice. Dr. Rattray previously served as the Global Chief Information Security Officer (CISO) at JPMorgan Chase and established their cyber defense strategy and program. As head of Global Cyber Partnerships, he led key industry initiatives including the establishment of the Financial Systemic Analysis and Resiliency Center (FSARC) and the Financial Cybersecurity Profile. He has previously served as Director for Cybersecurity in the White House, commanded the Operations Group of the Air Force Information Warfare Center, pioneered the Department of Defense (DoD) and U.S. national cyber exercise programs, and initiated the Air Force and DoD partnership with the defense industry.

Ms. Michelle J. Lee is a Senior Analyst at Next Peak LLC, a consulting firm specializing in cyber risk, geopolitical analysis, and digital resilience. She previously worked as a research assistant at Harvard Law School's Berkman Klein Center and the MIT Sloan School of Management. Michelle holds a B.A. in Media Arts and Sciences and Sociology from Wellesley College.

ACKNOWLEDGMENTS

The authors acknowledge the support of the U.S. Naval War College and thank the participants at the 2025 Cyber and Innovation Policy Institute Summer Workshop for their helpful feedback.

REFERENCES

Antoniuk, Daryna. 2025. "Moldova's Pro-EU Party Wins Election amid Cyberattacks, Kremlin Interference," September 29, 2025. https://therecord.media/moldova-election-pro-eu-party-wins-ddos-incidents-influence-ops.

Bajarūnas, Eitvydas. 2025. "Russia's Hybrid Warfare Tactics Target the Baltics," May 27, 2025. https://jamestown.org/russias-hybrid-warfare-tactics-target-the-baltics/.

Boyle, Seamus. 2024. "In a Crisis, Could China Coerce Taiwan Through Cyberspace?," February 29, 2024. https://thediplomat.com/2024/02/in-a-crisis-could-china-coerce-taiwan-through-cyberspace/.

CDAC (Cyber Defense Assistance Collaborative). 2024. *Case Study: Threat Intelligence Sharing,* January 4, 2024. https://crdfglobal-cdac.org/case-study-threat-intelligence-sharing/.

CISA (Cybersecurity and Infrastructure Security Agency). 2025. *Joint Cyber Defense Collaborative.* https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative.

Constantinescu, Vlad. 2022. "New FoxBlade Malware Hit Ukraine Hours Before Invasion, Microsoft Says," March 1, 2022. https://www.bitdefender.com/en-us/blog/hotforsecurity/new-foxblade-malware-hit-ukraine-hours-before-invasion-microsoft-says.

Council on Foreign Relations. 2025. *Here's How Much Aid the United States Has Sent Ukraine,* July 15, 2025. https://www.cfr.org/article/how-much-us-aid-going-ukraine.

CYBERCOM. 2023. *CYBERCOM's Under Advisement to Increase Private Sector Partnership,* June 29, 2023. https://www.cybercom.mil/Media/News/Article/3444464/cybercoms-under-advisement-to-increase-private-sector-partnerships-industry-dat/.

Datta, Pratim Milton, and Thomas Acton. 2022. "Ransomware and Costa Rica's National Emergency: A Defense Framework and Teaching Case." *Journal of Information Technology Teaching Cases* 12 (3). https://doi.org/10.1177/20438869221149042.

Edgar, Timothy. 2024. "Recent Botnet Takedowns Allow US Government to Reach Into Private Devices," March 13, 2024. https://www.lawfaremedia.org/article/recent-botnet-takedowns-allow-u.s.-government-to-reach-into-private-devices.

Fox, Christine H., and Emelia Probasco. 2023. *Volunteer Force: US Tech Companies and Their Contributions in Ukraine.* https://doi.org/10.51593/20230015.

Groll, Elias, and A. J. Vicens. 2023. *A Year After Russia's Invasion, the Scope of Cyberwar in Ukraine Comes into Focus.* CyberScoop, February 24, 2023. https://cyberscoop.com/ukraine-russia-cyberwar-anniversary/.

Kollars, Nina, and Michael Poznansky. 2021. *Statecraft and Strategy Under the Eroding Monopoly of Cyber Intelligence.* Council on Foreign Relations, August 31, 2021. https://www.cfr.org/blog/statecraft-and-strategy-under-eroding-monopoly-cyber-intelligence.

Kramer, Franklin D., Philip W. Yu, Joseph Webster, and Elizabeth Sizeland. 2024. "Strengthening Taiwan's Resiliency," July 2, 2024. https://www.atlanticcouncil.org/in-depth-research-reports/report/strengthening-taiwans-resiliency/.

Lemos, Robert. 2025. "As Tensions Mount With China, Taiwan Sees Surge in Cyberattacks," January 14, 2025. https://www.darkreading.com/cyber-risk/as-tensions-with-china-mount-taiwan-sees-surge-in-cyberattacks.

Marshall, Joe. 2023. *Project PowerUp – Helping to Keep the Lights on in Ukraine in the Face of Electronic Warfare.* Cisco Talos Blog, December 4, 2023. https://blog.talosintelligence.com/project-powerup-ukraine-grid/.

Microsoft Security Threat Intelligence Center. 2022. *Microsoft Investigates Iranian Attacks Against the Albanian Government.* Microsoft Security Blog, September 8, 2022. https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/.

NCSC (National Cyber Security Centre). 2025. UK Government. https://www.ncsc.gov.uk/.

New York Cyber Task Force. 2023. *Bridging the Trust Gap.* Columbia University School of International and Public Affairs. https://www.sipa.columbia.edu/sites/default/files/2023-12/NYCTF%202023%20-%20Trust%20Gap%20report%20(web).pdf.

NSA (National Security Agency). 2025. *Cybersecurity Collaboration Center.* https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/.

NTT Corporation. 2023. *NTT Joins US Government Public-Private Cybersecurity Initiative JCDC,* January 12, 2023. https://group.ntt/en/newsrelease/2023/01/12/230112a.html.

Rattray, Greg, and Seungmin (Helen) Lee. 2025. *Cyber Defense Assistance and Ukraine: Lessons and Moving Forward,* March 1, 2025. https://www.aspendigital.org/wp-content/uploads/2025/03/Aspen-Digital_Cyber-Defense-Assistance-and-Ukraine_April-2025.pdf.

Recorded Future. 2022. "Ministry of Digital Transformation of Ukraine and Recorded Future Sign Memorandum of Cooperation," December 6, 2022. https://www.recordedfuture.com/press-releases/120622.

Ribeiro, Anna. 2025. "Poland Faces Record Wave of Russian Cyber Sabotage, Sets €1 Billion Defense Budget," September 17, 2025. https://industrialcyber.co/critical-infrastructure/poland-faces-record-wave-of-russian-cyber-sabotage-sets-e1-billion-defense-budget/.

Smith, Brad. 2022. *Extending Our Vital Technology Support for Ukraine,* November 3, 2022. https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/.

Temple-Raston, Dina. 2022. *EXCLUSIVE: Rounding up a Cyber Posse for Ukraine,* November 18, 2022. https://therecord.media/exclusive-rounding-up-a-cyber-posse-for-ukraine.

Tomé, João, David Belson, and Kristin Berdan. 2023. *One Year of War in Ukraine: Internet Trends, Attacks, and Resilience,* February 23, 2023. https://blog.cloudflare.com/one-year-of-war-in-ukraine/.

Received 1 August 2025; Revised 30 November 2025; Accepted 9 December 2025

✧ Replace ✧

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 101-112
https://doi.org/10.55682/cdr/74cw-6fqw

RESEARCH ARTICLE

Evaluating Alternative Models for Organizing U.S. Cyber Forces

Nick Starck*, Todd Arnold

Army Cyber Institute, West Point, NY, USA

Despite the significant investment of attention and resources, the Pentagon and armed services continue to struggle to find, train, and retain the cyber personnel needed for great power competition. The 2025 National Defense Authorization Act directs an evaluation of alternative organizational models for U.S. cyber forces. Traditional models for military force generation, including special operations, have received significant attention. However, Congress also requires an assessment of alternative organizational models that could prove to be more effective. This article seeks to do so, challenging common assumptions about which organizational models are most relevant and instructive. In particular, we explore alternative models for cyber force generation that include the Uniformed Health Services, Defense Combat Support Agencies, Department of Defense specialized career paths, and private-sector workforce development. We assess each alternative in terms of its applicability, limitations, lessons for force generation, and potential to inform the dominant models in the current debate—namely the status quo, a special operations (SOCOM) model, or a separate cyber force.

Keywords: force generation, cyber forces, U.S. Cyber Command, USCYBERCOM, organizational models, talent management

* Corresponding author: nicolas.g.starck.mil@army.mil

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

After fifteen years and billions of dollars invested in training, recruiting, and infrastructure for U.S. Cyber Command (USCYBERCOM), the U.S. military remains unable to generate a sustainable cyber force. Meanwhile, cyber personnel are in high demand across the military, government, and private sector, with each employer attempting to attract and retain a limited talented workforce. Thus, a vigorous debate has emerged over different models for cyber force generation. One thing that appears to be in general agreement – the current approach is insufficient.

Three alternative models now dominate the debate. The first is the status quo. Second, and related, is “CYBERCOM 2.0.” This an organizational revision, informed by the experiences of the U.S. Special Operations Command (USSOCOM) to improve coordination and cyber force generation within the Services. USCYBERCOM, at Secretary of War Pete Hegseth’s direction, has started to implement this revision, which includes establishing several new organizations within the Command headquarters (Matishak 2024). Initially, "CYBERCOM 2.0" was deemed insufficient and sent back to the Command for reconsideration after being described as merely “status quo plus” (Pomerleau 2025) but was eventually signed after minor changes (DoW 2025). The third popular alternative is a separate cyber force (King 2025; Luttrell 2024). This idea predates the creation of USCYBERCOM (Conti and Surdu 2009). Today’s advocates for a separate cyber force argue that the existing Services’ primary missions (i.e., the Army focusing on land operations, the Navy on maritime, etc.) present inherent structural constraints on cyber readiness. Therefore, a new service or department is necessary because, under the status quo, other service missions will always supersede cyber readiness requirements, resulting in a distributed force generation approach incapable of generating adequate numbers of competent personnel (Lonergan and Montgomery 2024).

While the ongoing debate has value, the overwhelming focus has narrowed far too quickly. The three dominant alternatives-the status quo, a “USSOCOM-informed” revision, or a new cyber service-have overshadowed serious consideration of other models of force generation. The Fiscal Year 2025 National Defense Authorization Act (NDAA) directs an independent evaluation of different organizational models (U.S. Congress 2025). Congress also directed that “any other organizational models for the cyber forces of the Armed Forces determined feasible and advisable by the National Academies” be evaluated as well (U.S. Congress 2025).

This work is meant to provide such an outside-the-box evaluation, critical to designing the best way to generate cyber forces to compete with peer adversaries like China and Russia. Our analysis is grounded in the assumption that cyberspace is its own distinct domain (Lonergan and Montgomery 2024). This domain has been repeatedly defined as having its own operational logic (Alexander 2011; DoD 2022; Conti and Raymond 2017). We therefore assume that it requires force generation distinct from other domains. This challenge includes competing for technical expertise that is in high demand elsewhere in the economy.

In our analysis, we have deliberately sought diverse alternative models, both inside and outside the military. The focus is on models that have successfully addressed challenges in the recruitment and retention of specialized technical talent, rapid capability development in emerging domains, and navigating complex legal and authorities frameworks. We conclude that several alternatives offer applicable lessons in technical talent recruitment and retention that can be tailored and adapted to either of the status quo or USSOCOM-informed models. By evaluating alternative models against tailored assessment criteria, this article aims to provide decision-makers with clear insights and options to consider when developing future plans for cyber force generation, along with a framework to evaluate how these insights might be adopted.

MODEL SELECTION AND ANALYTICAL CRITERIA

Our analysis focuses on the following four alternative models. This selection offers a wide range of precedents and lessons learned that can inform the U.S. military's approach to generating cyber forces.

(1) U.S. Public Health Service Commissioned Corps (PHSCC) – The Public Health Service manages specialized uniformed personnel across multiple agencies.
(2) Defense Combat Support Agencies (CSA) - Agencies like the National Security Agency (NSA) blend military and civilian expertise in technical domains.
(3) Specialized Military Career Paths – The Pentagon manages alternative promotion structures for specialized professionals like doctors and lawyers.
(4) Private Sector approaches – The private sector, including the technology industry and major corporations, excels at attracting and retaining top technical talent in competitive markets.

Each model is assessed in terms of qualitative criteria, chosen to address the policy concerns underlying the Congressional revision debate. In particular, a model needs not only to be successful in management of its technical workforce, it also needs to offer lessons appropriate to the cyber field, compatible with the laws and regulations of the military, relevant to development of technical talent, and potentially tailorable for integration into the dominant models already under consideration, since one of these is likely to be the ultimate policy of choice. The criteria, therefore, are the following:

- *Applicability to Military Cyber Operations* – How well does the alternative align with established structures and requirements for generating personnel ready to conduct effective offensive and defensive cyber operations, especially at scale?

- *Legal/Policy Limitations* – Where does the alternative model deviate from the legal and policy limitations the U.S. military must abide by in implementing a force generation approach?
- *Workforce Development Lessons* – What are the key lessons or insights from how the alternative model develops its cyber or technical workforces?
- *Integration with the Dominant Models under Consideration* – How well can lessons from the alternative model be integrated into the three dominant cyber force generation models of the status quo, SOCOM-informed model, or a separate cyber force?

ANALYSIS OF MODELS

The following analysis applies each criterion to each alternative model. While no model stands out across all of the given criteria, several offer invaluable and applicable lessons if their limitations can be overcome. The results are summarized in Table 1.

U.S. Public Health Service Commissioned Corps (PHSCC)

The PHSCC is, along with the National Oceanic and Atmospheric Commissioned Officer Corps, one of the two U.S. uniformed services that are not military services (*U.S. Code 10 § 101*)*.* The PHSCC falls under the Department of Health and Human Services. It is composed exclusively of commissioned officers who are either accepted during their final year of schooling (PHSCC, n.d.) or enter the PHSCC via direct commission (warrant officers are authorized, but none have been commissioned in recent history). PHSCC officers hold ranks identical to those of the Navy and Coast Guard. They are considered active-duty personnel. Commissions into the PHSCC can be made for ranks up to captain (U.S. Army equivalent, officer grade 3) in one of the PHSCC's specialties upon passing an exam. It is also possible to commission directly up to the officer grade 6, but these are limited to 10 percent per year (*U.S. Code 42 § 209*)*.*

While a uniformed service, the PHSCC personnel system deviates in several ways from the armed services. Its officers receive normal military compensation. But they also receive bonuses based on their specialties that are significantly higher than their rank equivalents in the traditional military services. Permanent promotions are tied to professional ability, with examinations required for advancement. Temporary promotions, equivalent to but more flexible than military services' "brevet" ranks, may be made up to colonel without examination or time in service requirements to fill a vacancy. Furthermore, this requirement can be waived to fill a wartime vacancy (*U.S. Code 42 § 211*)*.*

In many ways, the PHSCC offers a compelling organizational model for generating a technical workforce within the federal government that could integrate with the three dominant models for cyber forces. It demonstrates that technically grounded selection, retention, and promotion systems and financial incentives to reduce pay disparities with the civilian market are feasible within the existing legal requirements and authorities of the federal workforce.

Table 1. Summary of Analysis of Organizational Models

Organizational Model	Applicability to Military Cyber Operations	Policy and Regulations Limitations	Lessons for Cyber Force Workforce Generation	Integration with any of the "Dominant Three" Models
Public Health Service Commissioned Corps (PHSCC)	Uniformed personnel Specialized skills and career paths Persistent mission	Not engaged in military operations Reliance on external credentialing Near-total identification of personnel late in their education	Flexibility for specialized skills and career paths Quickly onboarding personnel at various ranks based on experience and expertise	Viable option to consider for, or at least strongly inform, officer career paths within a Cyber Service and potentially warrant officers
Defense Combat Support Agencies	DOD organizations Global and across services Specialized functions	Predominantly serve in a supporting role Limited authority to conduct military operations Military model based on "donor" services, which is equivalent to the problematic status quo	Identification, recruitment, and development of civilian operational workforce	The successful growth and development of civilian personnel could be applied to all three models
Specialized Career Paths	Military officers Expertise focused Specialization in a professional field	External credentialing Focused on individuals who support service missions Relies on individual services to implement, perpetuating the status quo's challenges	Alternatives to prototypical career paths that support expertise	Could be applied in either the status quo or the SOCOM-informed model
Private Sector Approaches	Similar mission sets and organizational requirements Flexible on/off ramp to a company	Lower emphasis on developing employees Different metrics for cost and assessing risk	Highly selective personnel structure Quality over quantity Strong relationships with academia and tech to foster a talent pipeline Meaningful internships	More easily integrated into a full Service, but a JSOC-informed model could benefit if there were a method for personnel to return to their donor service if not ultimately selected for cyber work roles

Note. The authors also considered allied and partner force generation models. For example, Israel's cyber force development is closely linked to mandatory national service, enabling early identification and recruitment of highly skilled individuals into cyber units, which receive priority access to top performers and fast-track advancement. This "whole-of-nation" approach is reinforced by strong coordination between the military and the national technology sector (see e.g., Freilich, Cohen, and Siboni (2023) and Townsend (2018)). The United Kingdom's National Cyber Force, established in 2020 as a joint Ministry of Defence–GCHQ effort, integrates military and intelligence personnel. It has experimented with relaxing traditional military requirements—such as shortened basic training and the removal of weapons handling (Martin 2025)—to accelerate cyber recruitment and onboarding. While both of these models are well regarded and offer valuable insights, neither approach is scalable or fully applicable to U.S. military given differences in population size, legal constraints, institutional structures, and civil–military norms.

Furthermore, the PHSCC model is sufficient for the scale of the Cyber Mission Force (CMF), as both organizations consist of approximately 6,000 personnel. Finally, as a uniformed service that has many parallels to the military services, the PHSCC offers a model that could easily integrate into the existing joint military community.

Despite these advantages, the PHSCC example also has practical limitations. Most significantly, the PHSCC does not conduct military operations as traditionally conceived—its officers are considered noncombatants unless detailed to an armed service. That said, some aspects of public health threats and the PHSCC mission mirror features of the cyber domain (Smith 2016). The PHSCC's practice of almost exclusively recruiting medical personnel later in their educational progression is also distinct from the military's traditional approach to recruiting - both in timing and in the narrow selection from an externally credentialed pool of candidates. These practices may not translate directly to a military cyber service. Still, they do suggest that recruiting candidates with some degree of externally vetted aptitude for the demands of the technical mission can be an effective approach.

Defense Combat Support Agencies

CSAs are chartered by the Pentagon to perform a mission or set of functions on behalf of the entire military. CSAs include a wide range of organizations such as the Defense Commissary Agency, the Defense Health Agency, and the NSA. They generally act in support of combatant commanders conducting military operations (DoD 2010).

The CSA model offers several useful concepts for cyber force generation. First, the missions of CSAs span the globe and support the entire Joint Force. They fall under the office of the Secretary of War rather than any individual military departments (e.g., Department of the Army). Second, while these organizations include uniformed personnel from the armed services, people are assigned to them individually, rather than as units, as is the common practice when the services provide units to combatant commands. Civilians are also a significant component of the agencies' capabilities, to include leadership positions. Finally, the distinction between force providers and force generators enshrined in the Goldwater-Nichols Act does not have the same bearing on CSAs. While agencies may deploy personnel in support of operations, they are not bound by the force generation cycles that characterize service formations.

Like the PHSCC, CSAs offer a practical model for generating and employing a technical workforce that could integrate with popular proposals for cyber forces. As an existing model within the military, CSAs have a long history of successful support to and integration with the joint community in sustained, global operations. Additionally, they enable personnel management and the development of expertise in a tailored field. In particular, the NSA has demonstrated the capacity to develop and maintain a world-leading technical workforce that serves as the vital foundation and continued partner to USCYBERCOM. This success suggests that the ratio of civilian to military employees within the cyber workforce may not need to reflect the military-heavy proportions typical of the existing armed services. Finally, CSAs have provided reliable support to both combatant commands and, in the case of the NSA, the enduring requirement for national intelligence collection.

While these are significant advantages, the CSA model has several key limitations when applied to the challenge of cyber force generation. Most significantly, the CSA model has only been used to generate civilian workforces; it still relies on the armed services to generate and present uniformed personnel. As the status quo has demonstrated, reliance on the existing services has not proven sufficient in this critical regard. In addition, CSAs are explicitly restricted to the realm of supporting operations to the traditional physical domains of war, whereas cyberspace is a co-equal domain as defined in Joint doctrine. Limiting cyber operations to the role of a supporting function would fail to develop the personnel and capabilities necessary to realize the full potential of cyberspace as an independent domain in which U.S. forces can maneuver, create, and employ effects for national security.

Specialized Career Paths

Within the existing armed services, there are a variety of career paths that vary from the prototypical Army infantry officer, Air Force pilot, or Navy surface warfare officer. Military doctors, lawyers, and chaplains all have specialized rules under Title 10 of the U.S. Code. These specialized career fields require credentialing external to the military; they share a high degree of professional identity, and they are common across most of the services.

In addition to these professional career fields, the Army's functional area officers and the Navy's restricted line officers represent service-specific approaches to creating alternative career pathways. The underlying premise of these specialized career management approaches is that some service members' career progression may occur in a more specialized manner that differs from the more generalist model in the services. There are also various programs, such as direct commissioning (U.S. Army Talent Innovation Division 2025; U.S. Congress 2018), career intermission programs (Brading 2021) (U.S. Congress 2019 §551), and education or training with industry (DiCarlo 2024; U.S. Air Force Institute of Technology 2025), all of which can be leveraged to address specific aspects of talent management for these specialized fields.

Specialized career paths offer clear advantages that could enhance force generation for the cyber workforce. They could also integrate with the dominant approaches under consideration. Not all of the armed services have the same specialized career paths (i.e., Marines rely on the Navy for medical personnel). But these specializations still fit within the military's existing authorities, rank structure, and personnel systems. Recruiting, retention, and incentive pay are also commensurate with existing systems. Some of these systems are set by Congress, such as retention (*U.S. Code 37 § 301(d)*) and special pays (*U.S. Code 37 § 302*). Others are set by the services.

Expanding specialized career paths to a size and scope necessary for military cyber could prove difficult, however. All of the specialty paths depend on external credentialing bodies that are well-established and widely recognized. No such equivalent exists for cyberspace defensive and offensive operations. Granted, there are myriad information technology (IT) and cyber professional certifications. Yet most of these external credentials are less intensive than those required to become a doctor or lawyer; and while recommended, none are required to become qualified in many cyber work roles.

Additionally, the specialized career paths would require voluntary support and implementation from all of the services. The services' implementation of programs authorized by Congress varies widely, however, and they are typically more restrictive than what Congress authorized. For example, despite the Career Intermission Program being first authorized in 2014 and made permanent in 2019 (U.S. Congress 2019 §551), the Army only recently began such intermissions, and the associated service obligation it imposes is far greater than required by law (Brading 2021). In contrast, the U.S. Air and Space Forces opened intermission opportunities to most of their career fields in 2022 (U.S. Air Force Public Affairs 2022). Such service-specific divergences would likely result in widely varying approaches to cyber personnel, similar to the status quo.

Private Sector Approaches

The private sector, from technology companies and major corporations to small businesses, does not use military force in cyberspace. Nevertheless, it is under threat from nation-state adversaries and engaged in sustained operations in cyberspace. Private entities with significant resources, especially in the IT sector, have developed the capacity to conduct significant intelligence and defensive operations that stop short of offensive operations. The skills required for much of this work are closely related, if not identical, to those required to conduct military cyber operations.

Technology companies have developed various recruiting strategies to meet their personnel needs, which can rival those of the government. In general, they recruit heavily from top academic institutions that do research relevant to their business. They have student internship programs with academic partners. They also foster professional relationships with academic faculty who can help identify and recruit students for industry jobs upon graduation. These companies typically rely on a combination of internal promotion and external hiring to find people with the skills and experience they need. Their hiring practices, in turn, foster the cross-pollination of industry standards and best practices, creating a collaborative community of relationships that can be leveraged for mutual benefit. Tech companies are also famous for not hiring people just to fill open positions; instead, they often wait for a good match.

Workforce development within private industry offers several significant lessons for military cyber force generation. The emphasis on strong relationships with academia to identify and recruit students creates a robust pipeline for talent. Internship programs supplement scholarship with practical experience that can be leveraged as future employees. Further, the willingness of private companies to be highly selective, leaving positions unfilled rather than hiring someone who would be a bad fit, underscores the often-overlooked but negative impact on overall performance that can result from trying to grow a technical workforce without regard to talent, culture, and other factors.

Of course, the commercial practices also have limitations in the context of military cyber operations. The private sector can rely on financial incentives that are not fully replicable in the military—the U.S. government rarely pays as much as technology companies or major corporations with dedicated cyber staff. The acceptance of cross-pollination through personnel turnover could also prove challenging, given long timelines for clearances and other security requirements associated with military cyber operations. Further, the reliance on a steady influx of new personnel could erode the common cultural and technical foundations that are valuable for military cyber operations.

Finally, industry hiring practices may prove problematic when applied to filling mission-critical positions, regardless of the availability of an ideal candidate. It would require dramatic changes to the US military's recruiting practices and career pathways to recruit a skilled expert into a senior uniformed position rather than junior positions or internal promotion; the flow of industry leaders into and out of military leadership positions would likewise be a significant change. That said, any future cyber force generation model should account for streamlined and exceptional hiring processes to compete for top talent in a competitive market, as well as flexible separation mechanisms to maintain workforce quality.

CONCLUSION: DRAWING OUT LESSONS FOR MILITARY CYBER FORCE GENERATION DECISIONS

Even though no one model is a perfect fit, there are components of each alternative under consideration that could be applied and combined to improve military cyber forces. Each of the organizations examined above has developed their structures and policies for the specialized skills and technical career paths they need. Our analysis reveals several common lessons. For instance, the PHSCC and CSAs (such as the NSA) do not have the same personnel policies or retention incentives. Yet both have implemented personnel systems that meet their unique needs. Both kinds of organizations have also developed effective policies to identify and recruit individuals with the skills needed to succeed in their different missions. They also work to retain the talent they recruit and train. For some models, like the CSAs, this may include rotational programs within the same organization. For others, like private sector companies, long-term retention may involve a career that even includes leaving the organization to gain experience elsewhere, coupled with policies to facilitate easier reintegration. Finally, all of the models we examined demonstrate the value of selectivity based on technical competence – both in initial selection and in continued professional advancement. The nature of that technical competence may evolve over the course of a career. Nevertheless, maintaining a strong technical foundation is instrumental to effective operations through shared organizational cultures.

Below are the lessons from our evaluation, phrased in terms of guidance for the debate over improving cyber force generation. This analytical guidance provides a useful foundation for senior leaders and policymakers to evaluate and integrate the conceptual lessons from other models into an actionable plan for whatever cyber force generation model comes next.

Lesson one: Assure the compatibility and suitability of forces for offensive cyber operations. The military operates in unique and challenging environments, including those that require offensive action. Three of the four models could be readily accommodated within the existing U.S. approach to military organization, operations, and governance–including those involving combat. All four were potentially compatible in scale, although not in offensive combat applications per se. For example, the private sector has the scale but not the cultural acceptance of offensive cyberspace operations.

Lesson two: Generate cyber talent through adapted authorities and policies. Revisions to military authorities and policies are significant endeavors. Simply adapting or extending existing statutes is unlikely to be sufficient. While the initial CYBERCOM 2.0 initiative stayed within the confines of USCYBERCOM's current authorities, which it deemed adequate to support progress (Seffers 2025), it was initially deemed to not go far enough (Pomerleau 2025). The consideration of alternative models offers an opportunity for a more deliberate reconsideration of the nation's titles and authorities. Our analysis indicates that tailored revisions to the military's existing authorities are likely needed to enhance cyber force recruitment, retention, and readiness.

Lesson three: Prioritize sustaining the technical mastery of a highly capable cyber workforce. One of the most significant shortcomings of the status quo is its inability to provide and sustain quality forces at both the scale and the necessary level of expertise in their given field(s). Addressing this failure became a central element of the CYBERCOM 2.0 initiative. Its emphasis on "readiness and future force generation" highlights the need for cyber personnel to develop and sustain technical mastery over their career (Seffers 2025). Our analysis of alternative models indicates that effective force generation depends on organizational prioritization of technical mastery, at scale, in whatever model is chosen moving forward.

Lesson four: Require integration with joint community. Cyberspace is an integral part of all modern military operations. Our analysis identified potential elements of force generation across the alternative models that can, and some that cannot, readily integrate with existing

Joint Forces and joint operations. In addition to addressing the demand for operations in the cyber domain, any cyber force generation solution must also accommodate service and joint requirements.

The lessons offered by alternative models should be considered by policymakers and military leaders as they develop the future cyber force. We strongly recommend that, whatever model the military adopts, it should incorporate the tailoring and adaptation demonstrated by these organizations to more effectively create and retain a highly qualified technical workforce. There is nothing within existing federal authorities that would strictly preclude adopting elements of the successful programs found in these models. Regardless of which path is chosen in reforming or replacing USCYBERCOM, the lessons that can be learned elsewhere are invaluable for designing cyber force generation models that will be competitive in cyberspace.

ABOUT THE AUTHORS

Major Nick Starck is an active duty Army cyber officer. He previously served as a Platoon Leader, Battalion S6, Mission Element Lead, researcher at the Army Cyber Institute, and Senior Instructor in the Department of Electrical Engineering and Computer Science at the United States Military Academy, teaching courses on cyberspace operations and coaching the Cyber Team. He is a 2012 graduate from the U.S. Military Academy, where he commissioned as a Signal Corps officer, with one deployment to Afghanistan. He holds a B.S. in Electrical Engineering from the U.S. Military Academy at West Point, an M.S. in Electrical and Computer Engineering from Carnegie Mellon, and a Master of Science and Technology Intelligence from the National Intelligence University.

Colonel Todd Arnold is an active duty Army cyber officer who currently serves as the Technical Director of the Army Cyber Institute and as an Associate Professor in the Department of Electrical Engineering and Computer Science. He is a 2001 graduate from the U.S. Military Academy with multiple combat tours in Iraq. He has been a key contributor to the Army's efforts in cyberspace and was an initial member of Army Cyber Command, the Army Cyber branch, and the Army's capability developer detachment. He holds a B.S. in Computer Science from the U.S. Military Academy at West Point, a M.S. in Computer Science and Engineering from Penn State, and a Ph.D. in Electrical Engineering from Columbia University.

ACKNOWLEDGMENTS

The authors acknowledge the support of the U.S. Naval War College and thank the participants at the 2025 Cyber and Innovation Policy Institute Summer Workshop for their helpful feedback.

REFERENCES

Alexander, David. 2011. "Pentagon to treat cyberspace as operational domain." Reuters, July 14, 2011. https://www.reuters.com/article/us-usa-defense-cybersecurity/pentagon-to-treat-cyberspace-as-operational-domain-idUSTRE76D5FA20110714/.

Brading, Thomas. 2021. "Army Policy offering up to three-year service break." Army News Service, May 17, 2021. https://www.army.mil/article/246439/army_policy_offering_up_to_three_year_service_break.

Conti, Greg, and David Raymond. 2017. *On Cyber: Towards an Operational Art for Cyber Conflict.* Kopidion Press.

Conti, Greg, and Buck Surdu. 2009. "Army, Navy, Air Force, and Cyber—Is it Time for a Cyberwarfare Branch of Military?" *Information Assurance Newsletter* 12 (1). https://www.gregconti.com/publications/2009_IAN_12-1_conti-surdu.pdf.

DiCarlo, James. 2024. "Unveiling the Significance of the Army's Training with Industry Program," July 18, 2024. https://www.army.mil/article/277269/unveiling_the_significance_of_the_armys_training_with_industry_program.

DoD (Department of Defense). 2010. "Department of Defense Directive 5100.01: Functions of the Department of Defense and Its Major Components." https://dam.defense.gov/Portals/47/Documents/PDSD/510001p2.pdf.

DoD (Department of Defense, Joint Chiefs of Staff). 2022. *JP 3-12: Joint Cyberspace Operations.*

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

Freilich, Charles D., Matthew S. Cohen, and Gabi Siboni. 2023. *National Capacity Building, Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power.* Oxford Academic.

King, Andrew. 2025. "Why America Needs a Dedicated Cyber Force Now | Opinion." Newsweek, April 2, 2025. https://www.newsweek.com/why-america-needs-dedicated-cyber-force-now-opinion-2053910.

Lonergan, Erica, and Mark Montgomery. 2024. *United States Cyber Force: A Defense Imperative.* Foundation for Defense of Democracies. https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf.

Luttrell, Morgan. 2024. "The time is right for a new military force to defend cyber space." Defense News, May 21, 2024. https://www.defensenews.com/opinion/2024/05/21/the-time-is-right-for-a-new-military-service-to-defend-cyber-space/.

Martin, Alexander. 2025. "British military drops basic training to fast track recruitment of 'cyber warriors'," February 10, 2025. https://therecord.media/british-military-drops-basic-training-to-fast-track-cyber-recruits.

Matishak, Martin. 2024. "After prodding from lawmakers, Cyber Command readies a plan for the future," October 22, 2024. https://therecord.media/cyber-command-2-0-project-progress-military-congress.

PHSCC (U.S. Public Health Service Commissioned Corps). n.d. "Officer and Student Training Programs." Accessed July 31, 2025. https://www.usphs.gov/students/.

Pomerleau, Mark. 2025. "DOD leadership asks for CYBERCOM 2.0 relook." DefenseScoop, May 20, 2025. https://defensescoop.com/2025/05/20/cybercom-2-0-relook-dod-leadership/.

Seffers, George I. 2025. "Cyber Command 2.0 Eyes Creation of a Cyber Innovation Warfare Center," April 2, 2025. https://www.afcea.org/signal-media/cyber-edge/cyber-command-20-eyes-creation-cyber-innovation-warfare-center.

Townsend, Kevin. 2018. "From IDF to Inc: The Israeli Cybersecurity Startup Conveyor Belt." SecurityWeek, February 28, 2018. https://www.securityweek.com/idf-inc-israeli-cybersecurity-startup-conveyor-belt/.

U.S. Air Force Institute of Technology. 2025. "Education With Industry Program," July 31, 2025. https://www.afit.edu/CIP/page.cfm?page=1567.

U.S. Air Force Public Affairs. 2022. "Career Intermission Program application window opens April 1, reduces service obligation," March 28, 2022. https://www.spaceforce.mil/News/Article/2980107/career-intermission-program-application-window-opens-april-1-reduces-service-ob/.

U.S. Army Talent Innovation Division. 2025. "Direct Commissioning." Accessed July 31, 2025. https://talent.army.mil/direct-commissioning/.

U.S. Code 10 § 101. https://www.law.cornell.edu/uscode/text/10/101.

U.S. Code 37 § 301(d). https://www.law.cornell.edu/uscode/text/37/301d.

U.S. Code 37 § 302. https://www.law.cornell.edu/uscode/text/37/302.

U.S. Code 42 § 209. https://www.law.cornell.edu/uscode/text/42/209.

U.S. Code 42 § 211. https://www.law.cornell.edu/uscode/text/42/211.

U.S. Congress. 2018. *National Defense Authorization Act for Fiscal Year 2019.* https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.

U.S. Congress. 2025. *Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Section 1544.* https://www.govinfo.gov/content/pkg/PLAW-118publ159/pdf/PLAW-118publ159.pdf.

Received 1 August 2025; Revised 21 November 2025; Accepted 26 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 113-126
https://doi.org/10.55682/cdr/kpcg-emvp

PROFESSIONAL COMMENTARY

Built for Land, Not Cyber

Emily R. Otto*

Alperovitch Institute, School of Advanced International Studies, Johns Hopkins University, Washington, DC, USA
Center for European Policy Analysis, Washington, DC, USA

Despite a decade of reform and Congressional intervention, the military services continue to struggle to meet the operational requirements of cyberspace. Informed by my experience in both traditional Army and cyber units, this article argues that the root of the problem lies not in neglect or leadership resistance alone, but more prominently in structural misalignment. The services are optimized for their physical domains of warfare, not for the characteristics of cyberspace. My analysis utilizes Clayton Christensen's Resources, Processes, and Values (RPV) framework to examine constraints on how the Army generates cyber forces. Although suitable for land warfare, the Army's RPV is ill-suited to a domain characterized by interconnectedness, constant contact, dynamic terrain, and dual character as both weapon and battlespace. I highlight the friction that arises when an organization built for one domain is asked to generate forces for a different domain. Consequently, rather than continuously retrofitting existing services, I argue that the United States should establish a dedicated cyber service designed to maximize the unique capabilities inherent to the digital domain.

Keywords: cyber forces, organizational design, military services, cyberspace, cyber conflict

* Corresponding author: Erotto01@gmail.com

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

"CYBERCOM 2.0" was released on November 6th, 2025, as the Pentagon's revised cyber force generation model. This new model seeks to address shortfalls that have persisted over a decade under the services' mandate to man, train, and equip cyber forces. This revised model, together with years of Congressional involvement, makes the overwhelming case that relying on the traditional military services to produce cyber forces "has not met the unique requirements necessary to fight and win in the cyber domain" (U.S. Department of War 2025).

Why have the services struggled to meet these requirements? Some point to a lack of prioritization within the services (Luttrell 2024) or to cultural challenges (Lonergan 2025). Others go further and attribute longstanding shortfalls to negligence (Magee 2025). In this article, I provide professional insights based on roughly ten years of service, including both enlisted military intelligence roles and as a Cyber Warfare Officer. I have served in a traditional land warfare unit, the 1st Cavalry Division, as well as in the Cyber Protection Brigade (CPB) and the Cyber National Mission Force (CNMF). Given this experience, combined with my academic research, I argue that the military service branches are not entirely to blame for their inability to produce the personnel or capabilities required to address national security threats from cyberspace. Rather, the services are designed to address specific warfighting challenges and capitalize on opportunities within their respective physical domains of warfighting. Their resources, processes, and values are tailored to their originating domains to maximize U.S. military capability in sea, land, air, and outer space. But not cyberspace.

To explore why the services have not met cyberspace's unique requirements, this article employs Clayton Christensen's Resource-Processes-Values (RPV) framework as an analytical lens (Christensen and Overdorf 2000). This framework is typically used to help business leaders understand their own organization's strengths and limitations. It sheds light on the factors that impact what an organization can and cannot do. Typically, when Christensen's framework is applied, it is to help businesses seeking to adapt to a changing market. In response to cyberspace, however, the military services have sought to adjust only limited aspects of their organizations while maintaining their primary focus on their traditional domains—an approach that sustains organizational inertia. The underlying problem is that the services remain optimized for the generation of physical-domain military power, even though cyberspace demands the cultivation of digital exploits rather than kinetic force.

Using the U.S. Army to illustrate, this article argues that the persistent challenges in U.S. cyber force recruitment, manning, training, and equipping stem from requiring a service whose RPV—effective in its original domain—is misaligned with cyberspace. The Army is an appropriate case for examining misalignment because it produces the largest share of cyber personnel and capabilities across the services and exerts the greatest influence on their composition. Therefore, it has an outsized impact on U.S. Cyber Command (USCYBERCOM).

Conclusions drawn from looking at the U.S. Army in cyberspace are also generalizable to other service branches whose operations historically occur in a physical domain.

This article does not argue that the services should overhaul their entire organizations. It would be strategically detrimental if efforts to improve performance in cyberspace undermined the Army's core proficiency in land warfare. The services' central focus should rightly remain on their principal domains. Instead, a new service must be established to maximize cyberspace's capabilities for U.S. national security.

Before examining RPV misalignment, we must first understand the history that led the U.S. military to this point and the distinct characteristics of cyberspace from which my argument flows. Effective organizational design needs to account for these characteristics to maximize benefits from the cyber domain. Then I will introduce the RPV framework to analyze why the services continue to struggle. From there, we will explore how the Army's loyalty to being the best in the land domain causes it to struggle to support USCYBERCOM. For the sake of this article, I do not consider information technology (IT) management and security in day-to-day operations as "cyber forces." These tasks are equally important; they keep the Department of War Information Network (DoWIN, formerly DoDIN) secure, resilient, and functioning. However, they are not considered cyber forces by most of the personnel with whom I served alongside in defensive or offensive cyber operations. Therefore, while the Army has conflated terminology that includes both IT management and electronic warfare (EW) under the umbrella of cyber operations, I distinguish between them (Kamark and Theohary 2023).

Throughout, I ask you to keep in mind the service members affected by these structural flaws—national servants who are forced to choose between professional advancement within their service or dedication to safeguarding U.S. national interests in cyberspace. This professional commentary is dedicated to those who showed selfless service and chose the latter.

BACKGROUND

USCYBERCOM was established in 2010 as a subordinate command under U.S. Strategic Command (USSTRATCOM), a recognition that cyberspace was an important front in national security. By 2017, Congress elevated it to a unified combatant command, further signaling its vital role.

This Command relies on the armed services for force generation. One of the core functions of a military service, per the Goldwater-Nichols Act, is to organize, train, and equip forces for combatant commanders (U.S. Congress 1986). As a result, USCYBERCOM's operational units, the Cyber Mission Force (CMF), are sustained by the military services, which provide the personnel, training, and equipment needed to carry out missions. Congress has been forced to legislate down to the level of military occupational codes, training pipelines, and readiness reporting of the CMF because the services have failed to manage cyber personnel appropriately. The FY2023 National Defense Authorization Act (NDAA) micromanaged career paths, readiness reports, and force generation models—an unprecedented intrusion that indicates structural misalignment. Such legislative micromanagement is highly unusual. Congress historically entrusted the services to manage their own personnel systems. By dictating these details, lawmakers are signaling that the services' resources, processes, and values are structurally misaligned with cyberspace. Simply put, they have treated cyberspace as peripheral rather than a core mission. Consequently, Congress has had to assume a personnel management role it normally does not inhabit (Kamark and Theohary 2023).

Since the FY2023 NDAA, the services have continued to experience problems with cyber force generation. Pentagon leadership rejected initial drafts of "CYBERCOM 2.0," an effort to remediate some of the problems, as insufficient, describing it as little more than "status quo-plus" and requesting a complete review. The NDAA for fiscal year 2025 requires an independent evaluation for a separate cyber force, implicitly acknowledging that the current service-based model is underperforming (U.S. Congress 2024). Congress would not order an external review of whether to establish a new service unless there were credible indications of structural inadequacy within the existing force-generation system. My experience suggests the same.

The Pentagon released a revised version of "CYBERCOM 2.0" in November. This new model attempts to compensate for the services' failure. To understand why the services have struggled, it is imperative to understand why a domain's distinctive dynamics underpin the services' approach to resources, processes, and values. It is to this task we now turn.

CYBERSPACE AS A UNIQUE OPERATIONAL DOMAIN

Many scholars and government organizations describe cyberspace in terms of its composition—the hardware, software, data, and networks (Rattray 2001). For instance, the Pentagon defines cyberspace as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers" (Congressional Research Service 2024).

This article will use a definition that focuses on cyberspace's characteristics as a domain. These characteristics explain how the cyber environment operates as a unique domain of activity beyond its embedded objects. Cyberspace is unique because it is governed by a fundamentally different logic of interaction from physical domains—one that is informational, continuously contested, and detached from direct physical coercion. Describing cyberspace as merely 'distinct' risks implying continuity with the physical force-centric logic that underpins the traditional domains. This article instead treats cyberspace as unique in that its strategic effects emerge through exploitation, persistence, and informational advantage rather than through the application of physical force. The structural characteristics of cyberspace—its interconnectedness, constant contact, reconfigurable terrain, and dual character as both weapon and battlespace—make it inherently different from physical domains.

To illustrate the dual character of cyberspace, computer code is "simultaneously the means to maneuver and the space through which one maneuvers" (Fischerkeller, Goldman, and Harknett 2022). This characteristic creates a different relationship between the operator and the terrain compared to relatively static physical domains, like land, which require large forces to traverse and hold. Security in dynamic digital terrain comes not from holding territory, as it constantly shifts, nor from deterrence, given the domain's opacity, but from dynamic behavior: continually exploiting vulnerabilities while preventing adversaries from exploiting your vulnerabilities.

What does reconfigurable terrain mean? Unlike physical domains, cyberspace can be rapidly and unexpectedly altered (Libicki 2009). A software patch, a hardware upgrade, or the reconfiguration of a network can change the terrain in which cyber forces operate. What was once a vulnerability may disappear with a patch; what was once a secure enclave may become exposed after integration or migration. This volatility has no true likeness in the physical world—moving mountains or reshaping rivers takes centuries. Artillery shells will explode regardless of the target's shape or whether it has a new door or boarded-up windows. But in cyberspace, the topography is mercurial. Cyber forces cannot rely on static defenses or territorial control. They must flow within an ever-changing environment.

The distinctive characteristics of cyberspace also provide unique opportunities. Unlike physical environments, where military outcomes result from forcing one's will through violence on others, strategic outcomes in cyberspace are pursued through exploitation (Fischerkeller, Goldman, and Harknett 2022). States can erode their adversaries' sources of power or bolster their own by circumventing sanctions, degrading military readiness, eroding political trust, and stealing intellectual property at scale. These operations shift power through exploitation without requiring physical confrontation or concessions from adversaries.

RESOURCES, PROCESSES, VALUES FRAMEWORK

How should the armed services adapt? Clayton Christensen's RPV Framework can help organizations determine whether they are postured to succeed when faced with change. First, leaders must determine if they have the proper resources. Then, they need to examine their organization's processes and values to ensure they are aligned with the new environment. This framework introduces leaders to the idea that the capabilities that make their organizations effective in one environment can become liabilities in another.

Organizational capabilities stem from its resources, processes, and values. Resources can be tangible, such as personnel, equipment, and cash, or intangible, including designs, relationships, and knowledge. Processes are the ways in which people transform inputs—whether energy, capital, information, or labor—into desired outputs. Processes can be formal, such as target development and mission planning. They can also be informal, like backchannel coordination, creative workarounds, or mentorship.

Values influence processes and resources. Values are the guiding principles that help personnel make decisions and choose between competing priorities. They guide resource allocation and reward systems. They are also enduring; values are embedded in every decision, process, and interaction (Christensen 2016).

Christensen's research argues that organizations develop strengths through their established processes and values, enabling them to excel in particular tasks. Although initially they may depend on key individuals (resources), over time the organization becomes less defined by people and more by its routine processes and shared values. However, those same strengths can become liabilities when circumstances shift. Organizations struggle to change the way they work or the values that guide their priorities. In this way, the very foundations of an organization's success in one domain can limit its effectiveness in another (Christensen and Overdorf 2000). Applying this logic to the services, what makes them successful in training, manning, and equipping for land or maritime environments, for example, is the very thing that makes them unsuccessful in training, manning, and equipping for cyberspace. The following sections will explore examples of this in further detail.

In fact, the military situation between the services and USCYBERCOM is more difficult than the business situations studied by Christensen. Those firms were adapting to shifts within an existing market, not confronting an environment governed by an entirely different organizing logic. The services are not being asked to adapt to an entirely new operational environment and let go of their old one; they are being asked to maintain and improve their capabilities in their primary domain, while simultaneously carving out portions of their organization to adapt to a fundamentally different domain. The closest analogy to this is the Army being asked to produce sailors and then struggling because they must also prioritize their primary mission, land warfare.

Attempts have been made to ameliorate this situation by giving USCYBERCOM service-like authorities. These service-like authorities include its budget, acquisition process, establishing training standards, and special hiring and retention for its civilian personnel. But the Command is still at the mercy of the services in key areas, including the processes and values that govern training, the promotion system, or the assignment of personnel.

In the sections below, I will examine a select number of cases that exemplify RVP misalignment. They are by no means exhaustive, but rather illustrative of how the Army's originating domain is misaligned for cyberspace in each part of the RVP framework.

Resources

Human expertise is the decisive resource in cyber warfare. Because the domain is a collection of logical constructs, not physical ones, advantage in cyberspace derives from understanding and knowing a network better than the personnel who designed it (USENIX Enigma Conference 2016). Due to the dynamic, reconfigurable terrain, the personnel require near-parallel operations, training, and development. Sending personnel off to distant assignments for training, such as attending a six-month in-resident course whose annually updated curriculum lags behind the domain, removes people—the capability generators—from operations and significantly hinders cyber units that depend on their personnel's capabilities. The best cyber personnel I served with were teaching themselves new technology while assigned to operational units.

Lieutenant General William Hartman, speaking to the Senate Armed Services Committee, echoed this sentiment in 2025. He stated that USCYBERCOM seeks to recruit and retain top cyber talent, leverage the expertise of the Guard and Reserve, and deepen academic and industry partnerships. He concluded with a plan to compete with adversaries, who outnumber U.S. forces, by aiming to "overmatch quantity with quality" (Hartman 2025). Hartman is not referring to the quality of military platforms, like tanks and artillery, but the quality of the personnel and their technical knowledge. People generate the cyber capabilities required in an operating environment that is constantly changing by solving configuration puzzles, building exploits, and discovering vulnerabilities. Cyber capability advancement is more akin to knowledge generation than it is to weapons development.

Land operations are also people-centric, but they require personnel in their capacity to create mass with weapons platforms. Tanks, artillery, and rifles with soldiers produce kinetic firepower. The platforms' capabilities have a long shelf life; while skill is required, their effects are less sensitive to the thought-work of personnel. This is distinct from cyber capabilities, which reside in the individual's knowledge and skill, making them difficult to replicate. By way of analogy, when a trained cyber operator leaves the service, it is as if the Army lost the artillery piece entirely, not just the artilleryman. This difference in understanding resources is one reason why the services struggle to sustain quality cyber personnel: their personnel retention assumptions and standards are built around a desire to produce mass and the assumption that people can be, relative to cyber, easily produced. A commander I once served under lamented this problem, noting how difficult it was to manage a force when the equivalent of your Bradley fighting vehicle wanted to go back to the schoolhouse for an extended period to become an Abrams tank.

Although personnel are the primary resource, tools such as software are also important to augment an individual's training, management, and analysis of data and information. Currently, each branch manages its own piece of the software system—the Army's Persistent Cyber Training Environment (PCTE) and development environments, the Air Force's Unified Platform, the Joint Common Access Platform (JCAP) for offensive operations, Joint Cyber Command and Control for C2, and USCYBERCOM's sensors. The result is a patchwork of systems that lack interoperability (Pomerleau 2024). Even the "Unified Platform" cannot query datasets seamlessly. Redundant development of security operations pipelines also slows delivery. Although this fragmentation is problematic, it is merely a symptom of a deeper problem: the tools themselves were designed with physical domain characteristics as the baseline assumption, as illustrated by the failures of *Project IKE* and *Plan X*.

Plan X, a Defense Advanced Research Project Agency (DARPA) initiative that faltered, was moved to the Pentagon's Strategic Capabilities Office in 2019 and renamed *Project IKE* under a contract with Two Six Labs. This software illustrates two attempts to provide cyber forces mission management software to help plan, conduct, and assess cyber operations. These software solutions failed because they were designed with characteristics and underpinning assumptions derived from land warfare. The interconnectedness, constant contact, and reconfigurable terrain of cyberspace cannot be contained within a common operating picture (COP). A COP is a shared display of operational information collected from multiple sources, consolidated on a map, so that commanders can assess the readiness of forces and direct them accordingly. Throughout my seven years as a cyber officer, regardless of the unit, there was a constant push to create a COP for cyberspace (Pomerleau 2021). I saw non-organic cyber officers—officers who were not technical or whose thinking was already pre-configured with land warfare mindsets—grow increasingly frustrated because they couldn't "see" the operational environment.

While COPs are an effective concept for the physical domains, they break down when applied to cyberspace. One cannot construct a meaningful two-dimensional map of any large network without filtering out a significant amount of data. Cyber terrain is abstract, logical, made of routes, sessions, credentials, and services, and is constantly changing; therefore, there is no way to produce a map that can show where effects will land in ways a commander can intuitively read. The ability to "see" the Internet is dispersed across sensors that are fragmented and owned by disparate actors (service providers, cloud tenants, endpoint vendors, partners). There is no single authoritative sensor suite that can be centrally fused without legal, contractual, or technical barriers. The ephemeral scale and tempo of the domain also undermine mapping efforts. Network flow logs, host telemetry, audit trails, and application logs all require specialized analysis and interpretation. Simply overlaying them into a single map creates noise and false confidence, rather than clarity. Mapping cyberspace is closer to a knowledge map than a geographic map. Resources, in the form of software, such as *Plan X* or

Project IKE, that the services have provided, import the assumptions of the dynamics of their physical domain rather than the dynamics of cyberspace, leaving behind a trail of wasted funds, lost hours, and diminished morale.

Processes

U.S. Army processes—including interaction patterns and coordination, especially regarding training-are not aligned with cyberspace. Army processes reflect the industrial logic required for mass mobilization. It necessitates standardization, hierarchy, and linear progression across geographic terrain. This approach is optimal for predictable, reproducible outcomes—such as having similarly trained soldiers, maintaining equipment, and seizing land directly through established chains of command. This linearity ensures discipline and control in large-scale operations, but it also embeds rigidity: each phase of planning and execution follows a prescribed order, which leaves little room for adaptive iteration and decentralized innovation.

Cyberspace instead requires small unit, real-time technological innovation, and creative knowledge development to support exploitation of highly dynamic terrain. The industrial logic for mass mobilization—effective for land warfare in order to produce waves of tanks and battalions—is unsuitable for cyberspace, where success depends on knowledge creation and the ability to exploit and leverage the terrain.

U.S. Army training processes also reflect the logic for mass mobilization. Institutional courses, professional military education (PME), and developmental tours create predictable, certifiable competencies well suited to a relatively static physical battlefield (U.S. Department of the Army 2025). However, in domains characterized by exploitation, dynamism, and deep technical expertise, hyper-focusing on standardization and linear sequencing becomes a liability. Learning approached as a linear sequence assumes that the knowledge to be acquired can be decomposed into ordered steps that build predictably on one another. It is like an industrial production line: mastery of one step is a prerequisite for moving to the next. This works best when tasks are well understood, outcomes are stable, and variation is undesirable.

By contrast, the most highly skilled cyber service members I served with achieved proficiency through active discovery and experimentation, rather than relying solely on linear instruction. Their exploratory learning is driven by curiosity. Learners follow problems or anomalies into “rabbit holes,” allowing understanding to emerge through experimentation, iteration, and recombination. Exploratory approaches uncover underlying structures, and conducting systematic probing can yield operational success. Training processes for a cyber force require space for exploratory learning rather than linear sequencing.

Compounding the problems of misaligned training processes is the domain-dictated requirement for deep technical knowledge to contribute effectively to operations, planning, or staffing. Being able to make meaningful contributions today requires several years of training and experience, often close to a decade for mastery (Cobb 2025). Many cyber soldiers, specifically field-grade officers, arrive with a lack of basic domain knowledge. They are woefully underprepared. The amount of knowledge required is significantly higher for cyber operations than for land operations. That is not to say conducting land operations is simple. But service members are already accustomed to physical elements—gravity, fiction, spatiality, borders, terrain, visibility—before entering the Army. Most must learn digital fundamentals—authorization, privileges, network architecture, logical barriers, sensors, data flows, configuration—before they can think critically about operating in cyberspace.

These different competencies evolve on different timelines. Technical expertise requires constant maintenance, so expertise atrophies when personnel rotate to positions that do not require technical knowledge but are required for promotion. Promotion systems reward breadth and command time over long-standing technical depth, incentivizing generalists rather than technological specialists, because this approach is effective for officers in the land domain. The result is persistent shortfalls of officers who understand the environment in which they operate, because the domain requirements exceed what the Army's traditional officer model can reliably produce or retain.

Values

If processes determine how something is done, values dictate what is considered worth doing. Values permeate processes and the prioritization of resources, but they are most clearly revealed in decision-making. The Army's values have steered its approach to cyberspace in a manner that reinforces its primary warfighting identities while relegating cyber operations to a supporting role. In an effort to stay aligned with its land warfare mandate, the Army has also expanded its definition of cyber operations to include EW to justify decisions on training curricula, personnel management, and unit creation.

Cyber occupational specialty curriculum now requires cyber officers to "understand all aspects of cyber operations, electronic warfare, and cyber electromagnetic activities along with combined arms tactics, techniques, and procedures to support Multidomain Operations and Large Scale Combat Operations." The Army's cyber officer profile effectively demands simultaneous mastery of two domains (land and cyber), cyberspace engineering, EW, DoWIN defense, joint planning, and land-combat integration—an implausible bundle for one career track.

I am not suggesting that the curriculum was optimal before these changes, when I went through the Cyber Basic Officer Leader Course (BOLC) in 2017 or the Captains Career Course (CCC) in 2020. I spent a sizable portion of my training on planning a battalion-level ground operation. In 2017, the year I commissioned into the U.S. Army Cyber Branch, the Army began moving EW personnel into the cyber career field. Since then, EW has increasingly encroached on the cyber occupational specialty under the auspice of growing the cyber force.

Congress sought to stop this under Section 1543 in the 2025 NDAA, which put a "prohibition on disestablishment or merger of officer career paths within the Cyber Branch of the United States Army." In order to sidestep this prohibition, the Army simply added EW curriculum to a cyber officer's training.

Currently, the Army's 17A Cyber Warfare Officer course includes not only cyberspace operations but also extensive instruction in EW theory, spectrum fundamentals, antennas, electro-optics, and signals intelligence in support of EW. All of which were not a part of cyber officer training when I went through the schoolhouse. In effect, now, a "cyber" officer is trained as much in spectrum operations as in network exploitation, even though a separate 17B Electromagnetic Warfare Officer specialty exists. The curriculum creep of EW into cyber reflects the Army's drive to fold cyberspace into its traditional emphasis on land warfare by prioritizing spectrum control and maneuver support, rather than cultivating the specialized, persistent capabilities that USCYBERCOM requires for global operations (U.S. Army Cyber Center of Excellence 2025).

Claims of growing the cyber force are also hollow. As highlighted on The Cyber Center of Excellence (CCoE) website, "growth is concentrated in the 17E MOS, Electronic Warfare Specialist, reflecting the branch's focus on offensive and defensive cyber capabilities." Yet, this statement is misleading. EW is not offensive or defensive cyber. The Army has simply conflated its language in order to promote capabilities that are more aligned with land warfare. EW specialists monitor signatures and disrupt adversary networks through jamming—tasks rooted in the spectrum, not in hacking, hunting, or persisting on networks (Starrett 2025). By framing EW as cyber operations, the Army blurs the line between cyberspace and electromagnetic operations, subordinating true cyber operations in order to stay aligned with land warfare priorities.

The Army's effort to add cyber capabilities to its land warfare divisions further illustrates the conflation of cyber with EW. Although labeled "cyber units," these new units are not conducting network operations. Their capabilities are radio-frequency-enabled, meaning effects delivered through spectrum operations, not network exploitation. Personnel are then assigned to these units while billets go unfilled at USCYBERCOM (Pomerleau 2025). This framing subordinates cyber to land warfare priorities, rather than pursuing the cultivation of the specialized, offensive, and defensive on-network operations capabilities needed by USCYBERCOM.

YOU CAN'T GET THERE FROM HERE

The persistent misalignment between the Army's—and, by extension, the services'—resources, processes, and values on the one hand, and the characteristics of cyberspace on the other, explains why more than a decade of reform has failed to generate a cyber force capable of meeting national security requirements. The Army's institutional design reflects the characteristics of land warfare—hierarchical, industrial, and platform-centered—while cyberspace demands a force that is networked, exploratory, and knowledge-centered. The failure, therefore, is not negligence but incompatibility. Congressional intervention and the Pentagon's repeated revisions to the cyber force generation model underscore that the problems are systemic.

A separate cyber service, purpose-built for the domain, is the most logical and most feasible alternative available today. It would not supplant the traditional services but complement them, allowing each to specialize according to the characteristics of its respective domain. Only by aligning organizational design with domain characteristics can the U.S. military effectively harness cyberspace's potential and leverage the expertise of its service members, who remain its most critical resource.

To clarify the implications for all services, not just the Army, the logic developed in this article leads to a functional—not wholesale—division of cyber responsibilities. The services would retain steady-state network operations and baseline cybersecurity functions for networks that are inseparable from their domain-specific missions. For the Army, this includes signal units, Network and Enterprise Technology Command (NETCOM), and Regional Cyber Centers (RCCs) operating as cybersecurity service providers (CSPs). These organizations are responsible for communications, networking, information transport, and the continuous execution of defensive cyber operations–internal defense measures (DCO-IDM): monitoring networks, implementing defense-in-depth, enforcing compliance standards, patching and hardening systems, and conducting initial incident detection and response. These activities ensure availability, reliability, and resilience of service networks from the tactical edge to the strategic level, and they remain appropriately embedded within the services because they are tightly coupled to operational command and control (C2), logistics, and day-to-day force employment for land, sea, air, and space operations.

A separate cyber service, by contrast, would assume responsibility for cyber defense functions that are active, adversary-focused, and operational. This includes Defensive Cyber Operations–Response Actions (DCO-RA), which go beyond securing infrastructure to maneuvering within friendly networks to hunt, contain, and eradicate sophisticated adversaries—often requiring higher authorities due to their potentially disruptive effects. The cyber service would also provide surge incident response, intelligence-driven network hunting, and red-team assessments in support of service-owned networks. Critically, this is not a clean handoff but a deliberate seam: DCO-RA would be executed side-by-side with service cyber security service providers and network owners, preserving unity of effort while aligning the most specialized, adaptive cyber talent with a force designed for persistent threat engagement. This division generalizes across the services and reinforces the broader argument of the paper: cyber effectiveness depends less on reallocating everything to a new institution than on placing the right functions—preventive versus maneuver-oriented—within organizations structurally optimized to perform them.

Finally, the same logic extends even more clearly to offensive cyber operations (OCO), which should reside entirely within a dedicated cyber service. They would provide a unique strategic capability as well as provide support to the geographic combatant commands. OCO is inherently intelligence-driven, and persistent. It requires centralized authorities, specialized tradecraft, and continuous engagement with adversaries across geographic and organizational boundaries. Unlike network operations or baseline defense, offensive cyber capabilities are not tied to a service's organic platforms or day-to-day C2 responsibilities. Housing OCO within a cyber service would consolidate scarce expertise, standardize training and doctrine, and ensure unity of command over operations that carry strategic risk and political sensitivity. The services would remain consumers of cyber effects in support of their campaigns, but the planning, preparation, and sustainment of OCO forces would be conducted by a cyber service purpose-built for the domain.

ABOUT THE AUTHOR

Emily Otto is a Non-resident Fellow at the Center for European Policy Analysis and an Alperovitch PhD Fellow at the Johns Hopkins School of Advanced International Studies. Her research focuses on cyber conflict and cyber forces. Prior to her academic pursuits, Emily served a decade in the U.S. Army, primarily as a Cyber Warfare Officer, with earlier experience in Military Intelligence. She led a mission element and served as the Brigade Executive Officer while assigned to the Cyber Protection Brigade. She conducted full-spectrum cyber planning across offensive, defensive, and information operations and supported tri-national operational discussions while serving with the Cyber National Mission Force.

ACKNOWLEDGMENTS

I am grateful to the senior officers and leaders who tolerated sustained questioning and dissent, and whose challenges sharpened my thinking and conclusions. I would also like to thank Dr. Emily Goldman, Dr. Michael Fischerkeller, Jason Kikta, John Giordano, Dr. Michael Sulmeyer, and MAJ Travis Siemion for formative conversations on cyber force development, as well as Dr. Thomas Rid, Dr. Melissa Griffith, and Dr. Ben Buchanan at Johns Hopkins University for their continued mentorship.

REFERENCES

Christensen, Clayton M. 2016. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail.* Boston: Harvard Business Review Press.

Christensen, Clayton M., and Michael Overdorf. 2000. "Meeting the Challenge of Disruptive Change." *Harvard Business Review* March-April 2000. https://hbr.org/2000/03/meeting-the-challenge-of-disruptive-change.

Cobb, John. 2025. *An Insider's Guide to Cyber Readiness.* War on the Rocks, May 1, 2025. https://warontherocks.com/2025/05/an-insiders-guide-to-cyber-readiness/.

Congressional Research Service. 2024. *Defense Primer: Cyberspace Operations.* Congressional Research Service. https://www.congress.gov/crs_external_products/IF/HTML/IF10537.html.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford University Press.

Hartman, William J. 2025. *Posture Statement, U.S. Cyber Command,* April 9, 2025. https://www.cybercom.mil/Media/News/Article/4150133/posture-statement-of-lieutenant-general-william-j-hartman/.

Kamark, Kristy N., and Catherine A. Theohary. 2023. *FY2023 NDAA: Cyber Personnel Policies. No. R47270.* Congressional Research Service. https://www.congress.gov/crs-product/R47270.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar.* RAND Corporation. https://www.jstor.org/stable/10.7249/mg877af.

Lonergan, Erica D. 2025. "Cultural Change in Military Organizations: Hackers and Warriors in the US Army." *Texas National Security Review* 8 (3): 74–95. https://tnsr.org/2025/07/cultural-change-in-military-organizations-hackers-and-warriors-in-the-us-army/.

Luttrell, Morgan. 2024. *The Time Is Right for a New Military Force to Defend Cyber Space.* Defense News, May 21, 2024. https://luttrell.house.gov/media/in-the-news/opinion-time-right-new-military-service-defend-cyber-space.

Magee, Aden. 2025. *The Sad and Sorry Tale of Cyber Command's Seven-Year Failure.* War on the Rocks, September 4, 2025. https://warontherocks.com/2025/09/the-sad-and-sorry-tale-of-cyber-commands-seven-year-failure/.

Pomerleau, Mark. 2021. *A Cyber Tool That Started at DARPA Moves to Cyber Command.* C4ISRNet, April 20, 2021. https://www.c4isrnet.com/cyber/2021/04/20/a-cyber-tool-that-started-at-darpa-moves-to-cyber-command/.

Pomerleau, Mark. 2024. *US Cyber Command Aiming to Consolidate Disparate Programs in Warfighting Platform in 2024.* DefenseScoop, January 19, 2024. https://defensescoop.com/2024/01/19/cyber-command-consolidate-programs-warfighting-platform-2024/.

Pomerleau, Mark. 2025. *Army Looking to Inject More Cyber Capabilities into Formations at the Division Level.* DefenseScoop, August 22, 2025. https://defensescoop.com/2025/08/22/army-inject-more-cyber-capabilities-into-formations-divisions/.

Rattray, Gregory J. 2001. *Strategic Warfare in Cyberspace.* Cambridge, MA: MIT Press.

Starrett, Michael K. 2025. *Cyber Center of Excellence and Army Transformation.* Army.mil, July 3, 2025. https://www.army.mil/article/286843/cyber_center_of_excellence_and_army_transformation.

U.S. Army Cyber Center of Excellence. 2025. *Electromagnetic Warfare Officer,* September 28, 2025. https://cybercoe.army.mil/Cyber-Center-of-Excellence/Schools/Cyber-School/Cyber-Courses/Electromagnetic-Warfare-Officer/.

U.S. Congress. 1986. *Goldwater-Nichols Department of Defense Reorganization Act of 1986.* H.R. 3622, 99th Congress, 2nd Session. https://www.congress.gov/bill/99th-congress/house-bill/3622.

U.S. Congress. 2024. *Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025.* H.R. 5009, 118th Congress. https://www.congress.gov/bill/118th-congress/house-bill/5009/text.

U.S. Department of the Army. 2025. *DA Pam 600–3: Officer Professional Development and Career Management—Cyber Branch.* https://api.army.mil/e2/c/downloads/2025/02/19/9304a0aa/da-pam-600-3-cyber-branch-fy25.pdf.

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

USENIX Enigma Conference. 2016. *USENIX Enigma 2016 – NSA TAO Chief on Disrupting Nation State Hackers.* https://www.youtube.com/watch?v=bDJb8WOJYdA.

Received 1 October 2025; Revised 13 November 2025; Accepted 8 December 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 127-145
https://doi.org/10.55682/cdr/cybr-cu1t

RESEARCH ARTICLE

Why Culture Matters: Organizational Culture and Force Generation for the Cyber Domain

Erica D. Lonergan[2], Alexander Master[1]

[1]Army Cyber Institute, West Point, NY, USA
[2]Columbia University, New York, NY, USA

Public discourse about the potential for a new organization, a United States Cyber Force, reflects a growing consensus that significant organizational change is required to meet the U.S. military's current and future challenges in cyberspace. However, much of the discussion takes a mechanistic perspective, centering around restructuring cyber teams, creating new organizations, changing authorities, creating new policies, and so on. This perspective is important but it is insufficient. ***Culture matters.*** *Organizations ignore culture at their peril. This paper focuses on how service culture has shaped the U.S. Army's experiences with cyberspace as a case study to illustrate why culture must be considered in any organizational approach to how the U.S. generates cyber forces and conducts cyberspace operations. If the U.S. does not get organizational culture "right", no amount of organizational change will be effective in addressing its force generation challenges.*

Keywords: organizational culture, force generation, U.S. Cyber Force, U.S. Army, U.S. Cyber Command, USCYBERCOM

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

America faces a well-documented force generation challenge for operating in cyberspace (Onken et al. 2024; Szewczyk 2024; Bates and Rose 2022; U.S. GAO 2022; Wenger, O'Connell, and Lytell 2017). Force generation entails the organization, training, and equipping of military forces (U.S. Congress 1986). Much of the conversation about how to improve cyber force generation in the United States has taken a mechanistic perspective, centering around restructuring cyber teams, creating new organizations, changing authorities, creating new policies, and so on. Some argue for implementing incremental changes to the current force-generation model by increasing U.S. Cyber Command's (USCYBERCOM) service-like responsibilities (Long and Pytlar 2024; Haugh 2024). Others call for pursuing more systemic changes to establish a new branch of the Armed Forces focused on cyberspace, a U.S. Cyber Force (Lonergan and Montgomery 2024, 2025).

However, as these debates are unfolding, the discourse largely overlooks the role of organizational culture. Cultural considerations will frame and permeate all of these organizational choices—and, ultimately, contribute to their success or failure over the long term. If the U.S. does not account for organizational culture, no amount of organizational change will be effective in addressing current force generation challenges.

The purpose of this article is not to explore the merits of arguments on either side of the debate about whether a Cyber Force should be established. Instead, we focus on the critical role of culture in shaping the force, regardless of which course of action is pursued. That said, we do argue that the most effective way to create an organizational culture that is aligned with the requirements for generating cyber capabilities would be to establish a Cyber Force. An independent service would be relatively untethered from existing service cultures and would have the remit and autonomy to cultivate a distinct cyber culture. Yet, establishing a Cyber Force *in and of itself* is not sufficient to instantiate a culture that allows the U.S. military to compete and win in cyberspace; it will still need to be a deliberate effort.

Indeed, when the U.S. Space Force was established in 2019, leaders explicitly debated how the service would establish a distinct service culture (Sanders 2022). For example, in 2020 then-Chief of Staff of the U.S. Air Force, Gen. David Goldfein, reflected on the imperative to build a distinct service culture for the Space Force within the Department of the Air Force, noting that: "The objective for Chief [of Space Operations] Raymond and me is how do we build a foundation of trust and confidence and focused on integrated joint warfare. At the same time, how do we allow the Space Force to develop its own service culture" (Pope 2020).

A Cyber Force would pose unique cultural challenges. Unlike the Space Force, which was largely created out of the Air Force, a Cyber Force would likely incorporate personnel from across the existing services who comprise the joint Cyber Mission Force (CMF). Therefore, the dilemma would not only be discerning how to develop the "right" service culture, but also how to integrate personnel from disparate services who are already shaped by those existing service cultures and norms. Reflecting on his experiences as the commander of the Cyber National Mission Force (CNMF), Vice Admiral (retired) Timothy J. White noted the predicament of fostering a shared cyber culture, even in a joint operational environment: "Despite operating in an inherently shared technological ecosystem with common threats and challenges, the CNMF—the joint cyber force as composed of the individual services, each with its distinct organizational proclivities and perspectives—is still evolving toward a truly shared cyber strategic culture" (T. J. White 2020, 130).

The issue of organizational culture and its role in force generation has largely been underappreciated in the current debate (S. P. White (2023) being an exception). Instead, policymakers and experts have tended to focus on other issues, such as how to organize a potential Cyber Force; whether it should be organized under the Department of the Army or be a standalone military department (Couillard 2024); whether a U.S. Special Operations Command-like or U.S. Joint Special Operations Command-informed model is more appropriate for the cyber domain than a separate service (Long and Pytlar 2024); and what authorities might be needed to improve the effectiveness of USG cyberspace activities (Edwards 2025).

Culture is a contested concept and there is no one standard definition. Broadly speaking, it is often defined as "the set of basic assumptions, values, norms, beliefs, and formal knowledge that shape collective understanding."[1] The culture of an organization contains repertoires or "tool kits of symbols, stories, rituals, and worldviews" that help structure and organize members' behavior (Swidler 1986, 273). Culture is especially important for military organizations in structuring the identity and values of their members, as well as their behavior, including the development of doctrine or their propensity to innovate (Kier 1997; Goldman 2006). The academic literature on military culture describes how each service is defined by a distinct culture, which developed over time as a result of its history, the domain in which it operates, and the missions it is called to perform. That said, it is important to note that military cultures are not monolithic, and service cultures contain multiple (and often competing) subcultures. For example, in his seminal work on U.S. military service culture, Carl Builder finds that the U.S. Navy "worships at the altar" of tradition, is characterized by an elaborate hierarchy, focuses on size (defined by number of ships), and values independence and autonomy. In contrast, Builder depicts the Air Force as a service that "worships at the altar" of technology, focuses on qualitative technological edge, has a simple dichotomous hierarchy (pilots versus non-pilots), is less institutionalized, and instead embodies an idea of technologically-based warfare. Finally, according to Builder, the U.S. Army "worships at the

[1] See (Kier 1997, 28). To scope our analysis, we exclude behavior from our definition of culture to examine how ideas, beliefs, and constitutive identities may have an effect on behavior. This follows Jack Snyder's treatment of culture, which he defines as "a system of symbols that creates meaning within a social group," (J. Snyder 2002, 14). This is distinct from Snyder's definition of strategic culture as "the sum total of ideas, conditioned emotional responses, and patterns of habitual behavior that members of a national strategic community have acquired through instruction or imitation and share with each other with regard to" the use of force (J. L. Snyder 1977, 8).

altar" of country, embodies the concept of selfless service, measures its strength in terms of mass, valorizes the combat arms, and is less fascinated by technology (Builder 1989). While Builder's scholarship focuses on these three services, the U.S. Marine Corps and Space Force are also defined by distinct cultures, though the latter service is relatively new and its culture is still developing (Terriff 2006; Li and Melin 2023).

We argue that each of the military services' dominant cultures articulates values, ideas, and beliefs that are in tension with the requirements for developing effective cyber doctrine, organizing military forces for cyber warfare, and recruiting and retaining skilled cyber warriors.[2] Like the other operational domains, cyberspace is also defined by its own unique features, logic, and dynamics, distinct from those of the other domains of warfare (air, land, sea, and space). Effectively operating in and through cyberspace requires organizations and individuals to embrace different values, paradigms, and behaviors than those embodied by traditional service cultures.

The forces that currently operate in and through cyberspace are steeped in the cultural legacies of their existing services. Each of the services is currently responsible for recruiting, training, educating, and promoting those individuals. However, this force generation model creates a disconnect or misalignment between each service's culture, on the one hand, and the imperatives stemming from the cyberspace domain, on the other. Complicating the matter further, cyber forces coming from across the services bring together a multitude of differences in doctrine and terminology; standards for awards, promotions, and evaluations; and even military customs and traditions.[3]

ARMY CULTURE AND CYBER CULTURE

We focus on comparing and contrasting Army culture and cyber culture. Future research could extend this analysis to explore the relationship between cyber culture(s) and other service cultures, as well as broader U.S. military culture.

Each of the military services is defined by a distinct "personality" that has remained relatively constant despite changes in leadership, warfare, and other external factors. Builder argues that service personality is an important factor that shapes the development of strategy, separate from a service's institutional or bureaucratic interests. Together, these factors have constituted a service culture that can be identified and measured in terms of tangible policies, as well as more intangible ideas, beliefs, and values.

[2] On differences across U.S. military service cultures, see Zimmerman et al. (2019). At the same time, the fact that all of the existing services working together and, therefore, their combined service cultures, have proven insufficient for adequately organizing, training, and equipping cyber forces to date suggests that there are underlying commonalities across the services that reflect a broader shared U.S. military culture. This is consistent with the literature on American strategic culture and the American way of war, including its approach to technology (see Mahnken (2008)).

[3] On joint cyber culture, see T. J. White (2020).

Like any organization, the Army's culture is not monolithic (S. P. White 2019). Instead, it is composed of various entities (such as branches and functional areas, units, and components) that together encompass over 1.2 million individuals. Each of these entities can be characterized by distinct subcultures (such as the subculture of the infantry branch, or the subculture of the 101st Airborne Division) that nevertheless share common cultural attributes of the broader service culture.

Cyber cultures and subcultures are also shaped by the nature of the environment. Cyberspace is a constructed domain. Operations involve an ever-changing mix of technologies that require in-depth technical knowledge to exploit and defend. The domain is also interconnected and pervasive, touching on a growing range of human endeavors and becoming increasingly intertwined with the lives of people across the globe (Fernandes and Master 2025). These factors combine into an uncertain environment that involves interacting interests between many and diverse actors. Some nation-states even seek to undermine the fundamental nature of the open Internet by creating "splinternets" that can operate independently of global TCP/IP networks, or by applying censorship to deny access to "objectionable" content (Master and Garman 2023). Additionally, while military operations in cyberspace occur continuously below the threshold of armed conflict, they are seldom "won." Actors constantly seek means to counter the tools and techniques of their adversaries, rendering previously secure systems vulnerable and negating previously valuable accesses. Thus, enduring advantage comes not from the exploits or detection tools, but rather through the means by which they are built, adapted, and leveraged. It comes from the forces, organizations, and processes they use (Slayton 2017). It follows that an organizational culture complementary to these demands will be more effective.

It is beyond the scope of this article to comprehensively catalog all the elements and facets of both Army and cyber culture. Moreover, while the Army's service culture has developed over centuries and it is associated with a specific institution, there is no single "cyber culture" in the U.S. that is constituted within a given organization or entity. Instead, there is a proliferation of various cyber subcultures. These began to develop in the mid-20th century from various cultural movements and were embodied in different organizations and communities, ranging from the model train club at the Massachusetts Institute of Technology, to the counter cultural movements of the 1960s, to innovation hubs in Silicon Valley, to the communities formed through participation in hacker conferences like DEF CON, and others (Jordan 2016). Another cultural legacy comes from information security, private sector security companies, government efforts such as US-CERT, and the cybersecurity industry. Some of these attributes overlap with aspects of hacker subculture, which is the focus of our analysis, while others are distinct (Knerler, Parker, and Zimmerman 2022).

However, a brief comparison of several of the core values, ideas, and beliefs that constitute Army and cyber culture, broadly construed, illustrates important points of divergence, as well as areas of compatibility. We examine core cultural attributes along several different dimensions, including the motivating ethos, the unit of analysis, relationship to change, views about hierarchy and authority, relationship to technology, and beliefs about expertise. In depicting Army and cyber culture, we focus on analytical description rather than making normative judgments about whether these cultural attributes are "good" or "bad." Additionally, we largely focus on the attributes of the "hacker" subculture because of its association with offensive cyber activities and frequent comparison to military cyber forces. That said, there are also important cultural dimensions related to software development and cybersecurity subcultures. For instance, analysis of security operations centers of the financial sector and Fortune 500 companies may provide poignant lessons regarding organizational culture and defensive cyber operations (DCO).

At their cores, Army culture and cyber culture are each defined by a distinct motivating ethos. The Army styles itself as the portrayal of "selfless" service, with the "warrior ethos" inextricably tied into the idea of defending the Nation and Constitution (and doing so through deploying "forward," given deep skepticism of standing armies at home). The Army sees war as an inherently human (and enduring) endeavor (Zimmerman et al. 2019). Army culture also distinguishes between "war" and "peace" as binary states (Nagl 2005). The core ethos of cyber culture is passion and curiosity about technology and creatively overcoming limits (Conti and Easterly 2010). Another motivating philosophy among hackers is the use of technological tools to improve society, which is tied to cyber culture's skepticism of power, bureaucracy, and hierarchy.

Following from the idea that war is an inherently human endeavor, the Army is a people-centric organization that sees the small unit or group (e.g., fire team, squad, platoon) as the key unit of analysis. In the aggregate, the Army measures itself according to mass (e.g., number of personnel). People are also central to cyber culture, but in a different way. Cyber culture is both individualistic and communitarian. Cyber culture elevates the myth of the "10x coder," an individual whose technical capabilities and output far outpace those of their peers, underscoring the belief that individual skill can have extraordinary and disproportionate effects. At the same time, the often-invoked image of the lone "hacker in a hoodie" belies the communal aspects of cyber culture that are cultivated both virtually through participation in online communities and in-person through small meetings in Silicon Valley, hacker conferences, and other fora (Turner 2005; Conti 2005). And just as war is seen as timeless, Army culture is generally resistant to change; it is not a "learning institution" (Nagl 2005). Conversely, cyber culture embraces change and sees technology as a driver of broader societal change (Dery 1996).

Army and cyber culture also offer different beliefs about hierarchy and authority. While all military organizations are hierarchical, the Army values taking the initiative and prizes the concept of mission command and delegating authority to lower echelons, within acceptable boundaries. Within the Army's cultural hierarchy, the combat arms branches—maneuver, fires, and effects—are at the apex. In contrast, cyber culture is deeply skeptical of authority and hierarchy. It sees bureaucracies as "flawed systems…[that] hide behind arbitrary rules (as opposed to the logical algorithms by which machines and computer programs operate): they invoke those rules to consolidate power, and perceive the constructive impulse of hackers as a threat" (Levy 1984; Beltramini 2020). The core purpose of hacking is to find creative ways of circumventing how systems are designed—essentially, breaking the rules (Zuckerberg 2012).

When it comes to technology, Army and cyber culture exhibit important distinctions. While Army culture is not nearly as technology-centric as the Air Force, it also does not reject technology outright and indeed has relied on firepower (enabled by advances in technology) to achieve battlefield objectives (Nagl 2005). Yet cyber culture is fundamentally optimistic about technology, seeing it as a force for good in the world and providing the necessary tools for those seeking to exit from the dominant society in pursuit of a counter-cultural community (Turner 2006). Cyber culture is implicitly techno-utopian, believing that "computers can change your life for the better" (Levy 1984).

Finally, Army and cyber culture take different approaches to expertise. The Army espouses a generalist model of leadership, placing significant emphasis on experience in command roles. Individuals are seen as replaceable and interchangeable. Additionally, expertise is demonstrated through proficiency in physical feats and signaled to others through badges and other accolades (e.g., the Ranger tab). Cyber culture is highly meritocratic, with technical skill as the "coin of the realm," rather than "bogus criteria such as degrees, age, race, or position" (Levy 1984). Individuals compete in "quests"[4] to demonstrate their technical acumen.

IMPLICATIONS OF ARMY CULTURE

The differences (and some similarities) between Army and cyber culture are observable in practice in terms of how the Army has approached the cyber domain. Drawing on the discussion above, we illustrate the implications of Army culture when applied in a cyber context. We elaborate on four examples of the consequences, both positive and negative, of the interplay between Army and cyber culture.

Personnel are replaceable. The realities of ground combat have fostered a culture within the Army in which personnel are replaceable. Historically, combat, especially large-scale ground combat, has involved significant casualties (Clodfelter 2017). Subordinates fill the position of a leader who is killed or wounded, while unit adjutants and the Army personnel system move in replacement personnel and reconstitute units. These realities impact how the Army approaches the personnel aspects of force generation. Namely, the Army requires

[4] In a modern context, these might include capture-the-flag (CTF) events, bug bounty programs, and other hacking competitions.

large pools of individuals who are broadly interchangeable within certain categories, rather than a careful selection of the ideal person for each position.

The military occupational classification system (MOCS) provides an institutional mechanism to meet this imperative (U.S. Department of the Army 2022, 2025b). The pool of replacements is those individuals whose Military Occupational Specialty (MOS) or other identifiers match those coded for the billets. While specialization certainly has value within this system, it is constrained by a requirement of replaceability. Institutional concepts of key development (KD) positions, standardized position titles and descriptions, and routine permanent change of stations all reinforce this cultural norm. The idea that personnel are replaceable also permeates other aspects of the Army's culture, such as the service's generalist model of leadership for the officer corps, which prizes leadership within one's specialty as the most important form of expertise (especially in the combat arms branches), rather than deep technical expertise in a particular specialty. In other words, leadership itself *is* the specialty.

In contrast, operations in cyberspace are conducted across the competition continuum, often remotely and below the threshold of armed conflict, without direct casualties on either side. Therefore, casualties, and the corresponding requirement for replaceability, have a much lower mission relevance. This diminishes the value proposition for institutional practices that promote replaceability. Moreover, rather than prizing general leadership skills, the demands of the cyber domain require personnel who have cultivated deep technical expertise and domain acumen, often for narrow applications or specialties.[5] As a result, personnel are not easily substitutable or interchangeable. Another implication is that there is far less of a requirement for sheer mass to ensure sufficient numbers of personnel to achieve battlefield objectives; quality, in other words, is more important than quantity.

Soldiers must be physically fit. Ground combat often means fighting in austere conditions. This can mean traveling for long distances while carrying heavy loads, sprinting across the battlefield, traversing challenging terrain, physically carrying wounded soldiers, and, most fundamentally, directly engaging with and overcoming the enemy. Therefore, a core value of the Army is that soldiers must be physically fit. They must meet certain health and fitness requirements to join the Army and can be administratively separated from the Army if they fail to pass semi-annual tests assessing body fat, fitness, and medical qualifications. Enlisted personnel, regardless of MOS, receive promotion points for physical fitness.

These may be valid requirements for ground combat. However, when applied to cyberspace, they unnecessarily limit the pool of potential personnel for initial recruitment, introduce overhead costs (notably, time) for personnel to maintain such standards, can cause the loss of otherwise qualified personnel through inability to comply with standards because of injury,

[5] Examples include particular computing operating systems, mobile devices, enterprise networking equipment, Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, among others.

disability, or other reasons, and evaluate personnel on standards that may have little bearing on the performance of their daily duties.

With the exception of expeditionary cyber units (e.g., 11th Cyber Battalion) none of these physical imperatives is a requirement for effective warfighting in cyberspace. In fact, cultural norms around physical fitness and appearance could serve as an implicit barrier to recruiting personnel with the technical abilities needed to excel in cyberspace operations. This is not to validate the stereotype that all "hackers" are obese asthmatic nerds living in their mothers' basements (Kopan 2016). Rather, it reflects the reality that the target pool for recruits for cyber work roles is simply different from that for infantry, armor, artillery, and so on. Additionally, beyond the recruitment issues, maintaining physical fitness standards creates an opportunity cost in taking away time from training and education for cyber-relevant skills.

The Army deploys. To kill an enemy, they must be in range of your weapon system. Although the effective ranges of weapons have increased from the time of spears and arrows, ground combat still requires (relatively) close proximity. When coupled with America's geographical fortune of being surrounded by oceans to the east and west and friendly nations to the north and south, the Army has a force employment model based on deploying forces to the theater of operations.[6] War is fought "somewhere else" and therefore forces must be "deployable," ready to leave the homeland to engage in warfare.[7] Units must be capable of operating forward with reduced support. The Army Force Generation (ARFORGEN), Sustainable Readiness Model (SRM), and Regionally Aligned Readiness and Modernization Model (ReARMM) frameworks have been used over time to assess the "readiness" of units to be able to deploy and frame the Army's organizational thinking.

Readiness expectations permeate Army formations, down to the individual level. Soldiers must maintain certain medical statuses, execute family care plans for dependents, and update next-of-kin and will information to maintain "readiness" for deployments. In addition to requirements for deployability, the Army rewards deployment with overseas service ribbons, overseas service bars, and combat patches to be worn on uniforms. The deployment model also frames operations within the Army. Training programs are based on a cyclic build from individual through collective training, with new personnel and equipment coming in early in the cycle. This often coincides with the summer move cycle. The end of the cycle often culminates in a deployment to a combat training center (CTC) or geographic combatant commander's area of responsibility, and the campaign and contingency plans of these commanders include aspects to manage deployment and redeployment.

[6] This section about deployment cycles is specific to the U.S. Army, and may not apply to other nation-state armies in other contexts.

[7] The Soldier's creed of the Army includes: "...I stand ready to **deploy**, engage, and destroy the enemies of the United States of America in close combat" (emphasis added).

These expectations are misaligned for operations that do not involve forward deployment, such as most cyberspace operations. With some exceptions, the military can project power in and through cyberspace from the sanctuary of the homeland, given the interconnected nature of the global Internet. From an offensive perspective, notable exceptions are those targets that may require physical access or are in denied environments (Pomerleau 2023b). Another exception is "hunt forward" operations, in which teams are dispatched forward to conduct threat hunting on allied and partner networks—though these largely function as alliance reassurance mechanisms, rather than the application of force (Graham 2023). Wherever they are physically located, the operational tempo of cyber forces is different from the Army norm because they remain on a near-continuous elevated cycle, given the pace of online threat actor activity (below the threshold of armed conflict).

Small unit leadership. More than most of the other services, the Army is oriented around the individual and the small unit. Built on the doctrinal and technological changes that began before World War I, initiative,[8] independent action, and small unit tactics have become critical elements in ground combat (Biddle 2004). Relatedly, historical and socio-political factors have contributed to a more egalitarian approach to leadership, especially compared to earlier times and naval traditions. The Army emphasizes the concept of servant leadership, with its leaders encouraging the reading of books with titles such as "Leaders Eat Last" and "The Men, the Mission, and Me" (Sinek 2014; Blaber 2010).

Unlike the other cultural dimensions described above, in this case Army and cyber cultures are complementary. While cyberspace does not involve living together under austere conditions or maneuvering semi-independently to minimize the effects of massed rifle fire, a human-centric and egalitarian approach to leadership is also an important value in cyber culture and beneficial to cyberspace operations. Cyberspace is a complex amalgamation of diverse systems. No leader can have sufficient mastery of all the systems. Instead, they must be receptive to input from individuals who are experts on the different component systems—and such expertise may reside at lower levels in the chain of command. Additionally, mass has little meaning in cyberspace, so operational cyber teams are often relatively small. Finally, operations are often more about creatively identifying vulnerabilities to exploit or piecing clues together. Thus, operations are about arranging people around the problem rather than rallying around a weapon system.

Additional cultural challenges. The tensions discussed above are not unique to cyber forces. Underneath a common cultural umbrella, the Army is still a heterogeneous organization composed of various subcultures, each of which may be in tension with one another and the dominant culture. However, the particular tensions between the Army's culture and cyber

[8] This is a notable change from previous periods, caused by the increased lethality of rifle fire. It required a shift from centrally controlled close-order formations to dispersed formations. The increased lethality of artillery and the advent of radio communications expanded this trend.

culture has distinct implications for the organization's effectiveness in generating cyber forces. Furthermore, beyond those described above, there are aspects of the roles and relationships of cyber forces within the Army that give rise to additional tensions. There are also likely tensions between cyber culture and America's military culture more broadly that any new military cyber culture will need to address.

First, the forces that conduct cyberspace operations are relatively consolidated within the Army from an organizational perspective. A large portion of the Army's cyber forces are housed within two brigades and one service component command. This means cyber subcultures that are cultivated within the Army among its cyber personnel are largely isolated from the broader service culture. Cyber personnel serving in roles within "land domain" focused formations are primarily integrators and cultural interlocutors between cyber and Army forces.

Additionally, there is a distinct cross-cutting cultural community of military cyber personnel across all of the existing services. This is because, in many cases, the Army's cyber personnel (and those within the other services) work more closely with their counterparts in the other services than they do with members of other functional communities within their own services, given the joint nature of many cyber assignments (i.e., within various cyber mission teams or joint task forces under USCYBERCOM).

Furthermore, cyberspace activities are not limited to the military. Like some other subgroups, the cultural identification as a cyber professional extends beyond the military to cyber cultures and subcultures in broader society, such as hacker communities. Perhaps more significantly, cyberspace is a unique warfighting domain where operations can be conducted relatively independent of the land domain, free of its corresponding imperatives. Altogether, these factors compound the inherent tensions between Army and cyber cultures, further siloing (and potentially marginalizing) cyber forces within the Army.

HOW TO FOSTER CYBER CULTURE WITHIN THE MILITARY

This analysis is anchored in two fundamental premises. The first is that culture is an important, but often overlooked, factor in accounting for the military's ongoing force generation challenges in cyberspace. Specifically, there are inherent tensions between core facets of military culture, on the one hand, and the values, beliefs, ideas, and identities that constitute cyber culture, on the other. These cultural tensions make it difficult for military organizations to recruit and, especially, promote and retain personnel with the attributes and skills that are essential for the cyber domain. While we focus on the Army as an illustrative case, the same analysis could (and should) be replicated across the other military services. Doing so would likely yield similar results. The second premise is that neither Army nor cyber culture are monolithic, and there are some perhaps surprising convergences between elements of both cultures. In other words, the picture is more complex and nuanced than might otherwise be expected.

The tensions between Army and cyber culture raise practical questions about how military organizations can more effectively foster a cyber culture to improve force generation. For the Army to improve its effectiveness in cyberspace, it must deliberately align organizational culture based on the specific demands of cyberspace operations. Similar changes would need to be made across the military as a whole to address these broader mismatches. This includes both reducing or otherwise minimizing those misalignments that cause tension while fostering values and beliefs—along with the corresponding aspects of organizational behaviors—that are tailored to mission requirements.

This alignment must translate into tangible policy changes to promotion processes, evaluations, standards, and so on. Academic research has demonstrated the importance of promotion pathways for military innovation (Rosen 1991). For instance, while soldiers receive promotion points in the Army by scoring well on the fitness test and scoring high on weapons qualification—implicitly stating these are measures of competence—these acts do not inherently make an individual a better cyber soldier.[9] The Army could establish comparable (and equally valued) accolades, awards, and tabs to reward and signal mastery in the cyberspace domain (Conti et al. 2014). This would involve promulgating and normalizing cyber examples of achievement for use in awards, evaluations, soldier of the month boards, and so on.

Additionally, the Army should consider excepting cyber personnel from unnecessary requirements that limit the pool of talent or take away time from activities more directly aligned to their mission (Kollars and Moore 2019). These may include fitness or health standards. They may also include marksmanship training or land navigation. Instead, the Army must deliberately consider the traits and behaviors, of both organizations and individuals, that enable successful mission accomplishment in cyberspace and build an organizational culture around that through policies, how evaluations are written, and the countless other mechanisms through which the Army builds and communicates its cultural values.

These recommendations give rise to a number of challenges in implementation. For one, it is not clear that the Army as an organization will be receptive to making these changes, as many are fundamentally incompatible with their core responsibility to organize, train, and equip for warfighting in the land domain. Moreover, because all of the existing services—each defined by distinct service cultures—play a role in generating capabilities for cyberspace operations, it would be incumbent on all of the services to implement similar changes. For example, *all* of the services would need to align rewards and recognitions of personnel to cyber proficiency. This may include promotion tests, such as those that exist in the Air Force and Navy, and warfare badges similar to those the Navy already has for information warfare.

[9] However, because these are established symbols of competence in the Army, earning them can sometimes be an indicator of hard work, goal setting, or other intangibles that might be beneficial.

The Navy could prioritize cyber assignments as career stepping stones, rather than as a broadening assignment that surface warfare officers attend for short stints of time, despite the Navy having created two officer designators for the cyberspace domain in response to Congressional concern and intervention (Pomerleau 2023a).

All of the services should consider removing, waiving, or otherwise modifying physical fitness and medical requirements for cyber personnel. They could also reevaluate career progression models to remove requirements for generalizations and permit (but not necessarily require) specialization. On top of this, the Joint Force will need to address the tensions that will nevertheless persist between the various service cultures as they come together to conduct cyberspace operations in a joint environment.

A core challenge is that most of the required changes would run counter to the existing services' cultures and broader U.S. military culture. Cultures in general are resistant to change. Service cultures exist for a reason, and inducing cultural change to accommodate the needs of generating forces for the cyber domain risks undermining the services' primary missions. This suggests doubt about the likelihood of these changes being implemented—and in a way that is minimally consistent across the existing services.

Therefore, the importance of culture strongly underscores the argument for establishing a new branch of the Armed Forces for cyberspace—a Cyber Force (Lonergan, Arnold, and Starck 2024). The prevailing tensions between existing service cultures and those cultural attributes that are essential for the cyber domain will make it significantly more difficult to inculcate a shared, coherent culture conducive to cyberspace activities in the absence of an independent service. If the current military services continue to serve as the primary force generators for the cyber domain—even if USCYBERCOM is able to exert greater influence on this process—the reality is that each of the dominant service cultures will inevitably exert significant (and divergent) influences on how the military organizes, trains, and equips cyber forces.

At the same time, as was the case with the establishment of the Space Force, the decision to establish a Cyber Force, in itself, will *not be sufficient* to instantiate an optimal service culture. This must be a dedicated, deliberate effort. Cyber personnel would be joining the Cyber Force from five different services, each defined by a distinct service culture. Similar to the Space Force, the Cyber Force will likely be a relatively small organization within a large military bureaucracy. This creates the risk that any effort to instantiate a distinct culture, especially one that may be in tension with aspects of broader military culture, will be quickly quelled or simply overwhelmed by the dominant military culture.

Furthermore, policymakers will need to address how best to constitute the various subcultures that will exist within the Cyber Force to ensure consistency in broad values and norms across the service writ large, while creating space for specific subcultures to flourish. For example, there will likely be a subculture within the Cyber Force that adopts more traditional military values, especially around physical fitness, to account for those aspects of cyber operations that require close, physical access or that are deeply integrated with kinetic warfighting units (Paul, Porche, and Axelband 2014; Pomerleau 2023b). Alternatively, if some of these capabilities are retained by the existing services (e.g., tactical cyber capabilities within the Army), there will be a need for cultural touchpoints both between the Cyber Force and the other services, as well as a means of harmonizing cyber subcultures within service-retained cyber capabilities and that service's dominant culture.

Below, we offer several core tenets that the decision-makers responsible for building a Cyber Force (if one is created) should take into account to foster a distinct service culture matched to the nature of cyberspace.

- **Value expertise.** Cyberspace operations involve a technical field that requires in-depth knowledge to defend and exploit vulnerabilities. However, software can be changed in an instant. Therefore, people are often more important than technology. Additionally, while technical expertise is essential, it is not the only form of expertise. Cyberspace is a human-created environment, demanding socio-technological forms of expertise. The Cyber Force should avoid a singular focus on the technical expertise needed for operational tasks, but instead incorporate a broader set of expertise, including psychological, political, organizational, regional, and economic disciplines.

- **Foster a collaborative culture.** The computing field is too broad for a single individual to have expertise in all possible areas. The depth required to achieve mastery in a particular skill set is conducive to specialization. Therefore, various forms of expertise must be coordinated to accomplish technical operational tasks, those tasks must be integrated with the broader operational context to have impact, and all of this must include collaboration with the private sector, across the federal government, and with other organizations to translate strategic goals into operational objectives.

- **Promote adaptability, flexibility, and continuous learning.** The cyber domain is constructed. It is dynamic. Capabilities can change at the speed of a commit. Individuals and organizations must be able to grow new skills, approaches, and capabilities to adjust to an ever-changing environment. Large organizations often have a tendency to resist change, because it creates disruption and inefficiencies. Effective cyberspace operations require an organizational culture that not only accepts flexibility of change but encourages it. The Cyber Force must inculcate a culture that enables the organization and its personnel to keep pace with a rapidly changing environment.

- **Encourage condition setting and long-term thinking.** While advantage in cyberspace is fleeting, operations endure. Network design significantly impacts defensibility, and operational preparation of the environment (OPE) of an adversary network for cyber effects operations may take months or years to cultivate—but chance is also a factor. A Cyber Force will be best served by viewing the "long game," looking holistically at the aggregate, long-term, and strategic picture. Cyber forces can be operating constantly—seeking the adversary, gaining access, or improving understanding and defensibility of friendly networks. However, 100% operational utilization reduces the force's ability to surge in crisis, develop professionally, stymie burnout, and improve tools. At every echelon in cyberspace, mission assignment and resource allocation is a balance of short-term and long-term benefit.

The above values are meant to be a starting point for discussion about how to build an organizational culture tailored to the demands of cyberspace operations. They are essential whether or not a Cyber Force is established. Looking ahead, there are other critical decisions that leaders will need to make that will also be instrumental in shaping the culture of the Cyber Force, if enacted. For example, the service's force composition—both in terms of the constitution and relative proportion of active, reserve, and guard components, as well as the proportion of civilian to uniformed, military personnel—will be an important avenue for developing its culture. A more civilian-heavy Cyber Force or a non-traditional/flexible guard and reserve model may be key enablers of a distinct cyber culture. Another key consideration is identifying the initial leaders and cadre, as these individuals will be instrumental in the inculcation of such values and shaping of the initial organizational culture. Even if a distinct cyber service is not established, the previous examples and proposed values can serve as a guide for leadership at all echelons to recognize and mitigate the inevitable tensions between broader organizational culture, the demands of cyberspace, and their specific mission.

ABOUT THE AUTHORS

Dr. Erica D. Lonergan is an Assistant Professor in the School of International and Public Affairs at Columbia University. She is also an adjunct fellow in the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. Previously, Erica served on the faculty at the United States Military Academy at West Point, including in the Departments of Social Science and Electrical Engineering and Computer Science, and at the Army Cyber Institute. Erica also has an extensive policy background. Previously, she was a writer of the 2023 U.S. Department of Defense Cyber Strategy, and served as a Senior Director on the U.S. Cyberspace Solarium Commission. She also held an appointment as a Council on Foreign Relations International Affairs Fellow, with placement at JPMorgan Chase and U.S. Cyber Command at the Cyber National Mission Force. Erica has published widely on cybersecurity, strategy, and international security. Her co-authored book, Escalation Dynamics in Cyberspace, was published in 2023 with Oxford University Press. Erica earned her PhD in Political Science from Columbia University.

Major Alexander Master is an active-duty Army Cyber Officer at the Army Cyber Institute and an Assistant Professor in the Electrical Engineering and Computer Science department at the United States Military Academy at West Point, New York. He earned a Master of Engineering in Cybersecurity degree from the University of Maryland, and a PhD in Information Security from Purdue University. His research focuses on digital privacy, cybersecurity, computer networking, and Internet censorship. Alex was initially commissioned as a field artillery officer and deployed in support of Operation Resolute Support in 2015 as part of the conflict in Afghanistan. He has previously served on a National Cyber Protection Team, and subsequently spent several years supporting offensive cyberspace operations in the Cyber National Mission Force at USCYBERCOM.

ACKNOWLEDGMENTS

The authors acknowledge the support of the U.S. Naval War College and thank the participants at the 2025 Cyber and Innovation Policy Institute Summer Workshop for their helpful feedback. The authors are also immensely grateful to the anonymous peer reviewers for their inputs, which improved the quality of this manuscript.

REFERENCES

Bates, Chad, and Charlene Rose. 2022. “Understanding—and Fixing—the Army’s Challenge in Keeping Cyber Talent,” May 17, 2022. https://mwi.westpoint.edu/understanding-and-fixing-the-armys-challenge-in-keeping-cyber-talent/.

Beltramini, Enrico. 2020. “Against Technocratic Authoritarianism. A Short Intellectual History of the Cypherpunk Movement.” *Internet Histories* 5 (2): 101–118. https://doi.org/10.1080/24701475.2020.1731249.

Biddle, Stephen D. 2004. *Military Power: Explaining Victory and Defeat in Modern Battle.* Princeton, NJ: Princeton University Press.

Blaber, Pete. 2010. *The Mission, the Men, and Me: Lessons from a Former Delta Force Commander.* New York, NY: Dutton Caliber. ISBN: 978-0-425-23657-4.

Bratus, Sergey. 2007. “What Hackers Learn That the Rest of Us Don’t: Notes on Hacker Curriculum.” *IEEE Security & Privacy Magazine* 5, no. 4 (July): 72–75. https://doi.org/10.1109/MSP.2007.101.

Builder, Carl H. 1989. *The Masks of War: American Military Styles in Strategy and Analysis: A RAND Corporation Research Study.* Baltimore, MD: Johns Hopkins University Press. https://doi.org/10.56021/9780801837753.

Clodfelter, Micheal. 2017. *Warfare and Armed Conflicts: A Statistical Encyclopedia of Casualty and Other Figures, 1492–2015.* 4th ed. Jefferson, NC: McFarland & Company.

Conti, Gregory. 2005. “Why Computer Scientists Should Attend Hacker Conferences.” *Communications of the ACM* 48, no. 3 (March): 23–24. https://doi.org/10.1145/1047671.1047694.

Conti, Gregory, and Jen Easterly. 2010. “Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture.” *Small Wars Journal* (July). https://www.gregconti.com/publications/482-conti-easterly.pdf.

Conti, Gregory, Michael Weigand, Ed Skoudis, David Raymond, Thomas Cook, and Todd Arnold. 2014. “Towards a Cyber Leader Course Modeled on Army Ranger School.” *Small Wars Journal* (April). http://www.rumint.org/gregconti/publications/cyberleadercourse.pdf.

Couillard, Jeffrey. 2024. “Beyond USCYBERCOM: The Need to Establish a Dedicated U.S. Cyber Military Force.” *The Cyber Defense Review* 9 (1): 55–72.

Dery, Mark. 1996. *Escape Velocity: Cyberculture at the End of the Century.* New York: Grove Press.

Dykstra, Josiah, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2022. “The Economics of Sharing Unclassified Cyber Threat Intelligence by Government Agencies and Departments.” *Journal of Information Security* 13 (03): 85–100. https://doi.org/10.4236/jis.2022.133006.

Edwards, Jeffrey. 2025. *The Things That Bedevil U.S. Cyber Power,* October 16, 2025. https://warontherocks.com/2025/10/the-things-that-bedevil-u-s-cyber-power/.

Fernandes, John, and Alexander Master. 2025. “OACOK, OKOCA, or OCOKA? Reframing Terrain Analysis for Cyberspace.” *Gray Space: Cyber & Electromagnetic Warfare Journal* 1 (1). https://doi.org/10.13140/RG.2.2.36150.77124.

Fernandes, John, Nicolas Starck, Richard Shmel, Charles Suslowicz, Jan Kallberg, and Todd Arnold. 2022. “Assessing the Army’s Cyber Force Structure.” *The US Army War College Quarterly: Parameters* 52, no. 3 (August). https://doi.org/10.55540/0031-1723.3170.

Fox, Jaclyn, Alexander Master, Nicolas Starck, and Jessica Dawson. 2023. *Death by a Thousand Cuts: Commercial Data Risks to the Army.* Technical Report. United States Military Academy: Army Cyber Institute. https://doi.org/20.500.14216/1694.

Goldman, Emily. 2006. "Cultural Foundations of Military Diffusion." *Review of International Studies* 32 (1): 69–91. https://doi.org/10.1017/S0260210506006930.

Graham, Edward. 2023. *USCYBERCOM's Operations Have Strengthened Allies, Agency Lead Says,* March 8, 2023. https://www.nextgov.com/cybersecurity/2023/03/uscybercoms-operations-have-strengthened-allies-agency-lead-says/383717/.

Harrell, Nicholas, Alexander Master, Nicolas Starck, and Daniel Eerhart. 2025. "Tactics and Techniques of Information Operations: Gaps in US Response to Counter Malign Influence." *International Conference on Cyber Warfare and Security,* https://doi.org/10.34190/iccws.20.1.3271.

Haugh, Timothy. 2024. *Posture Statement of General Timothy D. Haugh 2024 - CYBERCOM 2.0,* April 12, 2024. https://www.cybercom.mil/Media/News/Article/3739700/posture-statement-of-general-timothy-d-haugh-2024/.

Jordan, Tim. 2016. "A Genealogy of Hacking." *Convergence: The International Journal of Research into New Media Technologies* 23 (5): 528–544. https://doi.org/10.1177/1354856516640710.

Khan, Shiraz. 2025. "A Conditions-Based Look at a Cyber Force." *Joint Force Quarterly* 118 (3): 83–91. https://digitalcommons.ndu.edu/joint-force-quarterly/vol118/iss3/12/.

Kier, Elizabeth. 1997. *Imagining War: French and British Military Doctrine Between the Wars.* Princeton, NJ: Princeton University Press.

Knerler, Kathryn, Ingrid Parker, and Carson Zimmerman. 2022. *11 Strategies for a World-Class Cybersecurity Operations Center.* MITRE. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf.

Kollars, Nina, and Emma Moore. 2019. "Every Marine a Blue-Haired Quasi-Rifleperson?," August 21, 2019. https://warontherocks.com/2019/08/every-marine-a-blue-haired-quasi-rifleperson/.

Kopan, Tal. 2016. *Could a 400-pound Couch-potato Have Hacked the DNC?,* September 27, 2016. https://www.cnn.com/2016/09/27/politics/dnc-cyberattack-400-pound-hackers/index.html.

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution.* Garden City, NY: Anchor Press.

Li, Jennifer J., and Julia L. Melin. 2023. *Developing U.S. Space Force Organizational Culture with Future-Facing Intention.* RAND Corporation, December 12, 2023. https://www.rand.org/pubs/perspectives/PEA575-1.html.

Lin, Herbert, and Amy B. Zegart, eds. 2019. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.* Washington, D.C.: Brookings Institute. https://doi.org/10.5771/9780815735489.

Lonergan, Erica, Todd Arnold, and Nick Starck. 2024. *The Case for a Prospective U.S. Cyber Force,* May 22, 2024. https://warontherocks.com/2024/05/the-case-for-a-prospective-u-s-cyber-force/.

Lonergan, Erica, and Mark Montgomery. 2024. *United States Cyber Force: A Defense Imperative.* Foundation for Defense of Democracies, Washington, D.C. https://www.fdd.org/analysis/2024/03/25/united-states-cyber-force/.

Lonergan, Erica, and Mark Montgomery. 2025. *Building the Future U.S. Cyber Force: What Right Looks Like.* Foundation for Defense of Democracies, Washington, D.C. https://www.fdd.org/analysis/2025/09/09/building-the-future-us-cyber-force/.

Long, Alan Brian, and Alex Pytlar. 2024. *An Argument Against Establishing a U.S. Cyber Force,* July. https://defensescoop.com/2024/07/11/argument-against-establishing-united-states-cyber-force/.

Mahnken, Thomas G. 2008. *Technology and the American Way of War Since 1945.* New York, NY: Columbia University Press.

Maschmeyer, Lennart. 2021. "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security* 46, no. 2 (October): 51–90. https://direct.mit.edu/isec/article/46/2/51/107693/The-Subversive-Trilemma-Why-Cyber-Operations-Fall.

Master, Alexander, and Christina Garman. 2023. "A Worldwide View of Nation-state Internet Censorship." In *Free and Open Communications on the Internet,* 22. Lausanne, Switzerland: Proceedings on Privacy Enhancing Technologies. https://www.petsymposium.org/foci/2023/foci-2023-0008.pdf.

Nagl, John A. 2005. *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam.* Chicago, IL: University of Chicago Press. ISBN: 978-0-226-56770-9.

Onken, Skyler, Nick Starck, Erica D. Lonergan, JC Fernandes, Todd Arnold, and Maggie Smith. 2024. *Beyond Binaries: Cyber Force Generation and the SOCOM-Like Model,* November 7, 2024. https://irregularwarfare.org/articles/beyond-binaries-cyber-force-generation-and-the-socom-like-model/.

Paul, Christopher, Isaac Porche, and Elliot Axelband. 2014. *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces.* RAND Corporation. https://www.rand.org/pubs/research_reports/RR780.html.

Pomerleau, Mark. 2023a. *After Prodding from Congress, Navy Creates Dedicated Cyber Work Roles Amid Readiness Concerns,* June 28, 2023. https://defensescoop.com/2023/06/28/after-prodding-from-congress-navy-creates-dedicated-cyber-work-roles-to-boost-readiness/.

Pomerleau, Mark. 2023b. *New DOD Doctrine Officially Outlines and Defines 'Expeditionary Cyberspace Operations',* May 12, 2023. https://defensescoop.com/2023/05/12/new-dod-doctrine-officially-outlines-and-defines-expeditionary-cyberspace-operations/.

Pomerleau, Mark. 2025. *New Cyber Mission Force Teams: 12 of 14 Now Established,* May 12, 2025. https://defensescoop.com/2025/05/12/new-cyber-mission-force-teams-12-of-14-now-established/.

Pope, Charles. 2020. *Goldfein Offers Optimistic Update on Air Force's Evolution and Future,* January 27, 2020. https://www.af.mil/News/Article-Display/Article/2066974/goldfein-offers-optimistic-update-on-air-forces-evolution-and-future/.

Rosen, Stephen Peter. 1991. *Winning the Next War: Innovation and the Modern Military.* Ithaca, NY: Cornell University Press.

Sanders, William D. 2022. "Space Force Culture: A Dialogue of Competing Traditions." *Air & Space Operations Review* 1 (2). https://www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-1_Number-2/Sanders.pdf.

Sinek, Simon. 2014. *Leaders Eat Last: Why Some Teams Pull Together and Others Don't.* New York, NY: Penguin Random House.

Slayton, Rebecca. 2017. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41 (3): 72–109. https://doi.org/10.1162/ISEC_a_00267.

Snyder, Jack. 2002. "Anarchy and Culture: Insights from the Anthropology of War." *International Organization* 56 (1). https://doi.org/10.1162/002081802753485124.

Snyder, Jack L. 1977. *The Soviet Strategic Culture: Implications for Limited Nuclear Operations.* Technical report R-2154-AF. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/reports/R2154.html.

Swidler, Ann. 1986. "Culture in Action: Symbols and Strategies." *American Sociological Review* 51 (2): 273–286. https://doi.org/10.2307/2095521.

Szewczyk, Zachary. 2024. *A Cyber Force Is Not the Only Solution,* July 25, 2024. https://warontherocks.com/2024/07/a-cyber-force-is-not-the-only-solution/.

Terriff, Terry. 2006. "'Innovate or Die': Organizational Culture and the Origins of Maneuver Warfare in the United States Marine Corps." *Journal of Strategic Studies* 29 (3): 475–503. https://doi.org/10.1080/01402390600765892.

Turner, Fred. 2005. "Where the Counterculture Met the New Economy: The WELL and the Origins of Virtual Community." *Technology and Culture* 46 (3): 485–512. https://doi.org/10.1353/tech.2005.0154.

Turner, Fred. 2006. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism.* Chicago, IL: University of Chicago Press. https://doi.org/10.7208/chicago/9780226817439.001.0001.

U.S. Congress. 1986. *Goldwater–Nichols Department of Defense Reorganization Act of 1986.* https://history.defense.gov/Portals/70/Documents/dod_reforms/goldwater-nicholsdodreordact1986.pdf.

U.S. Department of the Army. 2022. *Military Occupational Classification and Structure (DA Pam 611-21).* https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36922-PAM_611-21-000-WEB-2.pdf.

U.S. Department of the Army. 2025a. *FM 3-12 Cyberspace and Electronic Warfare Operations.* https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN45009-FM_3-12-000-WEB-1.pdf.

U.S. Department of the Army. 2025b. *The Army Personnel Development System (Army Regulation 600-3).* https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN42984-AR_600-3-000-WEB-1.pdf.

U.S. GAO. 2022. *Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking.* Technical report GAO-23-105423. Washington, DC: U.S. Government Accountability Office, December. https://www.gao.gov/products/gao-23-105423.

Wenger, Jennie W., Caolionn O'Connell, and Maria C. Lytell. 2017. *Retaining the Army's Cyber Expertise.* Research Report RR-1978-A. RAND Corporation. https://www.rand.org/pubs/research_reports/RR1978.html.

White, Sarah P. 2019. “Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine.” PhD diss., Harvard University. https://dash.harvard.edu/handle/1/42013038.

White, Sarah P. 2023. “The Organizational Determinants of Military Doctrine: A History of Army Information Operations.” *Texas National Security Review* 6 (1): 51–78. https://doi.org/10.26153/tsw/44440.

White, Timothy J. 2020. “Joint Operations in Cyberspace: From Operational Unity to Shared Strategic Culture.” In *Ten Years in: Implementing Strategic Approaches to Cyberspace,* edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, vol. Newport Papers No. 45, 129–140. Newport, RI: U.S. Naval War College Press. https://www.govinfo.gov/content/pkg/GOVPUB-D208_200-PURL-gpo183843/pdf/GOVPUB-D208_200-PURL-gpo183843.pdf.

Zimmerman, S. Rebecca, Kimberly Jackson, Natasha Lander, Colin Roberts, Dan Madden, and Rebeca Orrie. 2019. *Movement and Maneuver: Culture and the Competition for Influence Among the U.S. Military Services.* Report RR-2270-OSD. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2270.html.

Zuckerberg, Mark. 2012. “Letter to Investors: ‘The Hacker Way’.” *Wired* (February 1, 2012). https://www.wired.com/2012/02/zuck-letter/.

Received 01 August 2025; Revised 14 November 2025; Accepted 21 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 147-162
https://doi.org/10.55682/cdr/v5tk-6d9f

PROFESSIONAL COMMENTARY

Reclaiming the Cyber Domain: Revising U.S. Doctrine to Treat Cyberspace as Battlespace and Not a Function

Skyler Onken*[1], Margaret Webber†[2]

[1]Twenty Technologies Inc., Arlington, VA, USA
[2]University of New Hampshire, Durham, NH, USA

Cyberspace has been formally recognized as a domain of warfare for over two decades, yet U.S. military doctrine and practice continue to treat it primarily as a cross-domain enabler rather than a battlespace of independent operational and strategic consequence. This paper argues that the prevailing doctrinal framing—cyber as a support function within joint operations—has hindered the development of operational art, force generation models, and integrated campaign design for cyberspace. The paper critiques the conceptual conflation of cyberspace with the information environment and with electromagnetic warfare; it also bridges doctrine with recent scholarship on whether cyberspace constitutes an operational domain. It proposes the adoption of new doctrinal concepts, such as cyberspace control operations, as a foundation for differentiating cyberspace as battlespace rather than a supporting function. The paper highlights the risk of sustaining the supporting-role mindset in an era when adversaries, such as the PRC, employ cyberspace operations as primary tools for competition and deterrence. By clarifying the doctrinal vocabulary and contrasting U.S. practice with the approaches of its adversaries, this paper offers a framework for treating cyberspace as a true domain of warfighting in its own right.

Keywords: cyber, doctrine, joint domain, warfighting functions

* Corresponding author: skyler@twenty.io
† Both authors contributed equally to this research.

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

William Gibson's 1984 novel, Neuromancer, created a sensation among Sci-Fi enthusiasts by immersing readers into a strange new world described as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation" (Popova 2014). Gibson (1984) called his world "cyberspace". His readers reveled in it. Yet even Gibson admits that, while writing his novel, he delighted in the fact that cyberspace "was suggestive of something but had no real semantic meaning." For Gibson, cyberspace indicated a realm that was both substantive and superficial. He described it as a word that sounded like it meant something - or could mean something - "while still being essentially hollow" (Jones and Calleja 2011).

Today, we continue to apply multiple meanings to cyberspace, grapple with its definition and import, and tack the prefix *cyber-* onto more and more words. However, for military operations, specificity and definitions are of great importance. That is because doctrine, or the compilation of actions, definitions, and their application in warfare, guides commanders in their use of power on the battlefield—in any domain. Unfortunately, the concept of "cyber" remains doctrinally ambiguous and operationally diluted. Too often, the term cyber operations is used interchangeably to describe information security, network operations, network defense, the employment of non-kinetic effects, electromagnetic warfare, or intelligence collection. This conflation undermines coherent discussion of strategy, policy, and force design, impeding the U.S. military's ability to compete—and ultimately prevail—in one of the primary domains our adversaries now exploit for strategic advantage.

In 2004, the Joint Chiefs of Staff recognized cyberspace as a "domain of conflict" (Office of the Chairman of the Joint Chiefs of Staff 2004). In 2010, cyberspace doctrinally became a domain of warfare, alongside land, sea, air, and space, with the creation of the U.S. Cyber Command (USCYBERCOM).[1] Yet despite being an independent domain, the U.S. military services largely treat cyberspace as a supporting function—an enabler of traditional joint functions instead of a domain with distinct areas, terrain, and potential for conflict. Many casual analogies and comparisons to traditional concepts in the physical domains perpetuate misperceptions and ultimately fail to treat cyber as a distinct domain of warfare. Instead, they relegate it to a warfighting function or joint function. This paradox has created confusion in force development and narrowness in force employment, and has led to the domain's neglect in operations and strategy.

The resurgence of great power competition has refocused the services on large-scale combat operations (LSCO), emphasizing what the joint force must do once war begins. In contrast, U.S. cyber strategy—anchored in persistent engagement—centers on competing left of conflict through continuous action in and through cyberspace (Fischerkeller and Harknett 2019). This creates a structural tension: if cyberspace continues to be treated primarily as

[1] See https://www.cybercom.mil/About/History/

a supporting function for other domains, resourcing will naturally gravitate toward cyber activities that enable LSCO—often in the form of electromagnetic warfare (EW) or information operations (IO)—at the expense of the capabilities required for competition-phase advantage. Meanwhile, adversaries are already conducting cyber-centric campaigns; most recently, the PRC's Volt Typhoon activity sought to preposition access within U.S. critical infrastructure for deterrent and coercive effect (Cybersecurity and Infrastructure Security Agency 2024). These developments highlight the need to differentiate cyber operations that support traditional domains from those required to secure advantage in cyberspace itself.

This paper argues that current U.S. military doctrine and organizational practices focus solely on cyberspace as a cross-domain enabler, while neglecting it as a domain of independent operational and strategic consequence. Drawing from joint publications (JP), Army and Air Force doctrine, and historical comparisons to the evolution of air and space power, our paper illustrates how cyberspace operations remain overly generalized and conceptually tethered to supporting traditional warfighting functions in other domains. More critically, we illustrate how current ideas about cyber and joint functions neglect cyberspace as its own domain of warfare, resulting in poor operating concepts and the conflation of cyber with EW and IO. Lastly, we argue how viewing cyberspace solely through the lens of enabling operations in the other domains has undermined the doctrine, concepts, and capabilities that the U.S. military needs to prevail in cyber conflicts, particularly where physical domains are not contested. This gap is especially dangerous given that U.S. adversaries increasingly view cyberspace operations as an independent and central part of their national strategies to compete with and undermine the resolve of the United States.

The central problem is that doctrine treats all cyberspace activities as a single category, obscuring the difference between cyber operations that support other domains and those required to secure superiority within cyberspace itself. If cyberspace control operations were defined as a distinct mission, geographic combatant commands (COCOMs) would integrate cyberspace superiority into campaign planning and deliberately employ non-cyber assets to shape cyberspace terrain. Likewise, service doctrine would separate EW and IO from cyber operations, allowing each to mature its own organizing, training, and equipping practices. These changes would align cyber force generation with other domains and give the military a coherent way to resource and fight for cyberspace superiority.

CYBERSPACE IN JOINT DOCTRINE

Within joint doctrine, cyberspace is considered merely in terms of its contributions to operations in the other domains. Cyberspace is rarely viewed as a domain for achieving policy or military objectives in its own right.

For example, current joint doctrine defines cyberspace as a global domain within the information environment (Joint Chiefs of Staff 2018a). JP 3-12, *Cyberspace Operations*, characterizes the domain as dependent on physical domains and highlights its role in enabling fires, kinetic maneuver, and command and control (C2). Rather than treating cyberspace as an independent operational domain worthy of support, the publication frames it primarily as a means of supporting the other domains of warfare through effects that are often non-kinetic or informational. There are notional acknowledgements of the unique topologies and terrain that constitute cyberspace (Joint Chiefs of Staff 2018a). However, there is little or no discussion of how maneuver is conducted within the domain or coordinated within joint operations.

Army doctrine follows a similar logic. Field Manual 3-12, *Cyberspace and Electronic Warfare Operations*, portrays cyber operations as embedded within combined arms operations (Department of the Army 2021). There is no mention of the decisiveness of cyberspace as an independent domain (like land).[2] Instead, cyberspace is depicted as a cross-cutting tool to enhance the effectiveness of land operations. Furthermore, Army cyberspace force generation is restricted to only three of the six traditional warfighting functions—fires, intelligence, and protection. It does not focus on building competencies in cyber maneuver, C2, or sustainment (Department of the Army 2021). Here again, Army doctrine focuses on describing how operations within cyberspace support warfighting functions in land warfare (Department of the Army 2021).

The Air Force offers a slightly different view, nominally treating cyberspace as a co-equal domain. Still, Air Force Doctrine Publication 3-12 integrates cyber under its broader IW umbrella, alongside EW and intelligence, surveillance, and reconnaissance (ISR) (Department of the Air Force 2023). Offensive cyber capabilities are often framed as enablers for kinetic missions, such as disabling air defense systems before a strike. Thus, despite acknowledging cyberspace as an independent domain of warfare, the Air Force continues to place heavy emphasis on the domain's utility in supporting broader air campaign objectives (Department of the Air Force 2023).

Army and Air Force doctrine approach cyberspace in a manner consistent with how each service treats other non-core domains: they focus on integrating those capabilities into their primary mission sets. As stated in FM 3-12, the purpose of the publication is to "[describe] how commanders and staffs can integrate cyberspace operations and electromagnetic warfare into unified land operations" (Department of the Army 2021, v). This is analogous to FM 3-04, *Army Aviation*, which governs how aviation assets provide support to land forces (Department of the Army 2025). Yet while FM 3-04 offers non-aviators substantial insight into how the

[2] Cyber persistence theory explicitly challenges the idea of singular, decisive cyber outcomes, arguing instead that cyberspace advantage is achieved through continuous interaction rather than decisive blows (Fischerkeller and Harknett 2019). This view may explain why joint doctrine is hesitant to characterize cyberspace in terms analogous to the decisive operations associated with land, maritime, or air domains. However, joint doctrine does not reflect the concepts of cyber persistence theory either, suggesting that the lack of decisiveness stems from perceptions of cyberspace as a domain rather than from the debated nature of the argument.

air domain supports ground operations, FM 3-12 provides comparatively little guidance for non-cyber warfighters on cyberspace as a domain. More importantly, FM 3-04 does not represent a large share of the existing doctrine on the air domain. Instead, the Air Force provides a comprehensive corpus of air domain doctrine. This pattern indicates that as long as cyberspace remains framed primarily as an enabler of other domains, cyber doctrine will remain shallow and fragmented.

Several partners and allies mimic aspects of the American approach. On the one hand, NATO formally declared cyberspace an operational domain in 2016. It subsequently developed detailed frameworks for domain-specific planning that clearly delineate between cyber supporting joint functions and cyberspace as a domain of battle (Shea; Ablon 2019). However, Smeets (2023) shows that some NATO countries are reluctant to employ and develop cyber capabilities in ways that respect cyberspace as a battlefield in its own right.

In partial contrast, the Chinese People's Liberation Army (PLA) has more explicitly defined cyberspace as its own battlefield. Although they categorize cyber warfare as an element of IW, what they describe as the characteristics of military conflict in cyberspace more closely resembles the American conceptualization of a domain and battlespace rather than a supporting function (PLA National Defense University 2020). Chinese doctrine goes as far as stating that cyber is "the core center that determines the outcome of a war" (PLA National Defense University 2020). While U.S. doctrine discusses the impact of cyberspace on the physical battlefield, the Chinese recognize that "every time a new battlefield is opened up, the seizure and control of [the cyber battlefield] will become the key to victory in combat" (150). Chinese doctrine appears to provide a more holistic view of cyberspace than can be found anywhere in U.S. doctrine.

Military doctrine is essential for establishing common concepts and a shared vocabulary that enable services, commands, and leaders of all ranks to align and communicate clearly and precisely. However, the value and purpose of doctrine are not always appreciated. Critics argue that it can be cumbersome or constrain thinking, and therefore, doctrine is often disregarded or ignored. That said, the inconsistent application or adherence to doctrine should not cause us to dismiss it as useless. Rather, the objective of this paper is to examine the need for clear and precise doctrinal terminology to enable more effective and mature competition, deterrence, and warfighting in the cyber domain.

CYBERSPACE AS A DEBATED DOMAIN

Debates over cyberspace's status as a military domain have persisted for more than thirty years (Arquilla and Ronfeldt 1993). Among others, Libicki (2012) contends that cyberspace is not a traditional warfighting domain because it lacks tangible geography and is instead a human-constructed network of information systems. Dombrowski and Demchak (2014) state that cyberspace is not actually a domain, but a substrate upon "which modern society is built" (5). In contrast, Lambach (2019) demonstrates that states have begun to territorialize cyberspace—imposing boundaries and exercising control through infrastructure, regulation, and legal jurisdiction—thereby rendering it a governable and contestable space. Furthermore, Aucsmith (2018) argues that although cyberspace is different from the physical world of the past, it has become the global center of gravity for the existence of all nations.

Critics do not claim cyberspace is inconsequential, but that it is consequential because of its impact on kinetic domains. However, the validity of cyberspace's impact as an enabler in other domains should not be used to invalidate it as a domain of operational significance. Rather, it becomes even more crucial to clearly define cyberspace concepts and doctrine to distinguish between referring to it as an enabler versus a domain.

These perspectives illustrate the tension between cyberspace's non-physical nature and the reality that it has long been contested and fought over as an operational environment. As a result, defining the standards of control and superiority in cyberspace is critical for establishing better terminology for cyber doctrine. Furthermore, this section will briefly address what is meant by "cyber war," and the extent to which conflicts in cyberspace can be equated to those in other domains.

In some ways, establishing, maintaining, and contesting control in cyberspace mirrors the logic of territorial control in other domains, although the terrain spans both physical and logical planes. Control begins with the ability to exert influence over specific portions of cyberspace—servers, networks, services, or data flows—even when ownership or physical custody resides elsewhere. Ransomware provides a convenient illustration: a victim may physically possess the hardware yet lose functional control over its data and services. Similarly, a friendly cyber actor may contest a malicious adversary's activities on a third-party cloud provider's infrastructure. The physical servers remain under the provider's jurisdiction, yet both actors employ tactics, techniques, and procedures to gain or deny access, persistence, and effect—contesting a shared logical terrain. Thus, military control of cyberspace does not imply uncontested dominance or superiority, but rather the ability to reliably control the specific segments of the domain necessary to accomplish operational or strategic objectives.

Libicki (2012) argues that superiority in cyberspace is impossible because there are limitations to the domain that are insurmountable by even the most capable attacker. However, military superiority in cyberspace is defined as the degree of control of cyberspace "by one force that permits the secure, reliable conduct of operations by that force and its related land, air, maritime, and space forces at a given time and place without prohibitive interference". This definition parallels traditional notions of superiority in air, maritime, or land warfare. Superiority is not absolute; it is localized and temporal. It is an assessment validated only by the act of proving as much. The side that can consistently impose its will within the operationally relevant portion of cyberspace—whether by defending friendly networks, degrading adversary capabilities, or exploiting access to achieve operational effects—possesses the advantage.

Recognizing that cyberspace can be contested and controlled makes the plausibility of cyber war harder to dismiss. Skeptics maintain that "war" confined exclusively to the cyber domain is neither meaningful nor possible (Rid 2011). Yet recent events suggest otherwise. The ongoing activities attributed to the Chinese state-sponsored actor Volt Typhoon (Cybersecurity and Infrastructure Security Agency 2024) exemplify a form of cyber warfare aimed not at seizing territory but at achieving policy objectives through the persistent compromise of critical infrastructure. As Clausewitz reminds us, "war is merely the continuation of policy by other means." Using Clausewitz's criteria of war, a "cyber war" should demonstrate the threat of violence, instrumentality, and political purpose. In this sense, a cyber war may be waged entirely through digital means without kinetic engagement. Volt Typhoon's strategy—to pre-position access within U.S. critical systems to deter or delay American intervention in a Taiwan contingency—meets all the criteria. Whether or not analysts accept that Volt Typhoon constitutes an ongoing "cyber war," its activities meet Clausewitz's criteria and therefore fall within the spectrum of warfare. In that sense, it clearly demonstrates that adversaries perceive cyberspace as a domain in which war can be conducted independently of physical combat.

Critics also claim that the absence of kinetic victory conditions—territorial gains or human casualties—disqualify cyberspace as a domain and kind of war (Rid 2011). Yet such critiques often reflect a distinctly Western preference for decisive battle, rooted in a cultural tradition that equates victory with the destruction of an opponent's forces and the seizure of territory (Hanson 2013). The expectation of a singular, conclusive engagement is ill-suited to cyberspace, where the interconnected and digital nature of the domain precludes the permanent conquest or occupation of terrain.

Cyber persistence theory, which underpins the strategy of persistent engagement, clarifies what "victory" looks like in this environment (Fischerkeller, Goldman, and Harknett 2022). Rather than seeking decisive outcomes or permanent control, the theory holds that success derives from the continuous shaping of the strategic environment through constant contact, initiative, and exploitation of advantage—an operational necessity born of the inherent interconnectedness of cyberspace. Victory, therefore, is not an end state but an enduring condition maintained through persistent presence, contestation, and adaptation. Unlike a "fait accompli" in the physical domains, where victory is achieved by quickly seizing and holding terrain, a cyber fait accompli occurs when an actor can influence, access, and take initiative within an adversary's networks or systems long enough to impose costs or compel restraint.

This article positions itself within that debate by asserting that cyberspace is both constructed and contestable in line with the framework of persistent engagement. Here, cyberspace is a distinct, continuous battlespace in which operational and strategic interactions occur below the threshold of (kinetic) armed conflict. It is a man-made environment in which control and superiority can be gained or lost, even if it is not physically occupied.

THE JOINT FUNCTIONS IN CYBERSPACE

Domains of warfare entered our modern military lexicon as part of Joint Vision 2020, defining the arenas in which military forces operate. They have shaped force structure, purpose, and the operational environment ever since. Joint functions, by contrast, describe the core categories of capability and activity that enable commanders to conduct operations. Doctrinally, JP 3-0, *Joint Operations*, outlines seven joint functions (Joint Chiefs of Staff 2018b, xiii). Joint functions are not another level of organization; they are a heuristic model that helps commanders understand the various ways that power can be directed within the warfighting domains to achieve desired ends.

Information, the newest joint function, was formally added to the list in 2017. It arguably has the most convoluted description of all seven (Crosby 2019, 96). Nevertheless, to conduct successful joint operations, all seven joint warfighting functions—C2, information, intelligence, fires, movement and maneuver, protection, and sustainment—must be applied across all domains. Success also demands understanding how the joint functions contribute to combat power and how to integrate them collectively.

Therefore, successfully waging warfare in and through cyberspace requires commanders to perform the seven joint functions in cyberspace. Yet, as discussed above, cyberspace is most often framed as another joint function—not a domain in which the joint functions are brought to bear. This conceptual conflation obscures the operational reality that each joint function must also be executed within cyberspace. Misframing cyberspace as a joint function manifests as bias in operational planning and employment of the Cyber Mission Force (USCYBERCOM 2023), effectively overlooking and oversimplifying the modes of competition and warfighting in cyberspace.

Ironically, the ubiquitous nature of cyberspace may partially explain why it has been neglected as a warfighting domain. Whereas land, sea, air, and space have relatively clear and distinct boundaries, cyberspace is woven into nearly every modern weapon system and military operation. Cyberspace, therefore, manifests itself to most service members as a dependency or vulnerability in their more traditional warfighting tasks. This has given each service a clear stake in, and use for, cyberspace as an enabler, even while they overlook the potential, complexity, and nuance of the domain itself.

The overly generalized use of the term cyberspace has created ambiguity, which, in turn, has contributed to its neglect as a warfighting domain. The most egregious example of this generalization may be the conflation of cyberspace and EW, or the electromagnetic spectrum (EMS). Doctrinally, EW is an action using electromagnetic energy to influence radio frequencies (Joint Chiefs of Staff 2019a, 76–77). Although cyberspace can traverse the EMS (e.g., via digital radios), it is neither contained within or wholly dependent upon it (Joint Chiefs of Staff 2015, III–11). However, both the Army and the Air Force have invested in the creation of so-called "cyber capabilities" that are actually radio frequency (RF)-based EW capabilities (Pomerleau 2024b, 2024a). The trend of equating cyber with EW is, therefore, not only misleading but also a prime example of the deleterious effects of poor terminology in the cyber domain.[3]

Another conflation that affects cyber operations is the embedding of cyber within the information environment. Because cyberspace is doctrinally defined as being wholly contained within the information environment, it has become impossible to decouple cyber operations from IO and the—already convoluted—information joint function. JP 3-12 claims that the information function "encompasses the management and application of information and its deliberate integration with other joint functions to influence perceptions, behavior, action or inaction, and human and automated decision making" (Joint Chiefs of Staff 2018a, xii). While some operations in the information environment may be conducted solely through cyber operations, not all cyber operations affect the information environment as described in doctrine. Therefore, constraining cyberspace to the information environment inhibits more effective military planning by stove-piping the entire domain into a subset of activities that exclude cyber operations as a means to cyber ends. Some of our adversaries have recognized the folly of this fusion and have separated their cyber and information forces into distinct organizations (Bruzzese and Singer 2024). Meanwhile, our conflation of cyber as merely a component of the information environment will continue to undermine our operational advantages within cyberspace.

CYBER OPERATIONS & JOINT FUNCTIONS

This section examines the difference between cyberspace as an enabler versus cyberspace as a domain of warfare. Current doctrine defines cyberspace operations as the employment of cyberspace capabilities with the primary purpose of achieving objectives in or through cyberspace. Such breadth, while conceptually inclusive, has proven to be vague, obscuring the distinction between activities that merely support operations through cyberspace and those that seek to secure advantage within cyberspace.

[3] The conflation of different technologies is not unique to cyber. Rather, there is a tendency for emerging or advanced science to be inappropriately blended with existing or related technologies (Smith 2014).

To improve analytic and doctrinal clarity, we introduce the term *cyberspace control operations* to describe cyberspace operations aimed at controlling or establishing military superiority in cyberspace. This taxonomy has already proven useful, evidenced by existing doctrine that distinguishes land and sea operations from land and sea control operations (Joint Chiefs of Staff 2019b, 137). The distinction between these two terms illustrates how improved terminology can clarify when discussing cyberspace as either an enabling function or an independent domain of warfare.

Cyberspace operations should support all seven joint functions. For example, cyberspace operations can enable secure communications and protect the integrity of the Department of War Information Network (DoWIN, formerly known as DoDIN), without which mission execution—in cyberspace or in any other warfighting domain—would falter. However, in cyberspace control operations, the C2 function encompasses the time-sensitive synchronization of cyber effects and the management of complex authorities for cyber action. It must account for operations that occur at the speed of machines, happen simultaneously around the globe, and interact with non-combatants in unprecedented ways.

Similarly, maneuver for cyberspace control occurs through access discovery, exploitation, credential manipulation, and the denial of adversary presence. Protection for cyberspace control focuses on preventing the compromise of digital capabilities and equities. Sustainment is likewise the generation of capabilities and infrastructure for cyber combat power. Fires, perhaps the most discussed of the joint functions in cyberspace, would also include kinetic effects that set the conditions for cyberspace activities. Collectively, these functions exemplify cyberspace control operations in a way that cannot be misconstrued as enabling functions for other domains.

As with the information function discussed above, intelligence is another useful example that illustrates the consequences of confusing “cyber as an enabler” with “cyber as a domain”. Cyberspace operations are both a large consumer and producer of intelligence. As an enabler, cyber produces intelligence about the other domains. At the same time, cyber also consumes all forms of intelligence about the cyber domain during cyberspace control operations. Furthermore, the distinction between cyber as an intelligence producer and as an intelligence consumer is critical. Both types of operations often require similar capabilities for operational intelligence collection. However, in cyberspace, the same defenses protect from all forms of cyber operations, regardless of whether the adversary intends to collect intelligence or cause effects (Inglis 2019). Therefore, as with information, categorizing cyberspace operations as an intelligence function can inadvertently compromise cyberspace control operations by emphasizing intelligence gain or loss over movement and maneuver.

CYBERWARFARE IS MANEUVER WARFARE

The preceding analysis illustrates how current doctrine constrains cyberspace to a supporting role within the joint functions. It is particularly important to examine how this constraint has also stunted the conceptual development of cyber as a domain of maneuver warfare. Maneuver warfare defines how the joint force approaches seizing the initiative and shaping the battlespace. Without the concept of maneuver, a domain lacks the theoretical grammar needed to plan campaigns, integrate joint functions, or generate combat power and sustain superiority. Since the early 1990's, doctrinal theorists including Arquilla and Ronfeldt (1993), have recognized that cyberspace deserves its own concepts and definitions of maneuver. For instance, Applegate (2012) argued that the principle of maneuver applies equally to cyberspace. In his view, maneuver in cyberspace was not a means to enable operations in other domains, but rather the dynamic repositioning of digital forces through access, persistence, effects, and information flows to gain relative advantage. However, more than a decade later, Joint and Army doctrine still lacks any description of cyber maneuver, instead focusing on what that activity would enable (Department of the Army 2021, 1–3). Instead, cyber maneuver, as it exists today, typically sets the conditions for physical maneuver, such as disrupting enemy communications ahead of a ground assault (2–7).

Allen (2020) advanced this argument by describing cyber maneuver as a series of interlocking operational behaviors—preparing the environment, persistence, deception, tempo, and initiative—that collectively produce positional advantage. In Allen's framework, cyber maneuver is not a discrete event but an iterative process that parallels classical operational art. His articulation bridges the gap between maneuver theory and cyber operations, showing that maneuver in cyberspace consists of continually repositioning access and capabilities to maintain initiative and deny the adversary the same. Together, Applegate and Allen establish a coherent understanding of cyber maneuver, yet service and joint doctrine have failed to adopt these concepts, instead focusing on cyber as it aligns with service domain interests.

A lack of cyber maneuver doctrine forces warfighters to rely on analogies between movement and maneuver in the physical domains and in cyberspace. Using these analogies to explain cyber operations, tactics, and strategy has a prejudicial impact on operational planning. Furthermore, the predisposition to limit the purpose of cyber maneuver does not end with planning. It extends to acquisitions, effects, measures of effectiveness, measures of performance, and beyond. Descriptors such as the cyber bullet, cyber rifle, and cyber bombs provide a non-cyber commander with a visual representation of capabilities that fail to encompass or accurately represent a cyber effect, tool, or what the Cyber Mission Forces can offer. Inflexible notions of what physical bullets do are therefore applied to the cyber capability, creating a false equivalency and oversimplifying cyber maneuver.

The oversimplification of cyber maneuver has contributed to cyberspace operations being viewed almost exclusively as joint or warfighting functions, thereby relegating them to supporting physical-domain objectives. There is little doctrinal precedent or practical integration for leveraging physical-domain capabilities in support of cyber objectives or outcomes. Cyber needs are largely absent from phasing, logistics, or other aspects of joint plans. This one-directional “integration” reinforces the perception that cyberspace is a supporting utility rather than a battlespace.

HISTORICAL CONTEXT OF DOMAIN INDEPENDENCE

History suggests that new domains are initially treated as support functions before they are understood or acknowledged as independent operational and strategic arenas. In the case of air and space power, for example, the shift from support function to domain of warfighting typically requires a combination of technical innovation, bureaucratic entrepreneurship, and strategic necessity.

Early pilots and aircraft were seen as extensions of artillery and reconnaissance for ground forces. During World War I, air units were largely subordinate to Army field commands, mirroring today’s integration of cyber forces within service components. Only after decades of advocacy, bureaucratic wrangling, and another World War was the U.S. Air Force formally established. With it, military doctrine shifted from air support to air superiority and airpower from an auxiliary capability into a domain-defining concept.

Space followed a similar path. Initially a platform for communications and reconnaissance, it remained under Air Force control for decades. Scholars including Dolman (2012) argued that “space control”, like command of the air, would constitute a precondition for national security in the twenty-first century. The creation of the U.S. Space Force in 2019 marked a shift in this direction, treating space as more than just an enabler but also a contested domain that requires its own doctrine and force structure.

Cyberspace is not new. Yet today’s military thinking still parallels earlier stages in the emergence of other domains. While U.S. Cyber Command is a unified command, the services still own and train the bulk of cyber forces. Cyber units are deployed to either support other components or operate independently of air, land, sea, or space capabilities.

Comparative analysis underscores that the doctrinal and organizational maturation of other domains has always required both intellectual and institutional entrepreneurship. The air and space communities developed distinct professional identities, operational art, and doctrinal language that justified their independent status. Whether cyberspace ultimately achieves the same institutional independence will depend upon the military’s ability to convert concepts such as cyberspace control operations into coherent doctrine and enduring organizational practice.

DOCTRINAL GAPS AND RECOMMENDATIONS

Despite joint recognition of cyberspace as a domain, cyber doctrine remains immature. Without a doctrinal proponent for cyber at the operational level, its integration often depends on ad-hoc efforts by commanders. Conceptual confusion between EW, IO, cyberspace operations, and intelligence operations compounds the problem. The services also tend to combine defensive cyber operations with those who build and operate their networks. As a result, it is not uncommon for a network operator, such as a service Chief Information Officer (CIO), to use the term cyber to mean something categorically different than when used by a member of the Cyber Mission Force. Blurring these lines dilutes the distinct operational requirements of cyberspace, reduces its effectiveness as a domain, and hinders meaningful conversations on topics such as cyber readiness.

One critical implication of this doctrinal gap lies in its effect on force generation. The USCYBERCOM 2.0 effort attempts to refine how cyber forces are trained and equipped. However, this initiative requires a mature and coherent domain-specific doctrine to guide the creation of mission-ready forces.

The current lack of such doctrine impacts the development of a force generation model, such as that used by the exemplar: Joint Special Operations Command (JSOC). JSOC leverages well-established domain concepts in air, land, and maritime operations to rapidly generate and employ highly tailored, high-readiness forces. In contrast, because cyberspace is not conceptualized or matured as a domain with distinct operational ends and ways, a JSOC-informed or demand-driven model of cyber force generation will struggle to take root. This disconnect risks generating forces that are optimized to support traditional domains rather than operate effectively in the cyber domain against cyber-capable adversaries.

Closing these conceptual and doctrinal gaps requires a more deliberate effort to define the operational grammar of cyberspace and its relationship to existing domains. One necessary step is to formalize the concept of cyberspace control operations in joint doctrine, paralleling the existing terms of “land control operations” and “sea control operations”. Cyberspace control operations are the mechanism by which the Joint Force achieves localized and temporal advantage in cyberspace, wherein strategic and operational objectives can be pursued through sustained interaction, with or without a decisive or kinetic battle. This definition equips commanders with a lexicon to describe the establishment, maintenance, and contestation of control in cyberspace, along with the associated authorities and effects. Formalizing cyberspace control operations would also help articulate the relationship between the joint functions and cyberspace when viewed as a domain, rather than as an enabler. This conceptual clarity would, in turn, help commanders better integrate cyber operations into campaign design and joint operational planning.

It is also necessary to recognize that cyberspace is global and distributed by nature, and requires interaction among extra-national stakeholders. As a result, it is unhelpful to bound cyber terrain along the lines of typical geopolitical boundaries (e.g., Europe or the Indo-Pacific). We should think of it instead in terms of functionality (Raike 2018), as is the case for autonomous systems (Hawkinson 1996), cloud service providers, virtual private networks, and the like. Doing so would enable better planning, coordination, and assignment of command authority within cyberspace operations.

Trying to force cyberspace to fit existing geographic areas of responsibility is, like other misplaced metaphors and analogies, perhaps another original sin that has led to the issues presented within this paper. The distinction of cyberspace control operations, and the ability to align authorities and forces to them depends upon clearly defined boundaries that accurately reflect the battlespace. For example, who authorizes operations against the Russian military when the target is a third-party Brazilian company whose servers are hosted in the Chinese data center of a U.S. Cloud Service Provider? Nearly every geographical combatant commander could be involved, but none would have clear visibility of where their portion of cyberspace begins or ends. Long-standing authorities and global coordination challenges can only be addressed by recognizing cyberspace as a distinct geography.

Finally, cyberspace must be doctrinally disentangled from the broader information environment. Leaving cyberspace nested within this construct conflates cyber operations with IO and diminishes its role as a distinct domain. This doctrinal alignment reduces cyberspace to a set of non-kinetic effects or supporting functions in support of kinetic objectives. Doctrinally separating cyberspace from the information environment would enable the development of concepts that treat cyberspace as a battlespace with independent operational and strategic consequences.

While not a comprehensive list, we hope that these doctrinal changes will serve as a catalyst for treating cyberspace as a domain with its own operational significance. The PRC has embraced cyberspace, effectively prepositioning themselves to fully deter American resolve ahead of a potential invasion of Taiwan. While the U.S. military prepares for a kinetic fight that may never come, the cyber war is occurring now.

ABOUT THE AUTHORS

Skyler Onken is a co-founder of Twenty, a cyber warfare defense tech startup, and Major in the Army Reserves. He has been a member of the Cyber Mission Force since 2014 as an Interactive Operator, Cyber Capabilities Developer, Mission Commander, and Task Force Mission Director. He has served as a member of both National and Combat Mission Teams, site lead of Cyber Solutions Detachment-Georgia, and the Joint Mission Operations Center-Georgia. His most recent contributions include work on the CYBERCOM 2.0 Operational Planning Teams, and participation in the Secretary of the Army's Strategic Seminar on Cyber. As a reservist he continues to contribute to operations as a Master Cyber Operator within the 780th Military Intelligence Brigade's Individual Mobilization Augmentee program.

Dr. Margaret Webber is a lecturer for the University of New Hampshire's homeland security program and a soon-to-be-retired US Army officer who previously served as a strategic planner and a researcher at the Army Cyber Institute. She was also an assistant professor in the Department of Social Sciences at the United States Military Academy, teaching courses on American politics, cyberspace operations, and her elective, "Politics and the Internet" that investigated how citizen-government relationships have changed with the internet. Margaret also served as a cyber operations planner and mission commander for the Cyber National Mission Force, targeting violent extremist organizations and malicious cyber actors. Margaret's academic research and teaching interests are focused on third-party actors in cyberspace and the geopolitics of military cyberspace operations. She is a Senior Nonresident Fellow with the Atlantic Council's Cyber Statecraft Initiative and a Senior Fellow at the Washington College of Law, American University.

ACKNOWLEDGMENTS

The authors are deeply grateful to those who helped refine the concepts and content of this paper, including Dr. Erica Lonergan, Col. Todd Arnold, Maj. Nick Starck, Maj. JC Fernandes, Dr. Sam Tangredi, and the entire faculty of the Naval War College Cyber and Innovation Policy Institute.

REFERENCES

Ablon, Lillian. 2019. *Operationalizing Cyberspace as a Military Domain.* RAND Perspectives, June 20, 2019. https://www.rand.org/pubs/perspectives/PE329.html.

Allen, Patrick D. 2020. "Cyber Maneuver and Schemes of Maneuver." Fall 2020, *The Cyber Defense Review* 5 (3). https://www.jstor.org/stable/26954874.

Applegate, Scott D. 2012. "The Principle of Maneuver in Cyber Operations." In *Proceedings of the 3rd International Conference on Cyber Conflict.* https://ccdcoe.org/uploads/2012/01/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf.

Arquilla, John, and David Ronfeldt. 1993. *Cyberwar Is Coming!* RAND. https://www.rand.org/pubs/reprints/RP223.html.

Aucsmith, David. 2018. "Disintermediation, Counterinsurgency, and Cyber Defense." In *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.* Bloomsbury Academic.

Bruzzese, Matt, and Peter W. Singer. 2024. *Farewell to China's Strategic Support Force. Let's Meet Its Replacements.* Defense One, April 28, 2024. https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143/.

Crosby, Thomas. 2019. "Getting the Joint Functions Right." *Joint Force Quarterly* 94 (3): 96–100. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1913080/getting-the-joint-functions-right/.

Cybersecurity and Infrastructure Security Agency. 2024. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* Cybersecurity Advisory, February 7, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

Department of the Air Force. 2023. *Cyberspace Operations (AFDP 3–12).* Washington, D.C. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf.

Department of the Army. 2021. *Cyberspace and Electronic Warfare Operations (FM 3–12).* Washington, D.C.

Department of the Army. 2025. *Army Aviation.* Washington, D.C.

Dolman, Everett C. 2012. "New Frontiers, Old Realities." *Strategic Studies Quarterly* 6 (1): 78–97. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-1/dolman.pdf.

Dombrowski, Peter, and Chris C. Demchak. 2014. "Cyber War, Cybered Conflict, and the Maritime Domain." *Naval War College Review* 67 (2): 1–27. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1321&context=nwc-review.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford University Press.

Fischerkeller, Michael P., and Richard J. Harknett. 2019. "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation." Special Edition: International Conference on Cyber

Conflict (CYCON U.S.) *The Cyber Defense Review,* 267–283. https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf.

Gibson, William. 1984. *Neuromancer.* New York, NY: Ace Books.

Hanson, Victor Davis. 2013. *The Western Way of War: Infantry Battle in Classical Greece.* Knopf Doubleday Publishing Group.

Hawkinson, J. 1996. *Guidelines for Creation, Selection, and Registration of an Autonomous System (AS).* RFC 1930, March. https://datatracker.ietf.org/doc/html/rfc1930.

Inglis, Chris. 2019. "Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace." In *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations.* Rowman & Littlefield.

Joint Chiefs of Staff. 2015. *Joint Communications System (JP 6–0).* Washington, D.C.

Joint Chiefs of Staff. 2018a. *Cyberspace Operations (JP 3–12).* Washington, D.C.

Joint Chiefs of Staff. 2018b. *Joint Operations (JP 3–0).* Washington, D.C.

Joint Chiefs of Staff. 2019a. *DOD Dictionary of Military and Associated Terms (JP 1–02).* Washington, D.C.

Joint Chiefs of Staff. 2019b. *Joint Land Operations (JP 3–31).* Washington, D.C.

Jones, Thomas, and Jen Calleja. 2011. *William Gibson: Beyond Cyberspace.* The Guardian, September. https://www.theguardian.com/books/2011/sep/22/william-gibson-beyond-cyberspace.

Lambach, Daniel. 2019. "The Territorialization of Cyberspace." *International Studies Review* 22.

Libicki, Martin C. 2012. "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* 8 (2): 325–340.

Office of the Chairman of the Joint Chiefs of Staff. 2004. *The National Military Strategy of the United States of America.* Washington, D.C.: U.S. Government Printing Office.

PLA National Defense University. 2020. *Science of Military Strategy.* China Aerospace Studies Institute. https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf.

Pomerleau, Mark. 2024a. *'This is overdue' — Air Force creating tactical cyber capabilities to ensure air superiority.* DefenseScoop, May 23, 2024. https://defensescoop.com/2024/05/23/air-force-creating-tactical-cyber-capabilities-ensure-air-superiority/.

Pomerleau, Mark. 2024b. *Army building a new expeditionary cyber battalion.* DefenseScoop, November 26, 2024. https://defensescoop.com/2024/11/26/army-building-a-new-expeditionary-cyber-battalion/.

Popova, Maria. 2014. *How William Gibson Coined Cyberspace.* The Marginalian, August 26, 2014. https://www.themarginalian.org/2014/08/26/how-william-gibson-coined-cyberspace/.

Raike, Brian R. 2018. *Maneuver Warfare in Cyberspace.* Marine Corps Gazette, October 1, 2018. https://www.mca-marines.org/gazette/maneuver-warfare-in-cyberspace/.

Rid, Thomas. 2011. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Shea, Jamie. *Cyberspace as a Domain of Operations: What Is NATO's Vision and Strategy,* 2. https://doi.org/10.21140/mcuj.2018090208.

Smeets, Max. 2023. "The Challenges of Military Adaptation to the Cyber Domain: A Case Study of the Netherlands." *Small Wars & Insurgencies* 34 (7): 1343–1362. https://doi.org/10.1080/09592318.2023.2233159.

Smith, Frank L. 2014. *American Biodefense: How Dangerous Ideas About Biological Weapons Shape National Security.* Ithaca: Cornell University Press.

USCYBERCOM (U.S. Army Cyber Command). 2023. *Cyber Mission Force.* U.S. Army Cyber Command, November. https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/.

USCYBERCOM (U.S. Cyber Command). *Command History.* https://www.cybercom.mil/About/History/.

Received 1 August 2025; Revised 10 November 2025; Accepted 20 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 163-178
https://doi.org/10.55682/cdr/cybr-cag3

RESEARCH ARTICLE

Breaking the "Cyber" Cage: Reinventing Cyber Command for Great Systems Conflict

Chris C. Demchak*

U.S. Naval War College, Newport, RI, USA

In an era of escalating and pervasive digital conflict, this paper argues that the U.S. Cyber Command must be updated in its remit, reputation, and structure. In order to effectively match the changing global distribution of power and capabilities, especially with the rise of China, the Command's mission space should expand well beyond the "cyber" designation and constraints. Its broader mandate must encompass and employ the entire spectrum of advanced technologies from artificial intelligence and robotics to quantum computing. The renewed organization also needs to directly manage the intake and development of a robust digital talent pipeline for the needs of its own operations and those of the traditional services. Such restructuring and rebranding (potentially as a Digital Vanguard Command or a Cyber, Robotics, and Information Systems Command) places the organization as the central hub of advanced and comprehensive digital warfighting. By reinventing itself, in its publicly acknowledged function and in an expanded structure, U.S. Cyber Command can break out of the conceptual cage of a dated "cyber" identity, attract talent and enthusiasm for service, and more effectively bolster U.S. analytic superiority, operational effectiveness, deterrence, and systemic resilience in the turbulence of the mid-21st century's technology-driven Great Systems Conflict.

Keywords: cyberspace, cyber security, AI, resilience, "Great Systems Conflict", cyber force generation, robotics

* Corresponding author: chris.demchak@usnwc.edu

***Disclaimer:** The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

CONCEPTUAL CAGE OF OUTDATED TERMS

Over the past decade and a half since the establishment of the U.S. Cyber Command in 2009, the digitized world has moved from a relatively stable international system led by the United States to the emerging era of 'Great Systems Conflict' precipitated by China (Demchak 2021). For a quarter century, China has used its economic rise to strategically develop a large-scale socio-technical-economic system, aggressively seeking global advantage to displace the United States economically, politically, and technologically (Doshi 2021; Lind 2024; Mearsheimer 2003). This era exceeds prior Great Power competitions in intensity and ubiquity through the persistent exploitation of global digital connectivity (Shirk 2023). China relentlessly uses its socio-technical-economic scale to penetrate democratic states below armed conflict thresholds in extensive campaigns ranging from extortion to battlefield preparation (Mastro 2024). The resulting systemic hostility between the two 'Great Systems', China and the United States, now ushers in the rising 'Great Systems Conflict' era, fundamentally challenging global stability. The global environment is outpacing the conceptual expectations, structures, and institutional remits of existing U.S. national security organizations.

U.S. Cyber Command sits at the technological crossroads of this new era. Having been established to defend solely the military's networks, it now finds itself asked to defend the wider nation against massive assaults at the scale that a Great System like China can impose (Harknett and Smeets 2022). It has become the subject of an extended debate on whether its organizational structure is adequately scaled, manned, and empowered to effectively address the globally insecure cyberspace 'substrate' connecting the homeland to this now far more complex, turbulent, and hostile digitized world. As the main agency for U.S. military's cyber capabilities, Cyber Command struggles to effectively meet all the challenges it faces (Couillard 2024). Although the organization is recognized as the U.S. military's center of secretive offensive cyber activities, the Command is not widely perceived by other military or external stakeholder audiences as a major center of mastery over anything other than cyber across the entire digital ecosystem. That reputational shortcoming contributes to cyber force generation and related performance challenges sparking the current debate (Welch 2024).

This article argues that Cyber Command struggles today under a conceptual "cage" founded on a widespread perception of cyber as a separable "domain" - itself a term that expanded contemporaneously with cyberspace. That linguistic characterization now constrains the organization's identity and future capabilities (Gosain 2004). Three factors have built this "cage" over time. First, an initial mischaracterization of cyberspace has limited the internal stakeholders' definition of "cyber" operations, and ties the organization's identity to traditional military concepts despite significant differences (Slayton 2020; Kobie 2017). Second, early mischaracterizations contributed to a persistent misunderstanding of cyber operations by service audiences, leading traditional military leaders to undervalue cyber effects, providing lip service to cyber in their operational planning yet failing to effectively manage and retain cyber personnel (Hardison et al. 2019). Third, the wider societal audience, especially recruitable youth, have come to view cyber topics negatively as passé, tedious, technical work rather than an exciting frontier of innovations such as artificial intelligence (Pattnaik, Li, and Nurse 2023). As a result, while the current reform debate has converged on Cyber Command's force generation gap, the problems facing U.S. Cyber Command actually require removing this cage through a more systemic transformation of the Command's image, remit, and structure.

In an emerging future of Great Systems Conflict where China is reputed to have over a hundred thousand cyber warriors at any one time and to be dominating the new patents for advanced technologies, the threat environment is evolving differently than that imagined in 2009 with the establishment of a military command focused on cyber alone. The outlines of likely mid-21st-century conflicts suggest that combating the Chinese digitized tsunami will require a unifying 'pan-technology' military organization in response. Such a unit must ensure "analytic superiority" against all adversaries all the time by integrating across cyber's offspring in robotic, AI agentic, and algorithmic warfare at scale, as well as operating nonstop across cyberspace itself (Grossman and Goldman 2024; Jensen, Whyte, and Cuomo 2020). A Cyber Command reinvented as a 'Digital Vanguard Command' (DIGICOM) or 'Cyber, Robotics, and Information Systems Command' (CRISCOM) would be the updated 'go-to' locus of relevant and full-ecosystem digital expertise. It could absorb a subordinate unit offering direct enlistment and training, providing assets to the Command and sister services. While in-depth explorations of implementation exceed the scope of this article, such a restructured, reoriented, and rebranded organization constitutes a new approach to adapting the U.S. Cyber Command to the Great Systems Conflict era.

INADVERTENT MISALIGNMENT FROM THE OUTSET

Both "cyber" and "domain" are terms whose widespread use grew with the rise of the information age. As the last century closed, the Department of Defense increasingly digitized and networked its operations and turned to concepts such as "information warfare", "network centric warfare", and "computer network operations" to address the content and connectivity of a newly integrated digitally connected world (Warner 2012; Cebrowski and Garstka 1998). The term "cyberspace", however, seeped into U.S. military vocabulary in the 1990s alongside the term "domain", contributing to a doctrinal misunderstanding of cyberspace from the outset.

The word "cyberspace" was already in use elsewhere, having floated in niche academic, science fiction, and architectural (oddly enough) communities for years since Norbert Wiener's 1940s term "cybernetics" (Wiener 1948). Meant to capture human-machine control and communication derived from the Greek for steersman, *kybernetes*, cyberspace inspired the shorthand “cyber” adjective along the way. William Gibson’s seminal 1984 novel, Neuromancer (Gibson 1984), propelled the term into the national consciousness, representing a futuristic world dominated by networked computers (Arulmurugan and Jinnah 2024). Throughout the 1990s and early 2000s, cyberspace was still the exciting future of all things. As the United States defense community absorbed the longer term, the shorthand “cyber” grew from an adjective to a noun, concisely encapsulating everything from elite hacking units to the mundane reality of everyday information security.

Contemporaneously with cyberspace, the broader use of "domain" formally emerged in the military’s late-1990s "information environment" language. The full implications of the inter-state information technology struggle that would later drive Great Systems Conflict were just being recognized. By 1999, “ecommerce” had roiled the economy and China was surging internationally, in part by using digital technology to steal money and secrets, such that the US military needed to distinguish between the proprietary battlespaces of traditional services and the rising technological behemoth of the internet. By 2000, the U.S. military’s “Joint Vision 2020” for the first time characterized ‘information’ as a separable "domain" and distinguished between "physical and information domains" (Joint Chiefs of Staff 2000). Around the same time, “cyberspace” had prominently emerged in the wider defense community as an overarching term competing with “the Internet” to describe the global communications networks (Branch 2021; Rattray 2001). Then, in 2004, the U.S. National Military Strategy formally labeled cyberspace as a “global commons” and a “domain” of warfare equivalent to land, sea, air, and space (Alexander 2007). The U.S. military began to adopt the short term ‘cyber’ as a convenient catch-all noun to signify all things associated with computers and this new digital battlespace. That linguistic usage was formally blessed with the creation of the United States ‘Cyber’ Command in 2009 (Lilli 2020).

Framing cyberspace as a warfighting “domain” was bureaucratically rational to secure funding and authorities within the Pentagon’s organizationally rivalrous structure. But the term was not clearly defined. It was a mischaracterization.

Cyberspace is not now, nor has it ever been, a separable warfighting domain analogous to land, air, and sea. It is a ubiquitous and manufactured substrate, the ever-expanding foundational layer on which rest all modern information technologies—including artificial intelligence (AI), quantum computing, robotics, autonomous systems, and even information or electronic warfare. The early labeling of ‘information’ and then ‘cyberspace’ as ‘domain’ imposed conceptual barriers tied to the early misunderstandings of the substrate and the larger digitized ecosystem as largely networks and code. That limiting perception further separated cyberspace from the other concerns of military operations, such as kinetic and lethal exchanges. In 2002, a well-known defense policy scholar called cyber attacks “Weapons of Mass Annoyance” (Lewis 2002). By the early 2010s and the formation of Cyber Command, winning a war by fighting solely through networks was disparaged across the defense community. As a result, both early Cyber Command denizens and the Command's external audiences learned to view the organization's mission space narrowly as repelling adversaries from networks.

For this conceptually isolated 'domain', early grand strategic visions of a stand-alone battle 'domain' determining major outcomes or whole wars failed to broadly take root (Arquilla and Ronfeldt 1993). By the early 2010s, the dominant notion was that one was 'defending' the military networks that composed cyberspace, operating largely as a support function or working through the globe's networks for intelligence purposes. There was never to be "cyber war" because, it was argued, nobody was killed when a computer was hacked or data destroyed (Rid 2012). Cyber Command's remit and identity were conceptually 'caged' to digital networks and associated software early on [1]. As the Command consolidated, organizational forces would further lock these early misunderstandings into place.

FRAMING THE CAGE: INSTITUTIONALIZED CONCEPTUAL LOCK-IN

Organizations are products of their foundation, imbued with their founders' values, biases, and assumptions at the time of formation (Thompson 1967). The founding leader's vision sets the initial conditions (Santora and Sarros 2008). If the second leader cohort does not change this vision, then the third leader will find it particularly challenging to change without dramatic events. Each new employee group successively deepens the taken-for-granted aspects of the existing organizational rationale, creating powerful, self-reinforcing loops (Kramer 2010).

The organization's name, foundational story, and initial structure solidify into "deep institutions", unwritten rules and routines defining "how we do things around here" (Fountain 2001). A powerful path dependence emerges creating stability, efficiency, and shared identity from the founder's vision, a powerful core narrative, and well-established institutions (Schein 2010). However, the same forces can become the concrete that prevents adaptation after the second or third leader cohort (Barnett et al. 2015). When the external environment changes, the organization can find itself trapped on a path to obsolescence, unable to take innovative actions that would ensure its successful resilience to surprise and adversaries (Heine and Rindfleisch 2013). Especially challenging are new actions that are seen to contradict the narrative of the organization's mission (Schreyögg and Sydow 2011).

Cyber Command's founding reflects this organizational imprinting process. Naming the unit a 'cyber' command not only tied its evolution to then contemporary notions of cyber

[1] It is important to note that the narrowness of mission was also deliberately enhanced early on by some members of Congress fearing the Command's dual hat with NSA would provide too much concentrated bureaucratic power within the government and threaten citizen privacy externally. However, the prevailing view was that the "domain" could operationally be limited to networks and code, leading to the successful formation of the Cyber Command-NSA combination. See Shanker and Sanger (2009-06-13).

as digital networks, but it also influenced the thinking and emphases of its early leader cohorts. The organization's first leader, General Keith B. Alexander, was a highly respected four-star general with deep knowledge of signals intelligence and extensive expertise in managing large intelligence organizations. He was known to be an enthusiast for information technology, although not personally trained in computer science. His assignment was logical given his position as commander of the National Security Agency (NSA), the premier technical intelligence agency in the U.S. government (Aid 2009). He publicly emphasized the Command's role in blocking and ejecting criminals and adversaries from networks, an image consistent with the then common notion of cyber as a network defense mission (Alexander 2011). Under his organizational leadership, however, the Command acted as more of an intelligence agency, defining "cyber" operations as mainly discrete, highly classified, covert, tightly targeted, one-off missions focused on computer networks (Alexander 2007; Kaplan 2016).

Military terms were then imposed on this early "cyber as intelligence operations," imprinting by a particularly influential senior leader—Cyber Command's 'godfather', GEN James "Hoss" Cartwright, a well-respected Marine Corps aviator (CSIS 2025). As Vice-Chairman of the Joint Chiefs of Staff, he deliberately and successfully protected the bureaucratic funding and nurturing of the infant Cyber Command. He also argued strongly that using recognized military language on cyber operations would ensure acceptance of Cyber Command by the other services [2]. This imprinting solidified quickly in large part because the military officers then assigned to the infant Cyber Command generally had no computer science expertise, and traditional military language was more comfortable and consistent with their preexisting professional culture. The early architects of the service-delegated cyber component commands built to serve Cyber Command understood their organizations had to be accepted by their respective parent service. They not only labeled their operations in military terms but also attempted to observe military traditions and service-specific structures in their organizational design choices. For example, the Navy's Tenth Fleet was given a Maritime Operations Center, not because cyber operations were seen to fit that organizational design, but because "the other Fleets will understand who to call" [3]. As a result, existing military language and structural preferences shaped the early Cyber Command's operational interpretations of the characteristics of cyberspace and its mission spaces.

No concept is more representative of this early mischaracterization of cyber operations than framing them as "fires", a term developed for traditional physical and thus kinetic warfare. General Cartwright insisted on applying the joint term. He was deeply concerned about the digital transformation of the US military and the bureaucratic success of the new Command (Ashford 2010). "Sergeant Smitty needs to be able to understand what he is supposed to do," he told this author in 2012. "And every soldier or Marine understands 'fires'." He argued that

[2] Personal interview 2012

[3] Personal interview 2009 Washington DC with senior officers involved in the design of the Navy's Cyber Component Command.

it would help other military units relate to Cyber Command's mission, and new arrivals at the Command would also immediately understand what to do [4].

Characterizing digital operations as "fires", however, forced them into a conceptual box long developed by the U.S. Army's artillery doctrine, evolving from terms such as "supporting fires" (1944) [5] and "protective fires" (1992) [6]. Even though the 1998 JP3-09 Doctrine for Joint Fire Support first formally defined "fires" as having lethal and nonlethal effects, the common notions behind the term were tied to planned, episodic "attacks" [7] that drop munitions upon an enemy. By 2009, the term was widely understood to imply using force to achieve discrete, physically destructive effects. It reinforced a misunderstanding of "cyber" as discrete one-off events in a digital form of artillery to be "called for" as needed in the "real" fight occurring in the physical domains. The artillery connotation fit well in the early Command's operations, emphasizing discrete intelligence operations and its external reputation as a supporting function, not a fully engaged battle domain.

The early conceptualization of cyber became well entrenched. Officers and senior enlisted embraced the imagery in no small part because officers and senior leaders assigned to Cyber Command often had limited technical understanding of cyberspace as a complex substrate. With limited expertise, they had little desire to challenge or alter the taken-for-granted early "cyber" conceptualizations [8]. During a series of research interviews of senior officers assigned to cyber positions in the U.S. military and allied nations from 2009 to 2014, interviewees often defensively introduced themselves as "not a technology expert". They overwhelmingly defined cyberspace in ground force language such as "terrain" or signals terminology such as "networks", using physical analogies. The less technical the interviewee's background was, the more their language reflected land conflict and assault imagery [9].

[4] Not every Airman, however. According to a self-described "doctrinaire" who was involved, the senior Air Force leaders did not want their operations referred to as "fires". "Published on 12 May 1998, the approved JP 3-09 [Doctrine for Joint Fire Support] was the result of nearly ten years of rigorous debate, principally between the Air Force and the Army. The USAF opposed the project from the onset, citing objections to terminology and the basic need for "fires" doctrine. The introduction of the Joint Force Fires Coordinator (JFFC) was seen by the Air Force as an Army attempt to wrest away a large part of the Joint Force Air Component Commander's (JFACC) targeting and planning responsibilities". See Vittori (1999).

[5] Wartime issue of the Army's Field Artillery Journal December 1944, where the term is used 14 times. See U.S. Field Artillery Association (1944).

[6] Joint publication of Army Field Manual 7-90 and equivalent Marine Corps MCWP 13-15.2 "Tactical Employment of Mortars", where the term is used 381 times. See Department of the Army and United States Marine Corps (2004).

[7] One senior and exceptionally technically competent Israeli officer expressed his frustration with the constant use of the term "attack" to describe cyber assaults, explaining that it was long term repeat intrusions in campaigns that mattered, but that he and others had had to redefine the term "attacks" to mean campaigns to get the Americans to properly listen (2015 Tel Aviv personal interviews)

[8] Multiple personal conversations with retired and still serving officers who were assigned to the top ranks in Cyber Command.

[9] Personal interviews conducted with U.S. officers associated with Cyber Command or a service component 2010-2014. Similar interviews were conducted in Germany, the United Kingdom, and Israel 2011-2019. I offered all my interviewees anonymity and thereby are constrained from providing any further details save to note all the interviewees had direct and personal knowledge of the cyber command or equivalent in their military force. One senior German officer insisted in 2011 that cyberspace was all networks and that all one had to do was keep the adversary from accessing the network. He captured the perspective I often encountered in these interviews in which I always asked the same set of questions, beginning with asking for a description of cyberspace which would guide their operational presumptions.

Over time, this traditional military linguistic and semantic usage was locked in, creating a conceptual and reputational cage that hampers the Command's adaptation to a technologically diverse, turbulent ecosystem. Competing and fighting in, through, or enabled by cyberspace, i.e., "cybered conflict", is inaccurately defined by episodic words such as barrages, surges, volleys, dogfights, and fires (Boutelle and Filak 1996). The reality is more campaigns than massed thrusts, marked by iterative efforts to access others' systems and using varying exploits to surveil or manipulate what those targeted systems know, calculate, or do (Williams 2016). The desired operational outcomes such as deny, degrade, disrupt, and manipulate do not map cleanly onto the traditional military language about kinetic conflict (Jasper 2017). The traditional military language struggles to value persistence, entanglement, and the ability to achieve shaping effects through manipulation and degradation rather than big-stick deterrence and destruction (Fischerkeller, Goldman, and Harknett 2022). The conceptual cage of network 'cyber' was tightened by this linguistic straitjacket.

Ironically, insisting on military terms did not smooth relations with the traditional services and their commanders. Due to cyber operations' distinctly digital nature, there are no concrete cyber "weapons". Intruding remotely into foreign adversaries' dynamic networks and variable software means "munitions" (tools) cannot be designed, produced, and left on a shelf for a geographic combatant command's future use like missiles. A cyber "weapon" needs to have a digitized target that is technically receptive and therefore accessible at the precise exploitation moment to cause the desired effects. And misfires do not just blow something up nearby; malware can also travel unexpectedly far across other connections to have quite undesired and possibly catastrophic results (Lindsay 2013).

Such tools do not readily correspond to traditional senior military leaders' preferences for ready munitions stockpiles with well-defined effects. This discrepancy heightens friction with other military commanders at the highest levels. Traditional senior military leaders often do not understand why Cyber Command does not act as a "normal" command would in the joint environment when the Command refuses to release its cyber weapons to other commanders. The contradictions contribute to the difficulties in persuading other senior combatant commanders to accept Cyber Command's control of a part of what these commanders see as 'their' air, land, sea, and hence cyber battlespace. Senior traditional military leaders in the U.S. and allies hesitate to incorporate something they do not well understand or fully command into their operational decisions (Gomez and Whyte 2022). At least one combatant commander has constructed his own internal information unit under his control and focused on his area of operations in response (Pomerleau 2023).

The imprinted "cyber" conceptual missteps have operational consequences visible in Cyber Command's force generation challenges. When other military leaders struggle to understand or properly integrate or value cyber as a field or career choice, their respective services do not manage well or maintain the existing expertise of their cyber personnel. Recruits forced to enlist through the services soon learn their leaders do not value their career field. Technically trained military personnel who are repeatedly detailed to unrelated nontechnical positions leave the military (Lonergan and Snyder 2025). Those who feel unvalued or blocked in their career choice simply leave for commercial cyber jobs (Kamarck and Theohary 2022). The conceptual 'cage' ultimately damages the Command's ability to perform its mission in real time as well as to adapt to the changing environment.

Beyond the military itself looms a third factor, a change in societal zeitgeist that reinforces the internal institutional challenges, making the conceptual cage potentially even more strategically debilitating.

CYBER'S 'MEH' FACTOR: PERCEPTION AND TALENT GAP

Early in Cyber Command's origins, talent shortages were optimistically viewed as passing circumstances that would resolve themselves as more tech-savvy individuals grew up to join the ranks [10]. Ten years later, however, GAO reported that the next generation of cyber-competent recruits still failed to join the military in numbers anywhere near what was required (GAO 2019). Today, across the country, only 74% of the cyber security jobs are filled (CyberSeek.org 2025b). The wider talent gap stems from several sources, beginning with an overarching educational deficit. The U.S. population lacks basic technical education (Sanders 2022). Employers complain that graduates of cybersecurity programs lack the hands-on skills needed for operational work (Crumpler and Lewis 2019). Half the national population is put off pursuing the field, namely, young women deterred by male dominance and midcareer and older women by the fear of being undervalued (Giboney et al. 2023). Adding to these societal structural barriers are the typical bureaucratic barriers and the limited appeal of military service (Woodruff, Kelty, and Segal 2025).

Beyond these institutional and structural barriers, however, is a problem directly related to the Command's conceptual cage. The wider societal perception of the term "cyber" evokes "cybersecurity" and images of tedious rules, checklists, and routinized work rather than innovation, creativity, or progress. Industry surveys show that cyber security is widely viewed negatively as an IT cost burden to be minimized rather than a business function involving innovation and essential investments (Lemnitzer 2021; Wertheim 2020). This perception of routinized, highly technical careers undermines the younger generation's interest in working in the "cyber" field, whether in the military or not. It is tough to market a career in "military cyber" when the desired demographic perceives the term "cyber" as less appealing than terms like AI, data science, and quantum computing. While "indifference crosses all generations", a widespread "cyber-apathy challenge [exists particularly] with young people" (Hurley 2023).

[10] See previous footnote on personal interviews, 2009-2014.

In particular, the Generation Z cohort born since 1997 relates to digital technology and cybersecurity superficially, generally lacking an innate sense of, interest in, or nascent skills with the technological underpinnings of their digital ecosystem (Debb, Schaffer, and Colson 2020). They exhibit high confidence in their digital skills but limited attention to security hygiene (Kim 2019). And they generally resist basic cybersecurity instruction and tools provided by employers, families, or educators (Panda Security 2025).

Unsurprisingly, a generation indifferent to cybersecurity in their own use of technology use is unlikely to find enlisting in the miliary for cyber-related work attractive (Donegan 2024). These perceptions suggest that the talent crisis is not merely a recruitment problem to be solved by forming a separate cyber service or mirroring special units. The U.S. military's premier digital organization's brand reflects a deeper misalignment. While potential recruits and powerful adversaries are drawn to innovative technologies like AI, quantum computing, and robotics, Cyber Command's narrow 'cyber' framing artificially separates it from publicly declaring its intention to master and fully embrace these very technologies despite their fundamental dependence on the cyber substrate.

The commercial practices prevalent across the wider society correspond to, and strongly influence, these perceptions of cyber separated from advanced technologies in the attitudes and images absorbed by developers, users, and entrepreneurs. While the advanced technologies so appealing to the wider society are completely dependent on the security of the underlying cyber substrate, their commercial design, development, and widespread deployment are generally disassociated from cyber security save in the most basic of issues such as firewalls.

Artificial intelligence, for example, relies on algorithms that require access to vast, curated datasets for training and networked computing infrastructure for execution, and these can be corrupted by malicious cyber actors (Nguyen 2025). AI has the potential to revolutionize operations by moving mind-numbing tasks from humans to tailored "AI agents", best understood as machine learning (ML) models surrounded by software encased in hardware performing tasks. Each model, code, and machine element has a multitude of potential cyber attack opportunities for adversaries (Belani 2023). Despite all this cyber embedded in artificial intelligence's life cycle, commercial ML producers who provide models and services embedded in military capabilities have been slow to put securing their models against traditional cyber threats at the forefront of their design and development (Puthal and Mohanty 2021). Those who 'do' AI do not see themselves as 'doing' cyber (Mink et al. 2023). Accordingly, the users and entrepreneurs also rarely connect the two. Even the cyber security community itself has proven slow to integrate AI developer skills into their command of cyber, reinforcing the separation. Only ten percent of commercial cyber security job openings today specifically mention AI skills as a requirement for a cyber job (CyberSeek.org 2025a).

Across the wider society, the enthusiastic embrace of AI without deliberate integration of cybersecurity is mirrored across the spectrum of cyber-dependent advanced technologies and inevitably reinforces the perception of cyber as boring and unrelated to the exciting newer technologies. Quantum computing, for example, despite its hype as a revolutionary technology, remains intrinsically dependent on insecure digital infrastructures (Volya et al. 2023; Smith III 2020). Similarly, autonomous systems, from drones to ground vehicles, also entirely depend on software and networked hardware systems, as do nanoscience, space technology, and hypersonic capabilities (Lippi et al. 2025). This persistent commercial, cultural, and professional divide between AI and cybersecurity reverberates institutionally within defense structures as well (Tangredi and Galdorisi 2021). Without deliberate efforts to organizationally and operationally integrate cyber with its technological offspring, cyber weaknesses will be embedded in the next generation of AI-enabled military and civilian systems to dangerous consequences (Sangwan, Badr, and Srinivasan 2023).

BREAK THE CAGE TO REINVENT FOR THE FUTURE

There is no escaping cyber in the technological hostility that marks Great Systems Conflict. When military services separately design and develop systems using commercial firmware and components without integrated cyber expertise from design forward, the result is a proliferation of digitally enabled systems built atop unexamined vulnerabilities, gaps, and access points open to exploitation by adversaries such as China and Russia. Cyber Command’s current organizational structure reinforces the early conceptual mischaracterizations of "cyber" as one of many separable "domains" rather than the foundational substrate of an expanding digital ecosystem from which advanced technologies such as artificial intelligence, quantum computing, robotics, and autonomous systems emerge. This “domain” framing of cyber as coequal with other warfighting domains encourages other service components and defense agencies to separately develop emerging digital technologies without involving Cyber Command’s operational expertise. The resulting fragmentation means multiple organizations are each pursuing narrow technological goals without strategic coordination, broad-spectrum technical mastery, or robust mechanisms to avoid systemic vulnerabilities propagating across exceptionally complex, interconnected systems.

The current reform debate offers a fleeting chance to simultaneously address all these challenges, from the cage to expertise fragmentation, through fundamental reinvention rather than incremental adjustment. A reinvented Cyber Command can serve as the pan-technology nexus for expertise, training, cross-spectrum digitized operations research and testing, and active deployment to ensure these interdependent capabilities evolve within a unified, resilient digital ecosystem. Only such organizational and conceptual integration can provide the strategic coherence necessary for effective competition, deterrence, and warfighting in the digital battlespace. The strategic challenge today is redirecting the path-dependent organization of Cyber Command without dampening its successes. If the current debate remains mistakenly pitched as two separate choices, reforming Cyber Command or adding a separate cyber service, then the solutions will be partial at best.

One begins where one can. In this case, a first step in creating the future-ready military is to remove a debilitating attachment to a dated and narrow concept of “cyber” as a “domain” and its offspring as something beyond Cyber Command’s remit. The digitized conflicts to come are not military maneuvers that any general officer with any background can manage. Without reducing these linguistic, conceptual, and organizational barriers, incremental changes such as adopting a “SOCOM-like” model that keeps force generation within largely disinterested traditional services would not necessarily solve known weaknesses.

It is time to reinvent the Command, not as a better “Cyber” Command, but as a new entity, perhaps the U.S. Digital Vanguard Command (DIGICOM) or the U.S. Cyber, Robotics, and Information Systems Command (CRISCOM). Cyber can remain in the name, but never again by itself. While details in implementing this proposal will need research beyond the scope of this article, signaling of a new era could begin more quickly. The new name must signal a comprehensive, future-oriented pan-information technology mission that attracts recruits directly. Its structure must adjust to welcome them into a force generation unit subordinate to the former Cyber Command and able to recruit, train, and supply talent to itself and other services. The reinvented organization must have the mandate, structure, and authorities to manage the entire lifecycle of its force while proving better able to argue for funding to nurture the military’s mastery of cyber and its offspring across the technological ecosystem. The current debate about an impending overhaul of Cyber Command is the perfect opportunity to break from the ‘cyber’ cage, and adapt the U.S. military to deter, meet, and defeat the comprehensive and inundating assaults that mark the emerging Great Systems Conflict era.

ABOUT THE AUTHOR

Dr. Chris C. Demchak is the Grace Hopper Chair of Cyber Security and Senior Cyber Scholar in the Cyber Innovation Policy Institute at the U.S. Naval War College. She holds degrees in engineering, economics, and comparative complex organization systems / political science. In publications and current research on conflict, surprise, and resilience in a modern digitized globe penetrated by a global, insecure, complex, conflict-prone cyber “substrate,” Demchak takes a socio-technical-economic systems approach comparatively with emerging technologies, adversaries’ cyber/AI/ML campaigns, virtual wargaming for strategic/organizational learning, and global/national/enterprise resilience against complex systems surprise. Articles of note include “China’s Maxim (BGP Hijacking, 2018 and update 2021)”, “Four Horsemen of AI” (2019), “ ‘Sea-hacking’ Sun Tsu: Deception in Global AI/Cybered Conflict” (2021), “Achieving Systemic Resilience in a Great Systems Conflict Era” (2022), “Cybered Conflict, Hybrid War, Informatizaton Wars" (2020) and *Cyber Warfare and Navies* (2025 co-edit). Works in-progress of note include “How to Run and Defend a Digital Democracy” and “Great Systems Conflict: Cyber Westphalia, Warfare, and Operational Collective Resilience”.

REFERENCES

Aid, Matthew M. 2009. *The secret sentry: The untold history of the National Security Agency.* Bloomsbury Publishing USA.

Alexander, Keith B. 2007. “Warfighting in cyberspace.” *Joint Force Quarterly* 3rd Quarter.

Alexander, Keith B. 2011. “Building a new command in cyberspace.” *Strategic Studies Quarterly* 5 (2): 3–12.

Arquilla, John, and David Ronfeldt. 1993. “Cyberwar is coming!” *Comparative Strategy* 12 (2): 141–165.

Arulmurugan, S., and Abdul Mohammed Ali Jinnah. 2024. “The Cyberpunk Elements in William Gibson’s Neuromancer.” *Journal of Language and Linguistic Studies* 17 (3). https://www.jlls.org/index.php/jlls/article/viewFile/5562/1980.

Ashford, R. Brian. 2010. “The Missionary Work of Evolving the Digital MAGTF.” Master’s thesis, USMC Command and Staff College, Marine Corps University. https://apps.dtic.mil/sti/tr/pdf/ADA602215.pdf.

Barnett, Jon, Louisa S. Evans, Catherine Gross, Anthony S. Kiem, Richard T. Kingsford, Jean P. Palutikof, Catherine M. Pickering, and Scott G. Smithers. 2015. “From barriers to limits to climate change adaptation: path dependency and the speed of change.” *Ecology and society* 20 (3). https://www.jstor.org/stable/26270227.

Belani, Gaurav. 2023. “AI for Cybersecurity and Cybercrime: How Artificial Intelligence Is Battling Itself.” *IEEE Computer* (September 6, 2023). https://www.computer.org/publications/tech-news/trends/ai-fighting-ai.

Boutelle, Steven W., and Ronald Filak. 1996. “AFATDS: The Fire Support Window to the 21st Century.” *Joint Force Quarterly* 11:16–21.

Branch, Jordan. 2021. “What’s in a Name? Metaphors and Cybersecurity.” *International Organization* 75 (1): 39–70. https://www.cambridge.org/core/journals/international-organization/article/abs/whats-in-a-name-metaphors-and-cybersecurity/563998100A2FAF1E5DFDB5C52EC68569.

Cebrowski, Arthur K., and John J. Garstka. 1998. “Network-Centric Warfare: Its Origin and Future,” 124:28–35. 1. https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future.

Couillard, Jeffrey. 2024. “Beyond USCYBERCOM: The Need to Establish a Dedicated US Cyber Military Force.” *The Cyber Defense Review* 9 (1). https://www.jstor.org/stable/48770664.

Crumpler, William, and James A. Lewis. 2019. *Cybersecurity Workforce Gap.* Center for Strategic and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf.

CSIS (Center for Strategic and International Studies). 2025. *James E. Cartwright, Distinguished Senior Adviser (Non-resident), Office of the President.* https://www.csis.org/people/james-e-cartwright.

CyberSeek.org. 2025a. *AI + Security.* CyberSeek, October. https://www.cyberseek.org/index.html.

CyberSeek.org. 2025b. *CyberSeek expands cybersecurity workforce data coverage and enhances user experience,* June 2, 2025. https://www.cyberseek.org/docs/06-02-2025_CyberSeek_June_2025.pdf.

Debb, Scott M., Daniel R. Schaffer, and Darlene G. Colson. 2020. “A reverse digital divide: comparing information security behaviors of generation Y and generation Z adults.” *International journal of cybersecurity intelligence & cybercrime* 3 (1): 42–55. https://doi.org/10.52306/03010420GXUV5876.

Demchak, Chris. 2021. “Achieving Systemic Resilience in a Great Systems Conflict Era.” *The Cyber Defense Review* 6 (2): 51–70. https://www.jstor.org/stable/27021376.

Department of the Army and United States Marine Corps. 2004. *Tactical Employment of Mortars.* Department of Defense. https://www.trngcmd.marines.mil/Portals/207/Docs/TBS/MCWP%203-15.2%20Tactical%20Employment%20of%20Motars.pdf.

Donegan, John. 2024. *IT Security - Gen Z’s cybersecurity risks: Insights from recent survey,* July 19, 2024. https://insights.manageengine.com/it-security/genz-cybersecurity-risks-survey/#Other_key_survey_findings.

Doshi, Rush. 2021. *The Long Game: China’s Grand Strategy to Displace American Order.* Oxford University Press.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber persistence theory: Redefining national security in cyberspace.* Oxford University Press.

Fountain, J. E. 2001. *Building the Virtual State: Information Technology and Institutional Change.* Brookings Institution Press.

GAO (General Accounting Office). 2019. *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force.* https://www.gao.gov/products/gao-19-362.

Giboney, Justin Scott, Bonnie Brinton Anderson, Geoffrey A. Wright, Shayna Oh, Quincy Taylor, Megan Warren, and Kylie Johnson. 2023. “Barriers to a cybersecurity career: Analysis across career stage and gender.” *Computers & Security* 132:103316.

Gibson, William. 1984. *Neuromancer.* Ace Books.

Gomez, Miguel Alberto, and Christopher Whyte. 2022. “Cyber uncertainties: Observations from cross-national war games.” In *Cyber security politics,* 111–127. Routledge.

Gosain, Sanjay. 2004. “Enterprise information systems as objects and carriers of institutional forces: the new iron cage?” *Journal of the Association for Information Systems* 5, no. 4 (April): 151–182. https://doi.org/10.17705/1jais.00049.

Grossman, Robert L., and Emily O. Goldman. 2024. “The Importance of Analytic Superiority in a World of Big Data and AI.” *The Cyber Defense Review* 9 (2): 29–48. https://www.jstor.org/stable/48784774.

Hardison, Chaitra M., Leslie A. Payne, John A. Hamm, Angela Clague, Jacqueline Torres, David Schulker, and John S. Crown. 2019. *Attracting, recruiting, and retaining successful cyberspace operations officers: Cyber workforce interview findings.* RAND. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2600/RR2618/RAND_RR2618.pdf.

Harknett, Richard J., and Max Smeets. 2022. “Cyber Campaigns and Strategic Outcomes.” *Journal of Strategic Studies* 45 (4): 534–567. https://doi.org/10.1080/01402390.2020.1732354.

Heine, Klaus, and Heike Rindfleisch. 2013. “Organizational decline: A synthesis of insights from organizational ecology, path dependence and the resource-based view.” *Journal of Organizational Change Management* 26 (1): 8–28. https://doi.org/10.2139/ssrn.2178991.

Hurley, Billy. 2023. *How to get young people (and everybody else) to care about cybersecurity - It turns out Gen Z ate but left some online crumbs.* ITBrew, November 7, 2023. https://www.itbrew.com/stories/2023/11/07/how-to-get-young-people-and-everybody-else-to-care-about-cybersecurity.

Jasper, Scott. 2017. *Strategic cyber deterrence: The active cyber defense option.* Bloomsbury Publishing PLC.

Jensen, Benjamin M., Christopher Whyte, and Scott Cuomo. 2020. “Algorithms at war: the promise, peril, and limits of artificial intelligence.” *International Studies Review* 22 (3): 526–550. https://doi.org/10.1093/isr/viz025.

Joint Chiefs of Staff. 2000. *Joint Vision 2020: America’s Military Preparing for Tomorrow (JV2020).* Edited by Department of Defense. https://apps.dtic.mil/sti/tr/pdf/ADA377926.pdf.

Kamarck, Kristy N., and Catherine A. Theohary. 2022. *FY2023 NDAA: Cyber Personnel Policies.* Congressional Research Service (CRS), U.S. Congress, October 4, 2022. https://apps.dtic.mil/sti/trecms/pdf/AD1181856.pdf.

Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War.* New York: Simon & Schuster.

Kim, Min Ji. 2019. *A Gen Z’s perspective on cybersecurity.* Delinea Blog. https://delinea.com/blog/genz-perspective-cybersecurity.

Kobie, Nicole. 2017. *Is it time to drop "cyber" in security? - The prefix sounds old-fashioned and out of date.* ITPro, May 31, 2017.

Kramer, Michael W. 2010. *Organizational socialization: Joining and leaving organizations.* Vol. 6. Polity.

Lemnitzer, Jan Martin. 2021. “Why cybersecurity insurance should be regulated and compulsory.” *Journal of Cyber Policy* 6 (2): 118–136. https://doi.org/10.1080/23738871.2021.1880609.

Lewis, James Andrew. 2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Center for Strategic and International Studies. Washington, DC, November. https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats.

Lilli, Eugenio. 2020. “President Obama and US cyber security policy.” *Journal of Cyber Policy* 5 (2): 265–284. https://doi.org/10.1080/23738871.2020.1778759.

Lind, Jennifer. 2024. “Back to Bipolarity: How China’s Rise Transformed the Balance of Power.” *International Security* 49 (2): 7–55. https://doi.org/10.1162/isec_a_00494.

Lindsay, Jon R. 2013. “Stuxnet and the Limits of Cyber Warfare.” *Security Studies* 22 (3): 365–404. https://doi.org/10.1080/09636412.2013.816122.

Lippi, Giuseppe, Mahmoud Aljawarneh, Qais Al-Na’amneh, Rahaf Hazaymih, and Lachhman Das Dhomeja. 2025. “Security and privacy challenges and solutions in autonomous driving systems: A comprehensive review.” *Journal of Cyber Security and Risk Auditing* 2025 (3): 23–41. https://doi.org/10.63180/jcsra.thestap.2025.3.3.

Lonergan, Erica D., and Jack Snyder. 2025. “Cultural Change in Military Organizations: Hackers and Warriors in the US Army.” *Texas National Security Review* 8 (3): 74–95. https://doi.org/10.26153/tsw/60740.

Mastro, Oriana Skylar. 2024. *Upstart: How China became a great power.* Oxford University Press.

Mearsheimer, John J. 2003. *The tragedy of great power politics (Updated edition).* WW Norton & Company.

Mink, Jaron, Harjot Kaur, Juliane Schmüser, Sascha Fahl, and Yasemin Acar. 2023. "“Security is not my field, I'm a stats guy”: A Qualitative Root Cause Analysis of Barriers to Adversarial Machine Learning Defenses in Industry." In *32nd USENIX Security Symposium.* https://www.usenix.org/conference/usenixsecurity23/presentation/mink.

Nguyen, Vinh. 2025. *Securing Intelligence: Why AI Security Will Define the Future of Trust.* Council on Foreign Relations Digital and Cyberspace Policy Program, November 6, 2025. https://www.cfr.org/article/securing-intelligence-why-ai-security-will-define-future-trust.

Panda Security. 2025. "Gen Z facing increased cybersecurity threats," March 7, 2025. https://www.pandasecurity.com/en/mediacenter/gen-z-facing-increased-cybersecurity-threats/.

Pattnaik, Nandita, Shujun Li, and Jason R.C. Nurse. 2023. "Perspectives of non-expert users on cyber security and privacy: An analysis of online discussions on twitter." *Computers & Security* (February): 103008. https://doi.org/10.1016/j.cose.2022.103008.

Pomerleau, Mark. 2023. *Navy's Pacific information warfare command coordinating vast capability across region.* Defense Scoop, July 19, 2023. https://defensescoop.com/2023/07/19/navys-pacific-information-warfare-command-coordinating-vast-capability-across-region/.

Puthal, Deepak, and Saraju P. Mohanty. 2021. "Cybersecurity issues in AI." *IEEE Consumer Electronics Magazine* 10 (4): 33–35. https://doi.org/10.1109/MCE.2021.3066828.

Rattray, Gregory J. 2001. *Strategic warfare in cyberspace.* MIT press.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Sanders, Ronald. 2022. "The War for Cyber Talent: Can the US Win It?" In *The Great Power Competition, Volume 3: Cyberspace: The Fifth Domain,* edited by Ronald P. Sanders Adib Farhadi and Anthony Masys, 293–317. Cham: Springer International Publishing.

Sangwan, Raghvinder S., Youakim Badr, and Satish M. Srinivasan. 2023. "Cybersecurity for AI systems: A survey." *Journal of Cybersecurity and Privacy* 3 (2): 166–190. https://doi.org/10.3390/jcp3020010.

Santora, Joseph C., and James C. Sarros. 2008. "Founders, leaders, and organizational life cycles: the choice is easy–learn or fail!" *Development and Learning in Organizations: An International Journal* 22 (3): 12–15. https://doi.org/10.1108/14777280810861767.

Schein, Edgar H. 2010. *Organizational culture and leadership.* Vol. 2. John Wiley & Sons.

Schreyögg, Georg, and Jörg Sydow. 2011. "Organizational path dependence: A process view." *Organization studies* 32 (3): 321–335. https://doi.org/10.1177/0170840610397481.

Shanker, Thom, and David E. Sanger. 2009-06-13. "Privacy May Be a Victim in Cyberdefense Plan." *The New York Times,* https://www.nytimes.com/2009/06/13/us/politics/13cyber.html.

Shirk, Susan L. 2023. *Overreach: How China derailed its peaceful rise.* Oxford University Press.

Slayton, Rebecca. 2020. "What is a cyber warrior? The emergence of US military cyber expertise, 1967–2018." *Texas National Security Review* Winter:61–96. https://doi.org/10.26153/tsw/11705.

Smith III, Frank L. 2020. "Quantum technology hype and national security." *PRIO* 51 (5). https://journals.sagepub.com/doi/10.1177/0967010620904922.

Tangredi, Sam J., and George Galdorisi. 2021. *AI at war: How big data, artificial intelligence, and machine learning are changing naval warfare.* Naval Institute Press.

Thompson, J. D. 1967. *Organizations in action.* New York: McGraw-Hill.

U.S. Field Artillery Association. 1944. *The Field Artillery Journal.* December 1944 issue, 12. https://tradocfcoeccafcoepfwprod.blob.core.usgovcloudapi.net/fires-bulletin-archive/1944/DEC_1944/DEC_1944_FULL_EDITION.pdf.

Vittori, Jay M. 1999. "Fighting Fires with Fire-An Airman's Perspective on the Development of Joint Publication 3-09, Doctrine for Joint Fire Support." AU/AWC/236/1999-004. Master's thesis, Air War College, Air University. https://apps.dtic.mil/sti/pdfs/ADA395508.pdf.

Volya, Daniel, Tao Zhang, Nashmin Alam, Mark Tehranipoor, and Prabhat Mishra. 2023. "Towards secure classical-quantum systems." In *2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST).* https://www.cise.ufl.edu/research/cad/Publications/host23.pdf.

Warner, Michael. 2012. "Cybersecurity: A pre-history." *Intelligence and National Security* 27 (5): 781–799. https://doi.org/10.1080/02684527.2012.708530.

Welch, Carley. 2024. *A year into its cyber workforce initiative, DoD faces personnel shortages, bureaucratic hurdles.* Breaking Defense, August 29, 2024. https://breakingdefense.com/2024/08/a-year-into-its-cyber-workforce-initiative-dod-faces-personnel-shortages-bureaucratic-hurdles/.

Wertheim, Steven. 2020. “The Willingness Not to Believe.” *CPA Journal* (January 7, 2020). https://www.cpajournal.com/2020/01/07/the-willingness-not-to-believe/.

Wiener, Norbert. 1948. *Cybernetics: Or Control and Communication in the Animal and the Machine.* MIT Press.

Williams, Phil. 2016. “Crisis Managment in Cyberspace and in a "Cybered" World.” In *Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition,* edited by Phil Williams, 571–601. Carlisle, PA: Strategic Studies Institute, US Army War College.

Woodruff, Todd, Ryan Kelty, and David R. Segal. 2025. “Revisiting propensity to serve and motivations to enlist: Insights and implications for contemporary military recruitment challenges and research.” *Armed Forces & Society* 51 (2): 482–491. https://doi.org/10.1177/0095327X241259465.

Received 13 August 2025; Revised 12 November 2025; Accepted 19 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 179-190
https://doi.org/10.55682/cdr/e6rn-adte

PROFESSIONAL COMMENTARY

Bring Cyber to the Tactical Edge: The Case for Decommissioning USCYBERCOM

Sam J. Tangredi*

U.S. Naval War College, Newport, RI, USA

Public debates over the creation of a separate Cyber Force service, along with directives to expand the role of U.S. Cyber Command (USCYBERCOM), raise an opportunity to examine the control of cyber operations in a high-intensity war between technological near-peers. Fighting such a war effectively would require high-speed decisions within a contested electromagnetic environment. Sensors, satellites, networks, and long-haul communications would be continuously under attack. In addition to electronic warfare, the use of anti-satellite weapons should be expected. Data transmission between forward operational units—particularly strike groups at sea—and the rear area headquarters of the Combatant Commands (COCOMs) would be, at best, narrowband and intermittent. So would cyber support operations emanating from Ft. Meade, with USCYBERCOM-controlled operations confined to strategic-level attacks (and defense). Tactical units may be left to their own devices when integrating kinetic and non-kinetic operations against enemy forces. These possibilities argue for moving cyber warfare capabilities out to the tactical edge—to strike groups, Army divisions, Marine expeditionary units (MEU), and expeditionary air forces. There, they can be directly applied to engaging enemy combat networks and, especially, operational technology (OT)—perhaps the most vulnerable and least protected cyber-enabled systems. The article examines whether the current USCYBERCOM structure as an independent COCOM should be 'decommissioned' and its components 'recommissioned' under the command of the regional COCOMs, with the Cyber National Mission Force under either U.S. Strategic Command (USSTRATCOM) or U.S. Special Operations Command (USSOCOM).

Keywords: U.S. Cyber Command, USCYBERCOM, cyberspace, tactical, decommission, non-kinetic, warfighting

* Corresponding author: sam.tangredi@usnwc.edu

***Disclaimer:** The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

INTRODUCTION

Public debates over the creation of a separate Cyber Force service (Couillard 2024), along with directives to expand the role of USCYBERCOM (Matishak 2024), raise an opportunity to examine the control of cyber operations in a high-intensity war between technological near-peers (Matishak 2025). Fighting such a war effectively would require rapid decision-making within a contested electromagnetic environment. Sensors, satellites, networks, and long-haul communications would be continuously under attack. In addition to electromagnetic warfare, the use of anti-satellite weapons should be expected (Tangredi 2013). The same goes for considerable use of artificial intelligence (Swift and Siordia 2021).

Under this scenario, data transmission between forward operational units—particularly strike groups at sea—and the rear-area headquarters of the Combatant Commands (COCOMs) would, at best, be narrow-band and intermittent. So would cyber support operations emanating from Ft. Meade. In fact, cyber operators embedded within the geographic (regional) COCOMs may have little or no connectivity with USCYBERCOM headquarters, as Ft. Meade itself is an obvious target for enemy attack (whether by cyber attack on headquarters or critical infrastructure, special operations, or kinetic strikes). What is happening within the theater may be completely opaque to USCYBERCOM, thereby denying it from having any effect on tactical events. Even if USCYBERCOM headquarters remains unscathed, its operations might be confined to strategic-level attacks (and defense).

These possibilities support an argument for moving cyber warfare capabilities to the tactical edge (NIST 2015), to strike groups, Army divisions, Marine expeditionary units (MEU), and expeditionary air forces. Here, they can be directly applied to engaging enemy combat networks and, especially, operational technology (OT)—perhaps the most vulnerable and least protected cyber-enabled systems (Hilger 2025). If, indeed, the Pentagon is laser-focused on enhancing warfighting capabilities, then moving as much kinetic and non-kinetic capacity as possible out to the tactical edge would seem eminently logical. At the very least, granting the regional combatant commanders authority over all non-kinetic effects—including cyber—in their theaters of responsibility would be a step towards operationalizing the concepts of expanded maneuver (Walsh and Huber 2023) and distributed operations (O'Rourke 2025).

A potential impediment in moving cyber to the tactical edge is the current intensely consolidated structure of USCYBERCOM. The same goes for most plans to enhance this functional COCOM. Indeed, its most ardent supporters have called for even more consolidation in the form of a separate service—a Cyber Force—to control all Title 10 responsibilities for manning, training, and equipping cyber forces, as well as exercising operational control over all cyber warfare capabilities (Lonergan and Montgomery 2024).

Bringing cyber warfare capabilities to the tactical edge would seem to require movement in the opposite direction. It is time to examine the option of decommissioning USCYBERCOM and distributing its components. The term ‘decommissioning’ is chosen deliberately. The components—such as the individual Cyber Mission Forces—would not be disestablished. They would be redistributed as close to the tactical edge as possible. Strategic-level operations—such as those conducted by the Cyber National Mission Force (CNMF)—could revert to a sub-unified command under either U.S. Strategic Command (USSTRATCOM) or U.S. Special Operations Command (USSOCOM) (USCYBERCOM 2023, 2024). Another alternative would be to embed the offensive ‘strategic’ cyber missions within the National Security Agency (NSA), despite tensions between intelligence and operations (Lawson 2022; Warner 2020, 25).

In the end, tactical cyber operations would ultimately be under the command of regional Combatant Commanders, as are all other kinetic and non-kinetic warfighting capabilities of the joint forces in theater.

CONGRESSIONAL COUNTER-CURRENTS

Impediments to bringing cyber to the tactical edge within the current command structure are well known. At the same time, the Secretary of War has indicated support for increasing USCYBERCOM’s authority—originally referred to as CYBERCOM 2.0 (Lonergan and Montgomery 2024, 13)—but cross-currents have developed in Congress. The core issue is the relationship of USCYBERCOM to the regional COCOMs in responding to high-end conflict.

The Chairman of the House Armed Services Subcommittee on Cyber, Innovation Technologies, and Information Systems, Representative Don Bacon (R-Neb), stated in July 2025: “Since becoming Chairman of the Subcommittee, I’ve grown increasingly concerned that we are not correctly organized for the cyber fight we find ourselves in today, let alone a more complex and consequential future fight. Our Cyber Command does great working national threats, but I want to ensure our Cyber team is postured right for a potential fight with China over Taiwan” (Pomerleau 2025a). As a result of such concerns, “House and Senate versions of [FY26] NDAA legislation are asking for assessments that could alter how cyber capabilities are employed within geographic combatant commands” (Pomerleau 2025a).

One driver of these actions is the perspectives of the regional COMCOMs. USCYBERCOM could conduct cyber operations within their geographic theater without their concurrence; moreover, regional COCOMs do not have the capability or authority from the Secretary of War to conduct cyber operations directly in support of unfolding tactical actions. As noted in open sources, “unlike the other domains of warfare, there still is no cyber component at the geographic combatant commands” (Pomerleau 2025a). As a media-interviewed former official postulated, “I don’t think COCOM commanders are happy with that. I think they want the control” (Pomerleau 2025a). Another former official suggests, “some of the geographic combatant commands are probably saying, ’I just don’t have the authority’” (Pomerleau 2025a). To this is added the concern that USCYBERCOM headquarters might conduct cyber operations that inadvertently interfere with the kinetic/non-kinetic combined operational planning and execution as contained in the regional COCOM contingency plans—a cyber blue-on-blue.

Granted, there are USCYBERCOM-created Cyber Operations-Integrated Planning Elements (CO-IPEs) deployed to the headquarters of the regional COCOMs. However, these planning cells are designed to "assist in planning and understanding how to employ cyber operations," not conduct operations under the command of the Combatant Commander (Pomerleau 2025a). CO-IPEs are ultimately under the control of USCYBERCOM. They essentially act as liaisons between USCYBERCOM and the regional COCOMs (Pomerleau 2017). How well they do so remains an open question. Reportedly, there have been complaints that the CO-IPEs "haven't matured effectively to provide all the necessary answers and planning requests" (Pomerleau 2025a).

Interestingly, operational support (which may or may not be an accurate term) for the geographic regional and functional COCOMs is assigned to cyber units composed of commands and personnel from individual services. These include Joint Force Headquarters-Cyber Army, which is responsible for supporting Central Command, Africa Command, and Northern Command. Joint Force Headquarters-Cyber Navy is responsible for Indo-Pacific Command, Southern Command, and U.S. Forces Korea. Joint Force Headquarters-Cyber Air Force is responsible for European Command, Space Command, and Transportation Command. Joint Headquarters-Cyber Marine Corps is responsible for USSOCOM. There is also a Joint Force Headquarters assigned to the Department's information network (JFHQ-DODIN) (Pederson et al. 2022; DCDC 2025).

The Joint Force Headquarters-Cyber are under the operational command of USCYBERCOM. Administratively, they are under the direction of the Services. Their commanders are often multiple-hatted and charged with carrying out Service and Joint functions. For example, the commander of Joint Force Headquarters-Cyber Navy is quadruple-hatted as commander of U.S. Fleet Cyber Command, U.S. Tenth Fleet, Navy Space Command, and Navy Cryptologic Office. What these convoluted relationships between the Joint Forces Headquarters-Cyber and the regional COCOMs mean in practice is difficult to determine through open literature. However, it seems clear that the Joint Force Headquarters are considered "a component command of USCYBERCOM," not of the regional COCOM (Pederson et al. 2022).

Consider the possibility of high-end warfighting with China, during which long-haul communications and connectivity are intermittent. Will the consolidation of cyber warfighting capabilities under a single, independent functional COCOM remain effective? Or would dispersion of these capabilities to the tactical edge be an imperative?

USCYBERCOM has enjoyed support in Congress for at least a decade. Recent Congressional concerns over how cyber capabilities are employed within geographic COCOMs appear to suggest that decision-makers want it both ways: a USCYBERCOM responsible and accountable for all things military cyber, and dispersed cyber capabilities under the authority of individual regional COCOMs.

CONTINUING DEBATES OVER STRATEGIC POSTURE

Part of the debate over USCYBERCOM's role and authority is left over from the recent past when cyber operations were considered strategic-level activities to be tightly controlled by national command authorities. When the predecessor to USCYBERCOM was created circa 2005 as the Joint Functional Component Command for Network Warfare, it was a sub-unified command under (and part of) USSTRATCOM. At the time, cyber warfare capabilities were seen as strategic deterrents, analogous to strategic nuclear weapons (Warner 2020, 19). Indeed, some commentators still argue that "a major cyber attack could be just as damaging" as a nuclear attack (Straub 2019).

However, the elevation of USCYBERCOM to an independent COCOM, co-equal with the others, seemed a reasonable development as it became increasingly apparent that—primarily due to the anonymity of cyberspace—cyber attacks on businesses, individuals, infrastructure, and militaries were difficult to deter (Hollis 2010). The 'peacetime' cyber war—fought on various levels from criminal gangs to nation-states—was undeniable, and the creation of a COCOM to fight a continuing battle in the cyber domain seemed essential. The declaration of cyberspace as a separate warfighting domain also helped justify an independent USCYBERCOM (U.S., Chairman of the Joint Chiefs of Staff 2006). Nevertheless, cyber operations still appeared 'strategic' because they were conceived as primarily being conducted in cyberspace itself, rather than as a combined arm in tactical operations. At best, cyber operations were conceived as representing a strategic concept with (some) tactical effects that could be fought independently.

The difficulty of deterring cyber warfare led to the development of the concepts of "defend forward" and "persistent engagement"—arguably derivative of the long-standing naval concept of "forward presence" (Tangredi 2025). Goldman identifies this change as a "paradigm shift" in which the concept of cyber capabilities as a strategic capability acting as a deterrent and—when necessary—a "response force" to a "persistence force" that could provide continuing defense (and potentially offensive actions) in the ongoing 'peacetime' cyber war (Goldman 2020; Fischerkeller, Goldman, and Harknett 2022). Defend forward and persistent engagement subsequently became operational doctrine for USCYBERCOM as codified in the 2018 Department of Defense Cyber Strategy (USCYBERCOM 2022).

Nevertheless, a justification for consolidating all cyber authorities within USCYBERCOM is that it is both a strategic-level and a tactical-level command, with offensive cyber operations serving as both a strategic weapon capable of inflicting mass casualties and a precisely targeted weapon useful against a specific enemy unit. This parallels the earlier observation that Congress would like it both ways as concerns USCYBERCOM's authorities.

However, one could take the analogy further. During the Cold War, USSTRATCOM was in control of all strategic nuclear weapons. But tactical nuclear weapons (later referred to as non-strategic weapons) remained in the inventory of the regional Commanders-in-Chief (CINCs)—the predecessors of today's Combatant Commanders. These tactical weapons were deployed by forward-operating units (such as nuclear anti-submarine rockets aboard U.S. Navy warships). Both categories of nuclear weapons required Presidential authorization for use, but control over strategic and tactical weapons was split.

Arguing by analogy may have its critics. However, it is fair to ask if a similar strategic and tactical division between CINCs should also apply to cyber.

CYBERED WARFARE VERSUS CYBER WARFARE

Perhaps different terminology can facilitate a conceptual shift from the perception of independent warfighting conducted primarily in cyberspace to cyber operations as a "multi-domain" or "all domain" combined arm. ("Multi-domain" is a U.S. Army term; "all domain" is a U.S. Navy term. Essentially, they mean the same. The use of "all domain" actually preceded use of "multi-domain;" however, it was not as widely publicized.) In many writings, Demchak has used the term 'cybered' rather than 'cyber' to describe future wars in which cyber operations would be a 'normal' aspect of combined arms warfighting (Demchak 2010). This use of "cybered" is gradually spreading (Cyber Defense Review Winter 2022).

Instead of referring to cyber war, which can be viewed as a war conducted exclusively in cyberspace, cybered war implies that all modern warfare includes a cyber element—that all digital weapons represent the inclusion of a greater cyberspace beyond the networks that are connected to the internet. Such weapons are controlled by (hopefully) isolated data networks constructed in a manner similar to internet communications. The kill chains in which they are embedded have information, electromagnetic warfare, and cyber components. The OT that they employ could be vulnerable to cyber attack. Separations between cyber and other forms of electronic warfare may be very thin.

The use of the term "cybered" brings awareness that digitalization and the resulting cyber vulnerabilities exist across all levels of warfare and most combat engagements. The ongoing 'peacetime' conflict in cyberspace has a counterpart in other 'campaigning' activities. The use of "cybered" war implies that cyber warfare should be both 'mainstreamed' as a 'normal' aspect of war and that cyber capabilities should be distributed among operational units (as well as COCOM headquarters). One can also argue that it implies that cyberspace should not be considered a separate (albeit human-made) domain (Libicki 2012; Kreuzer 2021).

ARGUMENTS FOR AND AGAINST USCYBERCOM

Cybered war does not mean that there is not a valid argument for retaining an independently-operating USCYBERCOM for ‘peacetime’ (pre-hostilities) cyber conflict and in wars against technologically-inferior opponents, such as the Taliban and various sub-state threats. Ongoing ‘peacetime’ cyber conflict is global in nature and therefore not within the areas of interest of any particular geographic COCOM. ‘Peacetime’ preparations also need an organizer and champion. Obviously, USCYBERCOM, in conjunction with the NSA, plays a critical role in defending the U.S. military’s infrastructure—and thereby a significant part of national infrastructure—and in developing and applying tactics and techniques for long-term penetration of enemy networks (and conducting pre-war and intra-war espionage).

To some extent, this responsibility spills over to the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA). However, CISA is presumably not engaged in offensive cyber operations. Moreover, because so many assets and personnel have been concentrated in the armed forces for so long, a military ‘champion’ is often necessary for effective whole-of-government action (Democracy & Human Rights Working Group 2021; Oakley 2019). However, that does not necessarily require an independent COCOM; it could instead be a command within USSTRATCOM or USSOCOM.

Another argument is that an independent USCYBERCOM—indeed, the creation of a separate U.S. Cyber Force Service—is necessary for providing the level of training necessary for effective cyber warfare operators, as well as improving retention (Lonergan and Montgomery 2024, 14–22). Although the individual Services provide primary cyber training, this level of training has never been seen as sufficient to develop the level of cyber expertise to conduct offensive cyber operations, such as defend forward and persistent engagement. As an open source describes: “USCYBERCOM, launched over a decade ago, has struggled to grow its cyber workforce necessary to counter ever-growing cyber threats. The command has historically relied on the military services to provide digital personnel, which has led to readiness issues since the Services run their own recruitment and training systems for their cyber operations, and digital warriors tend to have inconsistent knowledge and experience when they are sent to USCYBERCOM” (Obis 2024).

Yet, there are alternatives to an independent COCOM (or Service) for providing advanced training. An existing Armed Service—the U.S. Army, for example—might be charged with providing the necessary advanced training, with the other Services sending their own operators to Army schools. The other Services would provide the ‘basic training’ and then a single Service would provide the advanced training. There are precedents for Services to send their personnel to other Services’ schools; parachute training is an example of consolidated training conducted by the U.S. Army.

Similar proposals for enhancements to USCYBERCOM have suggested a “SOCOM-like" model. This would increase its authorities over the training, assignment, and career progression for Service personnel involved in cyber operations, and also provide a separate system development acquisition budget (Smalley 2022; Pomerleau 2025b). During the ‘war on terrorism’ era, Congress gradually increased USSOCOM authority over planning and conducting special operations, directing the particulars of special operations training, and the acquisition of tailored equipment (Panella 2025). Some of these were Title 10 authorities previously assigned (and some perhaps still assigned) to the Services (USSOCOM 2025). Critics have argued that USSOCOM routinely violates the acquisition rules applicable to the overall military Department with considerable impunity (Capobianco and Phillips 2018).

Unlike USCYBERCOM, however, USSOCOM provides a Theater Special Operations Command (TSOCs) to regional COCOMs. TSOCs are “a sub-unified command of the geographic combatant command and the source of expertise in all areas of special operations [providing] the geographic combatant commander with a separate element to plan and control joint SOF in his theater [and] ensure SOF capabilities are considered throughout the entire planning process and that SOF are fully integrated into both peacetime and wartime planning” (USSOCOM 2025). USSOCOM can also provide to the COCOM joint special operations task forces (JSOTFs), “quick reaction command and control elements that can respond immediately to regional emergencies” (21). Of note is that the TSOCs are under the command (at least nominally) of the geographic COCOM, not USSOCOM. A side note is that recruitment and retention might actually be improved if cyber operations were under the aegis of USSOCOM, since cyber operators would perceive themselves as part of a highly elite force—cyber SEALs, as it were.

Providing Theater Cyber Operations Commands (TCOC) under the command of the geographic COCOMs might be an effective way to bring cyber to the tactical edge—or at least to COCOM headquarters. But this would of necessity entail a reduction of direct USCYBERCOM control over cyber operations. Perhaps if USCYBERCOM is to be retained as an independent entity, the model for its future organizational responsibilities should be that of U.S. Transportation Command (USTRANSCOM) rather than USSOCOM. USTRANSCOM provides a global-level ‘strategic’ service: the movement of joint forces into and within combat theaters for whichever geographic COCOM requires this service. USTRANSCOM assets are operationally directed by the geographic COCOMs. USTRANSCOM does not itself plan or engage in direct combat operations within a specific region, but refers to itself as providing “enabling capabilities” [1]. Direct combat is the exclusive responsibility of the regional COCOM.

[1] https://www.ustranscom.mil/

CONCLUSION

Loosening "the One Ring to Rule them All" ?

Ultimately, the proposal to decommission USCYBERCOM, and recommission its elements in a new configuration, is based on three premises. First, a cybered war against a technological peer/near-peer will not be fought exclusively within cyberspace as a “cyber domain.” It will also be conducted by tactical units physically ‘closing with the enemy’ (which might be conducted at both short- and long-ranges). Second, the need for cyber warfare capability embedded within units at the tactical edge is greatly increased by the nature of a future war against a technologically capable enemy with a greater number of tactical units, under a high level of electromagnetic warfare in which connectivity with headquarters is significantly curtailed. A third premise is that the priorities of individual COCOMs rarely match those of their counterparts and thus set up difficulties in the supported/supporting concept that supposedly ensures close trans-regional and trans-functional collaboration.

The third premise warrants further discussion. A noted (and perhaps natural) tendency of individual COCOMs is to disregard the requirements of other COCOMs and tenaciously fight for every asset and dollar that they perceive as necessary to complete their own missions. Inevitably, appetites outstrip supply, and intense mission focus affects collaboration. Each COCOM wants to be the resource priority for the Pentagon. This affects functional as well as geographic COCOMs, and there is no reason USCYBERCOM is not immune to this desire—and the inevitable consequences it brings. In theory, the Chairman of the Joint Chiefs and the Joint Staff would determine the allocation of resources (Lunkenbaugh 2025). However, each Combatant Commander—including Commander, USCYBERCOM—has a direct, Congressionally-mandated command relationship with the Secretary of War that, in many cases, will trump Joint Staff recommendations. This reality affects the relationship between the regional COCOMs and USCYBERCOM. As an open source describes, this issue is “with limited resources what gets the focus?...is Cybercom doing things that are of most interest to that combatant commander or are they working on targets that are of less interest to them, but of more interest to USCYBERCOM, which are typically CNMF targets” (Pomerleau 2025a).

Adding the three premises together with the assumption that future warfighting will be a multi-domain engagement against a technological near-peer carried out by necessarily semi-autonomous units at the tactical edge, it is fair to ask whether the current USCYBERCOM (to say nothing of an independent Cyber Force Service) is the optimal organizational structure to ensure victory. Should there be a separate, independent USCYBERCOM or should tactical cyber operations be embedded within the geographic COCOMs, with the ‘strategic level’ CNMF functions under USSTRATCOM or USSOCOM with their global mission responsibilities? Should USCYBERCOM hold the ‘one ring that rules all’ in cyberspace, or should those with ‘rings’ fighting on the tactical edge determine the full use of non-kinetic as well as kinetic fires?

To some extent, this is the debate already occurring over questions of cyber force generation and employment. Yet this debate is conducted through proxy arguments that ignore what may be the unacknowledged elephant in the room, namely, USCYBERCOM. It is well worth asking if this command is still fit for mission and, if so, whether more traditional models for providing forces to other geographic and functional combatant commands would be more effective in bringing military cyber to the tactical edge.

ABOUT THE AUTHOR

Sam J. Tangredi, Ph.D., CAPT, USN (Ret.) is the Leidos Chair of Future Warfare Studies and Professor of National, Naval and Maritime Strategy in the Center for Naval Warfare Studies of the U.S. Naval War College. He has wide experience as a strategic planner and director of strategic planning teams, including as Head, Strategy and Concepts Branch (N513), OPNAV. He has contributed to the writing of joint concepts, such as the Joint Operational Access Concept, and red teamed other joint concepts. He helped to establish the Joint Operating Environment (JOE) assessment. Sam has published seven books, over 200 journal articles, and numerous reports and presentations for a wide range of government and academic organizations (at various levels of classification). His latest authored book, Algorithms of Armageddon: The Impact of Artificial Intelligence on Future Wars (co-authored with George Galdorisi) was published in May 2024 (Naval Institute Press). He was co-editor of AI at War: How Big Data, Artificial Intelligence and Machine Learning Are Changing Naval Warfare (Naval Institute Press 2021), and, most recently, Cyber Warfare and Navies, co-edited with Chris C. Demchak (Naval Institute Press 2025). His book Anti-Access Warfare: Countering A2/AD Strategies—widely considered the definitive work on that subject—was re-released by Naval Institute Press in paperback in 2023. His previous writings have won fifteen professional literature awards including the U.S. Naval Institute's General Essay prize, AFCEA Cyber Edge award, and U.S. Navy League's Alfred Thayer Mahan Award. Dr. Tangredi is a retired U.S. Navy surface warfare officer who held command at sea.

REFERENCES

Capobianco, Joe, and David Phillips. 2018. *Strengths and myths of what makes special operations forces acquisition special.* U.S. Army (official website), May 14, 2018. https://www.army.mil/article/205259/strengths_and_myths_of_what_makes_special_operations_forces_acquisition_special.

Couillard, Jeffrey. 2024. "Beyond USCYBERCOM: The Need to Establish a Dedicated U.S. Cyber Military Force." *Cyber Defense Review* 9 (1): 55–72. https://www.jstor.org/stable/48770664.

DCDC (Department of Defense Cyber Crime Center). 2025. "Department of Defense Cyber Crime Center." Accessed July 1, 2025. https://www.dcdc.mil/.

Democracy & Human Rights Working Group. 2021. *U.S. Military Role in Democracy, Human Rights, and Humanitarian Assistance.* McCain Institute, March 10, 2021. https://www.mccaininstitute.org/resources/reports/u-s-military-role-in-democracy-human-rights-and-humanitarian-assistance/.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford University Press.

Goldman, Emily O. 2020. "The Cyber Paradigm Shift." In *Ten Years In: Implementing Strategic Approaches to Cyberspace,* edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, 31–45. Newport Paper 45. Newport, RI: Naval War College Press. https://digital-commons.usnwc.edu/usnwc-newport-papers/45/.

Hilger, Ryan. 2025. "Cyber Threats to Warships." In *Cyber Warfare and Navies,* edited by Chris C. Demchak and Sam J. Tangredi, 51–64. Annapolis, MD: Naval Institute Press.

Hollis, David M. 2010. *USCYBERCOM: The Need for a Combatant Command versus a Subunified Command.* U.S. Army (official website), June 29, 2010. https://www.army.mil/article/41585/uscybercom_the_need_for_a_combatant_command_versus_a_subunified_command.

Kreuzer, Michael P. 2021. *Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Levels of Warfare for the Information Age.* The Strategy Bridge, July. https://thestrategybridge.org/the-bridge/2021/7/

8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age.

Lawson, Ewan. 2022. “Between Two Stools: Military and Intelligence Organizations in the Conduct of Offensive Cyber Operations.” *Cyber Defense Review* 7 (3): 67–77. https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/.

Libicki, Martin. 2012. “Cyberspace is Not a Warfighting Domain.” *I/S: A Journal of Law and Policy for the Information Society* 8 (2): 325–340. https://kb.osu.edu/server/api/core/bitstreams/0f5c21be-28f3-5951-926c-6bdcab243319/content.

Lonergan, Erica, and Mark Montgomery. 2024. *United States Cyber Force: A Defense Imperative.* Washington, DC: FDD Press.

Lunkenbaugh, Josh. 2025. *Joint Staff Automating Resource Allocation Process.* National Defense, February 13, 2025. https://www.nationaldefensemagazine.org/articles/2025/2/13/joint-staff-automating-resource-allocation-process.

Matishak, Martin. 2024. *Proposal for Cyber Force study is watered down in final defense bill.* The Record, December 8, 2024. https://therecord.media/cyber-force-study-proposal-watered-down-defense-bill.

Matishak, Martin. 2025. *Pentagon fast-tracks ‘Cyber Command 2.0’ review, requests authorities wish list.* The Record, February 21, 2025. https://therecord.media/hegseth-cyber-command-2-0-review-authorities-wish-list.

NIST (National Institute of Standards and Technology). 2015. *Tactical Edge.* Computer Science Resource Center. https://csrc.nist.gov/glossary/term/tactical_edge.

O’Rourke, Ronald O. 2025. *Defense Primer: Navy Distributed Maritime Operations (DMO) Concept.* Technical report IF 12599. Congressional Research Service, July 5, 2025. https://www.congress.gov/crs-product/IF12599.

Oakley, David. 2019. *The Problems of a Militarized Foreign Policy for America’s Premier Intelligence Agency.* War on the Rocks, May 2, 2019. https://warontherocks.com/2019/05/the-problems-of-a-militarized-foreign-policy-for-americas-premier-intelligence-agency/.

Obis, Anastasia. 2024. *Lawmakers resurfacing cyber force idea in 2025 NDAA.* Federal News Network, June 7, 2024. https://federalnewsnetwork.com/defense-main/2024/06/ndaa-proposal-reigniting-debate-over-separate-cyber-force/.

Panella, Chris. 2025. *Special ops cracked the code on a problem plaguing the US military: getting better weapons faster.* Business Insider, March 4, 2025. https://www.businessinsider.com/us-special-operations-forces-has-answer-to-militarys-weapons-problem-2025-3.

Pederson, Eric, Don Palermo, Stephen Fancey, and Tim Blevins. 2022. *DOD Cyberspace: Establishing a Shared Understanding and How to Protect It.* Air, Land, Sea Application Center, January 1, 2022. https://www.alssa.mil/News/Article/2891794/dod-cyberspace-establishing-a-shared-understanding-and-how-to-protect-it/.

Pomerleau, Mark. 2017. *Cyber Command stands up planning cells at combatant commands.* C4ISRNet, October 11, 2017. https://www.c4isrnet.com/show-reporter/ausa/2017/10/11/cyber-command-stands-up-planning-cells-at-combatant-commands/.

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

Pomerleau, Mark. 2025b. *DOD leadership asks for Cybercom 2.0 relook.* DefenseScoop, May 20, 2025. https://defensescoop.com/2025/05/20/cybercom-2-0-relook-dod-leadership/.

Smalley, Suzanne. 2022. *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/.

Straub, Jeremy. 2019. *A cyber attack could wreak destruction comparable to a nuclear weapon.* The Conversation, August 16, 2019. https://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173.

Swift, Scott H., and Antonio P. Siordia. 2021. “Mission Command and Speed of Decision.” In *AI at War: How Big Data, Artificial Intelligence, and Machine Learning Are Changing Naval Warfare,* edited by Sam J. Tangredi and George Galdorisi, 135–149. Annapolis, MD: Naval Institute Press.

Tangredi, Sam J. 2013. *Anti-Access Warfare: Countering A2/AD Strategies.* 101–103. Annapolis, MD: Naval Institute Press.

Tangredi, Sam J. 2025. "New Theory of Navies: Maritime, Air, Space and Cyber." In *Cyber Warfare and Navies,* edited by Chris C. Demchak and Sam J. Tangredi, 360–370. Annapolis, MD: Naval Institute Press.

U.S., Chairman of the Joint Chiefs of Staff. 2006. *The National Military Strategy for Cyberspace Operations.* https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.

USCYBERCOM (U.S. Cyber Command). 2022. *CYBER101-Defend Forward and Persistent Engagement,* October 25, 2022. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

USCYBERCOM (U.S. Cyber Command). 2023. *About the Cyber National Mission Forces,* December 6, 2023. https://www.cybercom.mil/Media/News/Article/3610711/about-the-cyber-national-mission-forces/.

USCYBERCOM (U.S. Cyber Command). 2024. *CNMF marks a decade Defending the Nation,* January 17, 2024. https://www.cybercom.mil/Media/News/Article/3647031/cnmf-marks-a-decade-defending-the-nation/.

USSOCOM (U.S. Special Operations Command). 2025. *Introduction to Special Operations Command.* N.d. https://www.socom.mil/FactBook/2006.

Walsh, Thomas A., and Alexandria L. Huber. 2023. "A Symphony of Capabilities: How the Joint Warfighting Concept Guides Service Force Design and Development." 4th Quarter, *Joint Forces Quarterly* 111:4–15. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3568312/a-symphony-of-capabilities-how-the-joint-warfighting-concept-guides-service-for/.

Warner, Michael. 2020. "A Brief History of Cyber Conflict." In *Ten Years In: Implementing Strategic Approaches to Cyberspace,* edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, 13–30. Newport Paper 45. Newport, RI: Naval War College Press. https://digital-commons.usnwc.edu/usnwc-newport-papers/45/.

Received 1 August 2025; Revised 28 October 2025; Accepted 16 December 2025

✧ Conclusion ✧

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 3, 193-199
https://doi.org/10.55682/cdr/ygas-hy7p

EDITORIAL

Reform or Replace: The Strategic Dilemma of U.S. Cyber Forces

Michael Poznansky*, Chris Demchak, Frank L. Smith III

U.S. Naval War College, Newport, RI, USA

The essays in this volume collectively address a wide range of questions related to the debate about force generation and employment in cyberspace. Among the authors, there is a near-universal consensus that the status quo could—and should—be improved in meaningful ways. The overarching sentiment that major changes are needed is widely shared. However, the diagnosis of the problem and the remedies offered vary dramatically.

We first take stock of where the arguments and evidence presented within the pages of this special issue lead us by focusing on two key dimensions of debate:

(1) How differing perspectives of the cyberspace-as-domain question shape views about force generation and employment decisions; and

(2) What timing considerations and risks associated with different proposals imply about the costs and benefits of incremental versus radical change.

We then identify enduring challenges that nearly all proposals must wrestle with regarding the perennial competition for talent, defense of the homeland, and relationships with cyber intelligence organizations. Finally, we conclude by outlining directions for future work on these critical topics.

* Corresponding author: michael.poznansky@usnwc.edu

Disclaimer: *The views expressed in this work are those of the author(s) and do not reflect the official policy or position of their employer(s), the U.S. Naval War College, the U.S. Military Academy, the Department of War, the U.S. Government, or any subdivisions thereof.*

WHERE DOES THE DEBATE LEAD US?

The array of options presented in this special issue offer policymakers much to consider and promising ideas to work with. Across the articles, we identified two key issue areas that help make sense of the different assumptions at work and the trade-offs involved: the question about cyberspace as a domain, and the question of timing surrounding reforms.

The Domain Question

Despite the lack of consensus on what cyberspace fundamentally represents, it is clear that it constitutes a multi-faceted, highly-dimensional problem space. When considering the future of force generation and employment, differing (and sometimes conflicting) proposals are heavily influenced by the perspectives and assumptions of their proponents. Is it a military domain pure and simple, a domain with special distinctions, or something else, such as a ubiquitous substrate? The intent of asking these questions is not to rehash longstanding fights about the definition or meaning of cyberspace. Rather, the answers one gives are significant because they connect to the core questions at the heart of this special issue.

By and large, authors tended to adopt, implicitly or explicitly, a singular view of cyberspace.[1] These views, in turn, seemed to exert a great deal of influence on the proposed solutions. At the risk of oversimplification, the more that a given author or authors saw cyberspace as unique, the more radical their proposals were relative to the status quo. In contrast, those who believed cyberspace is essentially a warfighting domain—albeit one with distinctive characteristics—tended to advance solutions that were more evolutionary in nature.

It is worth considering the possibility that cyberspace is many things at once—a domain of warfare, a domain of near-constant competition, and a globally ubiquitous societal substrate. When it comes to a hot war, the reality is that cyber is essential to the fight. In addition to supporting kinetic operations, it has its own independent effects on the battlefield. It is also the case that each of the armed services has long relied on cyberspace and digital infrastructure for essential functions and kinetic operations, rendering it distinct from more traditional domains. To complicate matters, there is a substantial amount of cyber activity that occurs in peacetime and during state-on-state competition, below or orthogonal to the traditional threshold of conventional armed conflict.

By privileging one of these perspectives over the others, decision-makers may inadvertently constrain the decision space and fail to fully accommodate the variety of environments and missions in which cyber is employed. It remains an open question whether cyber *in* war requires different organizational constructs and force employment mechanisms than those used in relentless cyber warfare among states outside armed conflict. Tangredi, for example,

[1] This reflects how much of the literature handles the cyberspace as a domain question. See, for example, Demchak (2022), Fischerkeller, Goldman, and Harknett (2022), Healey (2013), Lynn (2010), and Rid (2013)

offers an interesting and provocative organizational solution: to give combatant commanders control over cyber operations and assets needed in the event of armed conflict within their geographic theaters, and let U.S. Cyber Command (USCYBERCOM) handle the daily ongoing national mission set. And yet, even the adoption of this proposal would not alleviate the reality that services would still need their own indigenous capabilities to remain operational, another testament to the multifaceted nature of cyberspace. Either way, it is imperative that proposals for organizational reform or replacement sufficiently address the many faces of cyber operations.

The Timing Question

A second key strategic challenge consistently highlighted in this special issue pertains to timing. For those interested in more radical change, two questions that must be addressed more comprehensively are the time required to implement significant change and the vulnerabilities that may arise during the transition. For example, how feasible is it to create a new cyber service or a digital command without exposing the United States and its allies to unacceptable risk in the process? In other words, even if one accepts these proposals as sound, there remains the thorny question of how to implement them with sufficient urgency and speed to deny adversaries the ability to exploit the transition. USCYBERCOM was created over 15 years ago, and it has taken many years for the Command to develop the operational capacity it has today. To paraphrase Francis Bacon—courtesy of Warner and Goldman in this special issue—the cure shouldn't be worse than the disease.

It is equally important not to let those advocating for more incremental change off the hook. If radical transformation introduces risks, taking only smaller steps comes with its own challenges. Timing issues manifest differently here. Rather than determining how best to bridge the gap between radical change and effective implementation, the evolutionary camp must explain how to address known, longstanding problems before the threat environment degrades further or adversaries preempt the small improvements, rendering reforms too little, too late. If necessary reforms to USCYBERCOM or the nation's cyber force generation take years or longer to materialize, it could always be argued in retrospect that the potential disruption caused by more radical change would have been more timely and worthwhile—so long, of course, as those solutions would have actually fixed the underlying issues.

The complexity of strategic timing risk opens the possibility for interesting policy choices and unusual bedfellows. In theory, someone could intellectually align with the evolutionary camp and yet support radical change based on a practical assessment that their preferred option – incremental change – incurs too much risk by taking too long due to a lack of bureaucratic urgency. Alternatively, one may believe that radical change is warranted but seek to mitigate disruption risk by ultimately supporting incremental change as the least bad option in a highly dynamic geopolitical environment. Either way, both policymakers and analysts must compare and contrast proposed reform solutions and the risks associated with the speed or delay of enacting them to ensure more favorable outcomes for cyber force generation and use.

ENDURING CHALLENGES AND OPPORTUNITIES

Moving beyond the underlying assumptions about the fundamental nature of cyberspace and the timing risks of incremental versus radical change, the articles in this special issue speak to several enduring challenges that any viable solution must address.

First, there is the seemingly relentless talent shortfall. Competition for high-end cyber talent is fierce. The U.S. military is competing with a vibrant private sector. One key question arising from this special issue is whether and how the proposed force generation and employment models help on this front. It is often and reasonably posited that a separate service, whether an independent cyber force or a full-fledged department, will help recruit and retain new talent (Lonergan and Montgomery 2024). If prospective recruits see a professional cyber community they want to be part of, with a mission focused on achieving outcomes they care about, they may be more likely to sign up. Or perhaps prospective recruits might be more attracted to and more likely to be retained in military service if USCYBERCOM more effectively marketed the intriguing and compelling aspects of its missions and overall impact. The same applies to the services' recruitment and career management, which could more effectively engage cyber warfighters by clarifying doctrine and delegating cyber power to the tactical edge (Lawrence 2025). In any scenario, critically, the organizational culture must be a fit. Comparative analyses that address these talent-related issues would be valuable.

Second, there is the question of the home front. In any war involving the U.S., one of the primary means by which an adversary would try to reach out and touch the homeland is through widespread digital disruption of critical infrastructure (Office of the Director of National Intelligence (ODNI) 2023). There is debate about the likelihood and feasibility of this. Regardless, the U.S. must prepare for this possibility. This raises difficult questions about how to draw appropriate lines between externally facing entities, such as the military and the intelligence community, and those that are internally facing, such as the Department of Homeland Security and law enforcement. Additionally, there are the challenges and opportunities involved with public organizations interacting with, relying on, and perhaps delegating some missions to the private sector, which controls key resources and employs much of the critical talent needed to defend the homeland. Understanding how reforming or replacing the existing model of military force generation and employment will enhance or detract from the ability to coordinate with domestically focused agencies and commercial actors is critical.

Third, the perennial question of intelligence remains (Lindsay 2025). Debates about whether the U.S. needs a separate cyber service or whether effective reform is possible do not necessarily imply that the so-called dual hat arrangement—in which the director of USCYBERCOM also directs the National Security Agency (NSA)—must disappear (Chesney 2020; Sulmeyer 2017). But for some of the proposals, including the more radical suggestions to decommission USCYBERCOM or build out a new digital command, the thorny issue of how to partner with NSA and deconflict where necessary is incredibly important. The prospect of a separate cyber service has significant implications for NSA and the broader dynamics of cyber intelligence. At present, USCYBERCOM and NSA are increasingly assuming responsibility for key aspects of training previously handled by the armed services. If a separate cyber service is created, it will raise questions about how to resolve new tensions between these organizations.

ENVISIONING THE FUTURE(S)

A key strategic challenge for shaping the future of cyber force generation and employment is to carefully consider what happens next. Providing the rationale for one choice or another requires more than just fixing what is broken today. It also requires explaining how the proposed fix is expected to adapt to an uncertain future, such as a world of more authoritarian, competently digitized, and hostile states. Future research is needed on a range of questions, from how military bureaucracies cope with organizational and technological change to how to more effectively allocate limited resources and responsibilities in the event of war.

In the context of the military bureaucracy, does a separate cyber service ease or aggravate turf battles? Does a new cyber service, or a more empowered USCYBERCOM, cause the Army, Navy, Marines, Air Force, and Space Force to abandon cyber, or, conversely, do they invest in whatever service-specific cyber talent they must retain? If there were no USCYBERCOM, would the remaining combatant commands be more or less effective in acquiring the specialized cyber talent they need from the existing services?

Then there are questions about emerging technologies and the allocation of scarce resources during future warfare. Does an expanded USCYBERCOM or a new cyber service struggle as the traditional services redirect resources, recruitment bonuses, and talent to artificial intelligence (AI)? What visions of the future occupy the minds of military and civilian decision-makers likely to enact these policies? How do these proposals provide a feasible and future-proof operational response to unknown developments in robotics, AI, and quantum technologies? Choose wrong, and American competition, deterrence, and warfighting could all suffer.

Taken together, the contributions in this special issue make one point unmistakable: the U.S. cannot afford to treat cyber force generation as a technical afterthought or a bureaucratic reshuffle. It is a strategic choice about how it will fight, compete, and endure in an environment where the domain, the battlefield, and broader society are increasingly intertwined in cyberspace. Whatever policymakers ultimately opt to do, delay and drift are themselves decisions—and ones that will be exploited by capable adversaries and paid for in lost talent, fragile partnerships, and vulnerable infrastructure. The task now is not to wait for a perfect design, but to move deliberately toward resilient arrangements that can evolve, absorb shocks, and integrate public, private, intelligence, and military strengths faster than rivals can pull them apart.

There are no risk-free options on the table. Radical change invites temporary vulnerability, while incrementalism invites a lack of needed urgency and potentially long-term obsolescence. However, the collective wisdom in this special issue makes it clear: the current model is under internal strain and external threat. We must move beyond admiring the problem to implementing solutions that survive contact with the future. Time is the one resource we cannot generate, and our adversaries are not waiting for us to finish the debate.

ABOUT THE GUEST EDITORS

Dr. Michael Poznansky is an Associate Professor in the Strategic and Operational Research Department and a core faculty member in the Cyber and Innovation Policy Institute at the U.S. Naval War College. He is the author of *Great Power, Great Responsibility: How the Liberal International Order Shapes US Foreign Policy* (Oxford University Press, 2025) and *In the Shadow of International Law: Secrecy and Regime Change in the Postwar World* (Oxford University Press, 2020). Dr. Poznansky has held fellowships with the Belfer Center at Harvard Kennedy School, the Dickey Center at Dartmouth College, and the Modern War Institute at West Point. He holds a Ph.D. from the University of Virginia.

Dr. Chris C. Demchak is Grace Hopper Chair of Cyber Security and Senior Cyber Scholar, CIPI, U.S. Naval War College, with degrees in engineering, economics, and comparative complex organization systems /political science. Her long-term expertise focuses on digital surprises disrupting today's complex "socio-technical-economic systems (STES)". She has written on emerging technologies, adversaries' cyber/AI/ML campaigns, virtual wargaming for strategic/organizational learning, and national/enterprise resilience against complex systems surprise. Books of note include: *Wars of Disruption and Resilience* (cybered conflict); *Designing Resilience*; and *Cyber Warfare and Navies (2025*). Articles of note include "China's Maxim (BGP Hijacking, 2018 and update 2021)", "Four Horsemen of AI" (2019), " 'Sea-hacking' Sun Tsu: Deception in Global AI/Cybered Conflict" (2021), and "Achieving Systemic Resilience in a Great Systems Conflict Era" (2022). Works in progress include *Great Systems Conflict: Cyber Westphalia, Warfare, and Collective Operational Resilience*, "Rise of China and Great Systems Conflict", and "Quantum AI Cyber Dancing with Thorns".

Dr. Frank L. Smith III is a Professor and Director of the Cyber and Innovation Policy Institute at the U.S. Naval War College. His interdisciplinary research and teaching examine the relationship between emerging technology and international security. Previous work includes his book, *American Biodefense*, the edited volume, *Cyber Wargaming*, and articles published in *Security Studies*, *Social Studies of Science*, *Security Dialogue*, *Health Security*, and *The Lancet*, among others. He has a Ph.D. in political science and a B.S. in biological chemistry, both from the University of Chicago.

REFERENCES

Chesney, Robert. 2020. *Ending the 'Dual-Hat' Arrangement for NSA and Cyber Command?* Lawfare, December 20, 2020. https://www.lawfaremedia.org/article/ending-dual-hat-arrangement-nsa-and-cyber-command.

Demchak, Chris C. 2022. "What Corrodes Cyber, Infects Its Offspring: Unlearned Lessons for Emerging Technologies." *The Cyber Defense Review* 7 (1): 153–162. https://www.jstor.org/stable/48642047.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory, Redefining National Security in Cyberspace.* Oxford University Press.

Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Cyber Conflict Studies Association.

Lawrence, Susan S. 2025. *President's Commentary: Focus on The Cyber Edge.* AFCEA Signal Media. https://www.afcea.org/signal-media/presidents-commentary-focus-cyber-edge.

Lindsay, Jon. 2025. *Age of Deception: Cybersecurity as Secret Statecraft.* Cornell University Press.

Lonergan, Erica D., and Mark Montgomery. 2024. *United States Cyber Force: A Defense Imperative.* FDD Press.

Lynn, William J. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89 (5). https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

Office of the Director of National Intelligence (ODNI). 2023. *Annual Threat Assessment of the U.S. Intelligence Community.* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

Rid, Thomas. 2013. *Cyber War Will Not Take Place.* Oxford University Press.

Sulmeyer, Michael. 2017. "Getting to Ground Truth on the Elevation of U.S. Cyber Command," August 31, 2017. https://warontherocks.com/2017/08/getting-to-ground-truth-on-the-elevation-of-u-s-cyber-command/.

WEST POINT
PRESS

THE ARMY CYBER INSTITUTE AT WEST POINT
2012

https://cyberdefensereview.army.mil/