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

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.