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

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.