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

CONCEPTUAL CAGE OF OUTDATED TERMS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