The US Army War College Quarterly: Parameters

Volume 52
Number 3 *Volume 52, Number 3 Autumn Issue*

Article 8

8-25-2022

Assessing the Army’s Cyber Force Structure

John Fernandes

Nicolas Starck

Richard Shmel

Charles Suslowicz

Jan Kallberg

See next page for additional authors

Recommended Citation

John Fernandes, Nicolas Starck, Richard Shmel, Charles Suslowicz, Jan Kallberg & Todd Arnold, "Assessing the Army’s Cyber Force Structure," *Parameters* 52, no. 3 (2022), doi:10.55540/0031-1723.3170.

Assessing the Army’s Cyber Force Structure

Authors

John Fernandes, Nicolas Starck, Richard Shmel, Charles Suslowicz, Jan Kallberg, and Todd Arnold

Assessing the Army's Cyber Force Structure

John Fernandes, Nicolas Starck, Richard Shmel, Charles Suslowicz, Jan Kallberg, and Todd Arnold

ABSTRACT: The skill and capacity of Army cyber forces have grown in the decade since their creation. This article focuses on needed structural changes to the Army's portion of the Cyber Mission Forces that will enable their continued growth and maturity since the Army's past organizational and structural decisions impose challenges impacting current and future efficiency and effectiveness. This assessment of the current situation highlights the areas military leadership must address to allow the Army's cyber forces to continue evolving to meet the needs of multi-domain operations.

Keywords: workforce development, task organization, cyberspace operations, unity of effort, unity of command

Training and equipping a new military force capable of conducting operations in a new domain is an iterative process. The last time the United States embarked on such an effort was the birth of aviation units and the emergence of the air domain at the dawn of the twentieth century. Tactics, force structures, and strategies for utilizing the new capabilities evolved after the establishment of military aviation but were defined and limited by the lack of crisis at the time. World War II forced the rapid maturation of the Air Corps and resulted in the creation of the US Army Air Corps, a cohesive fighting force designed for the challenges of the air domain.[1] Like the Army Air Corps, the Army's cyber forces are reaching maturity with tangible capabilities and operational experience against adversaries and will benefit from assessing the impacts of prior organizational and personnel decisions in preparation for multi-domain operations.

A significant and sophisticated intrusion into military networks provided the impetus for standing up US Cyber Command (USCYBERCOM) and for cyberspace to join air, sea, land, and space as a warfighting domain. The Army and the Department of Defense (DoD) have made significant strides to establish

[1] Tami Davis Biddle, *Air Power and Warfare: A Century of Theory and History* (Carlisle, PA: US Army War College Press, 2019), https://press.armywarcollege.edu/monographs/378/.

competence within the domain.[2] From a force structure perspective, major highlights include:

- establishing US Army Cyber Command (ARCYBER) in 2010;
- forming an offensive cyber force by creating the 780th Military Intelligence Brigade (Cyber) in 2011;
- creating the Cyber Protection Brigade (CPB) in 2014 to house the defensive force;
- establishing the 915th Cyberspace Warfare Battalion (CWB) in 2019 for tactical cyberspace electromagnetic activities requirements, and all Cyber Mission Force (CMF) teams; and
- achieving full operational capability in 2018.

On the personnel front, the Army established the Cyber branch in 2014 and integrated electronic warfare in 2018. Recently, the Army formalized the cyberspace capabilities development officer/warrant officer military occupational specialties (MOSs) to provide the organic ability to design and create specific cyberspace capabilities.

From doctrine to training to organization, the branch and the cyber units have had to identify needs, experiment, and develop solutions to meet the evolving demands of cyberspace operations. In this article, we examine the challenges associated with two initial force structure decisions and provide considerations for overcoming them.

First, when the Army created its cyber units, offensive and defensive cyber operations were isolated within two distinct and separate brigades. The historical divide continues with unintended consequences. Despite creating a new branch and military occupational specialties, the organizational decision to separate offensive cyber operations (OCO) and defensive cyber operations (DCO) negatively impacted personnel and resourcing.

Second, these units have complex chains of command with separate administrative control (ADCON) and operational control (OPCON) relationships. Currently, the operational command of a cyber team is not aligned with the team's administration and leadership, including personnel ratings, property accountability, Unified Code of Military Justice authority, and

[2] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010, 97–108, https://www-foreignaffairs-com.usawc.idm.oclc.org/articles/united-states/2010-09-01/defending-new-domain.

command itself (for example, a company commander tracks a cyber team's training and medical readiness while the team lead is responsible for daily operations). These complexities cause confusion and consternation and hamper unity of effort.

While these organizational decisions were deliberate and motivated by operational demands, they hindered unity of effort within the Army's cyber forces, imposing organizational and operational costs. Introspection is occurring across the joint cyber community. With all CMF teams recently achieving full operational capacity, US Cyber Command is evaluating its current size and requesting additional teams to be fielded by the Army and Air Force.[3] To bring a more unified approach to cyberspace, the Air Force realigned its internal components' structure and composition by redesignating and reassigning several units under the 67th Cyberspace Wing.[4] Now is an ideal time to re-examine the Army's internal structures to support cyberspace operations better. The Army would be remiss to ignore the implications of past decisions made of necessity without reassessing their effectiveness. We argue the Army must push for greater unity within the Cyber branch so the organization continues to progress as an effective fighting force in cyberspace.

Background

The majority of the decade since US Cyber Command and US Army Cyber Command's establishment was dedicated to building and training the force. While the inchoate force stood up teams, designed—and redesigned—training pipelines for various specialties, and struggled to recruit and retain talent, the forces were in constant contact.[5] The Army's original concept was to provide 41 teams, and shortly after that the mandate expanded to include 21 reserve component defensive Cyber Protection Teams (CPTs) (11 Army National Guard and 10 Army Reserve).[6] To meet this immense manning requirement, planners drew soldiers primarily from the Military Intelligence (MI) and Signal Corps (SC) branches, the two branches already engaged in offensive and defensive cyber operations. The rapid

[3] *Fiscal Year 2021 Budget Request for U.S. Cyber Command and Operations in Cybersopace: Hearings before the Committee on Armed Services, Subcommittee on Intelligence and Emerging Threats and Capabilities, US House of Representatives*, 116th Cong. (2020), https://www.congress.gov/116/chrg/CHRG-116hhrg40605/CHRG-116hhrg40605.pdf; and Mark Pomerleau, "Cyber Command's Force Is Growing, in Part, to Support Space," FEDSCOOP (website), April 8, 2022, https://www.fedscoop.com/cyber-commands-force-is-growing-in-part-to-support-space/.

[4] Mark Pomerleau, "Air Force Revamps Its Teams for U.S. Cyber Command," C4ISRNET (website), September 18, 2020, https://www.c4isrnet.com/cyber/2020/09/18/air-force-revamps-its-teams-for-us-cyber-command/.

[5] Jim Garamone, "Rogers Outlines Cyber Challenges Facing DoD, U.S.," Department of Defense (website), September 9, 2015, https://www.defense.gov/News/News-Stories/Article/Article/616569/rogers-outlines-cyber-challenges-facing-dod-us/.

[6] Edward Cardon, "2014 Green Book: Army Cyber Command and Second Army," US Army (website), September 30, 2014, https://www.army.mil/article/134857/; and *US Army Cyber Posture: Hearing before the Armed Services Committee, Subcommittee on Cybersecurity*, 115th Cong. (2017) (statement of Lieutenant General Paul M. Nakasone, Commanding General, US Cyber Command), https://www.armed-services.senate.gov/imo/media/doc/Nakasone_05-23-17.pdf.

assembly of personnel into "cyber" units (the branch was not yet approved) brought the unique attitudes, traditions, and perspectives of the previous branches to the units. Given the immediate operational necessity created by adversary activity, personnel assignments and missions aligned with the previous branch's mission. Signal Corps soldiers were assigned to the cyber protection brigade, and intelligence soldiers were assigned to the 780th Military Intelligence Brigade. As a result, the early incarnations of the branch's units did not share a common attitude, mission, or understanding of each other's capabilities.

Similarly, the Army's basic manning requirement to field 41 teams placed immense stress on the entire chain of command of its nascent cyber units.[7] The Army Cyber School, responsible for individual MOS training, was not established until 2015, so training fell upon the cyber brigades.[8] The preponderance of training still falls on the brigades due to specific training requirements for each cyber work role—a jointly defined job standard similar to a MOS (we discuss work-roles in more detail later in the article).

Training and equipping incoming personnel and organizing them into teams was the brigades' all-consuming mission. When a team achieved initial operational capability, it was turned over to its operational command. Once a team achieved full operational capacity, the ADCON chain of command maintained the team's full operational capacity manning and began building the next team. This task separation enabled the Army chain of command to focus on building teams while separate operational commands focused on employing the teams. However, this process crystallized the administrative control and operational control split into a permanent fixture. The decision to build units aggressively and prioritize arbitrary checkpoints enabled the Army to achieve required operational readiness conditions rapidly, but at the expense of developing the most effective and efficient units.

Ultimately, these organizational challenges—the offensive cyber operations and defensive cyber operations split and divided chains of command—and the resulting personnel challenges are a by-product of the herculean effort necessary to overcome the traditional glacial pace of the Department of Defenseand Army bureaucracy. However, the cyber force has matured and gained operational

[7] Cardon, "Army Cyber Command."

[8] George I. Seffers, "U.S. Army Builds Cyber Branch One Step at a Time," *Signal Magazine*, Armed Forces Communications and Electronics Association, April 1, 2015, https://www.afcea.org/signal-media/education/us-army-builds-cyber-branch-one-step-time.

experience, and the situation has changed. The Army must reassess prior decisions and adjust to meet the force's and nation's long-term needs.

Offense and Defense Split

Siloing the force's offensive and defensive elements created barriers within the force that are continually being reinforced, including operational and cultural challenges and impacting the soldiers and civilians who comprise the Army's cyberspace forces.

Under the current structure, the Cyber branch has effectively created specialization in offense or defense roles, with soldiers' designations determined by their initial assignment. Once inside the offensive or defensive silo, personnel cannot easily move between workspaces, discuss missions, or build a cohesive culture. Personnel in both offensive and defensive units complete a job qualification record (JQR) to demonstrate proficiency for a specific work role. This time-consuming process entails specialized training, requires operational experience, and introduces a significant organizational cost to transfer between offense and defense. These artificial barriers foster the incorrect belief that experience in one form of cyber operation does not translate to the other and bifurcates the branch.

The centralized selection lists exemplify the reinforcement of this bifurcation. Individuals selected to lead offensive cyber units primarily have an offensive background (and military intelligence origin). Defensive units are generally led by officers with defensive (and Signal Corps) experience. Although introducing the Assignment Interactive Module (AIM) Marketplace provided increased autonomy to soldiers, it created another avenue through which a soldier can be designated as a specific type of cyber soldier. Leaders now have an opportunity to screen future subordinate leaders for previous experience within a particular operational facet. While valuable on the surface, this possibility reinforces the chance of a first assignment determining a soldier's career path.

Since military operations and the cyberspace domain are complex, specialization can be beneficial and desirable. However, structural separation between offense and defensive cyberspace units and operations combined with the inadvertent individual specialization in defensive or offensive cyber operations creates potential problems.

Challenges

While the barriers have changed over time, the potential for real or perceived preferential status exists while two distinct silos exist. Initially, the DCO forces were built from scratch, while OCO forces could leverage existing, albeit limited, expertise. The additional accesses, authorities, infrastructure, and training required for successful offensive cyber operations fostered a feeling of superiority or preferential status for the units rather than a recognition of the requirements for successful offensive cyber operations. This perception is exacerbated by the additional support attached to offensive cyber units (for example, military intelligence support and developer capacity). This skewed perspective—of importance, impact, and necessity—can damage morale and result in dangerous implications for planning and resourcing.

These perceptions regarding superiority and preferential treatment can have resounding impacts on unit morale, retention, and culture. Consequently, members of the negatively perceived group (defensive cyber operations) may attempt to become a member of the positively perceived group (offensive cyber options) if possible.[9] Since mobility between offense and defense has been relatively constrained, the members of the negatively perceived group may change their valuation method.[10] For example, defensive cyber operations could redefine their internal value as the total number of missions executed rather than resources allocated. However, these changes in valuation can increase differences in culture between defensive and offensive cyber operations. Alternatively, the negatively perceived group may "activate competitive strategies to achieve a positive social identity" with the unintended negative outcomes of subgroup conflict.[11] Specialization heightens this perception of conflict and may cause job dissatisfaction, frustration, and morale problems.[12] At the organizational level, there may be a rise in the promotion of self-interest of the subgroups (defensive and offensive), along with additional organizational cost to manage where the subgroups intersect, such as requirements for schoolhouse training, operational support from ARCYBER or CYBERCOM, or the Army's requirement process.[13]

The perspective mentioned above results in the Army's defensive cyber forces being unnecessarily deprioritized. Specialized skillsets like capability development (creating hardware or software solutions) and reverse engineering (deconstructing

[9] Samuel Fernández-Salinero and Gabriela Topa, "Intergroup Discrimination as a Predictor of Conflict within the Same Organization: The Role of Organizational Identity," *European Journal of Investigation in Health, Psychology and Education* 10, no. 1 (May 2019), https://www.mdpi.com/2254-9625/10/1/1.

[10] Fernández-Salinero and Topa, "Intergroup Discrimination."

[11] Fernández-Salinero and Topa, "Intergroup Discrimination."

[12] Bernard Oladosu Omisore and Ashimi Rashidat Abiodun, "Organizational Conflicts: Causes, Effects and Remedies," *International Journal of Academic Research in Economics and Management Services* 3, no. 6 (Nov 2014), https://www.mdpi.com/2254-9625/10/1/1.

[13] Omisore and Abiodun, "Organizational Conflicts."

an unknown piece of hardware or software to determine how it functions) were seen as offensive functions and placed in OCO units, even though they are also critical for effective incident response. Like personnel prioritization impacts resource allocation, decisions will also be shaped by an environment where the offense is viewed as superior, more critical, or more challenging. The unintended personnel and resource implications of the perceptions of offensive and defensive cyberspace operations work in opposition to the relative restrictions placed on the conduct of different operations based on legal authorities. Given the potential global implications, the authority to conduct offensive cyber operations is held by US Cyber Command, given the appropriate determinations by the National Command Authority (the president, secretary of defense, or designee).[14] By contrast, a standing authority requires defensive cyber operations be conducted on the Department of Defense information networks, with authority delegated to the service-component organizations like Army Cyber Command.[15] This requirement suggests defensive cyber operation should have fewer internal barriers and more freedom of action. However, even when network owners fully cooperate with a defensive mission, it can take days or weeks to work through organizational hurdles, gather resources, and take necessary network actions. Deliberate effort and attention by commanders are needed to address the inequalities in perception and resourcing to resolve those issues and their resulting operational harms.

At the individual level, this disparity in treatment feeds myopia across the branch regarding the capabilities and requirements of different cyberspace missions. Bright young soldiers are lured to specific units with the promise of more glamorous offensive work, preventing their exposure to the challenging, multitudinous, and critical defensive cyber work required across the Army. Failure to expose officers and noncommissioned officers to the full spectrum of cyberspace operations feeds a dangerous misconception that advanced understanding is not portable to different aspects of the cyberspace domain and that the highest levels of proficiency do not require both perspectives.

Siloing reduces our effectiveness in planning and executing operations by limiting cross-pollination between the offensive and defensive forces. A critical tenet of Army planning is that the "enemy has a vote." This belief is codified in our doctrine, with the enemy being a mission variable and enemy analysis being a portion of intelligence preparation of the battlefield and part of paragraph

[14] Robert Chesney, "The Domestic Legal Framework for US Military Cyber Operations," Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2003 (Stanford, CA: Hoover Institution, July 2020), https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3668463_code119080.pdf?abstractid=3668463&mirid=1.

[15] Center for Strategic Leadership, *Strategic Cyberspace Operations Guide* (Carlisle, PA: US Army War College, August 2021), https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf.

one of the operations order.[16] Soldiers with significant experience in either offensive or defensive cyber operations can provide unique and critical insights into the other forms of operation.[17] When we look to the field Army, the billets for cyber officers (17A and 17B) are primarily planner roles down to the brigade level, where cyber officers will be responsible for planning and integrating offensive, defensive, and electronic warfare capabilities. An officer whose career has only exposed them to one facet may not be able to utilize the other two aspects as effectively.

The partitioning of cyber forces exacerbates problems posed by the small size of the branch. With a single brigade for both offense and defense, leaders who stay within those silos can have outsized impacts. Battalion commanders return as brigade commanders, and their leadership styles, command climates, and assessments of subordinate leaders endure beyond the typical two-year command and further reinforce the force's cultural divide. It becomes less likely commanders will bring a fresh perspective, and units become more susceptible to dangerous forms of groupthink. Subordinates who interact negatively with a leader can anticipate meeting with the leader repeatedly, creating an environment suited to the establishment of fiefdoms and other forms of counterproductive leadership.

Considerations for Mitigation

Without deliberate effort, the challenges stemming from the bifurcation of offensive and defensive cyber capabilities will remain unsolved. While the Military Intelligence and Signal Corps branch lineages are less immediate, the resulting latent cultural and functional divisions remain. From senior leaders down to individuals serving on offensive and defensive teams, we must acknowledge all these challenges and actively work to minimize their effects. Bridging the divide may include deliberately seeking the opposite perspective when planning operations, seeking collaboration opportunities across silos, and conducting leader professional development programs to expose personnel to the other areas. At times, it may mean putting unit pride aside to acknowledge the contributions of the entire force. Professional military education should provide the impetus for this balanced exposure that is expanded through self-development and the

[16] Headquarters, Department of the Army (HQDA), *The Operations Process,* Army Doctrine Publication (ADP) 5-0 (Washington, DC: HQDA, July 2019), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18126-ADP_5-0-000-WEB-3.pdf.

[17] Chuck Suslowicz, Jan Kallberg, and Todd Arnold, "Government Cyber Breach Shows Need for Convergence," C4ISRNET (website), December 28, 2020, https://www.c4isrnet.com/opinion/2020/12/28/government-cyber-breach-shows-need-for-convergence/.

operational domain. Below are three ways to address the challenges through the Army's systems.

Enforce Breadth of Assignments for Officers

Some branches deliberately assign officers across segments of the branch to increase the understanding of the broader branch. For instance, the Infantry branch emphasizes officers serving in heavy and light units, while other branches such as Logistics, Military Intelligence, and the Signal Corps balance serving in division and brigade combat teams with the branch-specific strategic units. The Cyber branch must do the same to prevent fracturing the force and developing senior leaders with little understanding of or experience with entire portions of the domain. As a whole, the branch must value and promote breadth of experience. For officers, this training could be accomplished after the career course, an ideal period to refresh knowledge of the other aspects of the branch. The Cyber schoolhouse could provide additional specialized training if required. Similar models are used with branch-detailed personnel and the Cyber branch's training for company-grade officers who voluntarily transfer into the branch.

Determine Appropriate Specialization within the Cyber Force

While there is a need for understanding across offensive and defensive cyber operations, the existence of work roles and the recent creation of capability developers indicate specialization is required to establish and grow proficiency. This need is especially true for enlisted personnel and warrant officers, who are typically more specialized than commissioned officers. Specialization by mission, however, may be less appropriate than specialization based on function or technology. For instance, an expert at attacking Windows systems is probably well suited to defending Windows systems as opposed to analyzing network traffic in a Linux environment. Alternatively, soldiers who worked on electronic warfare systems for four years may be challenged to train their subordinates on host-based forensics as an NCOIC in a defensive unit.

Within the Signal Corps branch, warrant officers specialize as network and system engineers (255N and 255A) and within the Cyber branch the new cyberspace capabilities development MOSs (170D, 17D) are specialized by technology, not as offense or defense. Determining the proper set and scope of specializations requires analysis of individual tasks, knowledge, skills, and behaviors across offense and defense jobs and the increasing billets outside those units. Integrating job qualification records with existing Army programs, such as Critical Task Site Selection Board, for entry-level and advanced institutional training, individual tasks refinement, and additional skill identifiers or special qualifications identifier may help the Cyber branch identify and sustain the right specializations in the correct billets.

Consider Specialized and Integrated Units

The lineage of divided offensive and defensive units is not the only solution. The 915th Cyberspace Warfare Battalion and the Multi-Domain Task Force are steps toward more integrated cyber units. Across the Army, units dedicated to specific functions (such as combat support sustainment battalions) and units (such as brigade combat teams) integrate multiple functions to provide greater operational flexibility and internal support. The degree of mission specialization and the echelon at which to integrate functions is a multifaceted problem involving tradeoffs and should be based on careful analysis. As the cyberspace domain continues to mature, leadership should consider specialized and integrated units to meet the needs of the Army and Joint force.

Divided Chains of Command

Another structural challenge facing the Army's cyber forces is the complex chains of command constructed across the branch. At every level, cyber personnel face disconnected and competing leadership chains with conflicting priorities. Most cyber forces are assigned to Army Cyber Command, the force provider for joint and service requirements. Active-duty CMF teams are assigned to one of the two brigades for administrative control but fall under the operational control of the Cyber National Mission Force, a combatant command, or a combat support agency.

Further complicating matters, each brigade is assigned to the two-star operational headquarters of their mission's progenitor branch. The Cyber Protection Brigade is subordinate to the Network Enterprise Technology Command (a major subordinate command under the administrative control of Army Cyber Command) and the 780th Military Intelligence Brigade to the Intelligence and Security Command (a direct reporting unit to the Army's Deputy Chief of Staff for Intelligence).[18] Within this construct, the command relationships and responsibilities are often muddled, while support relationships are rarely used or defined. The persistent separation of administrative and

[18] HQDA, *Army Commands, Army Service Component Commands, and Direct Reporting Units,* Army Regulation (AR) 10-87 (Washington, DC: HQDA, December 11, 2017), https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN2541_AR10-87_WEB_Final.pdf.

operational control deleteriously affects the Army's ability to conduct effective cyberspace operations.

This divided chain of command diverges from the principles of unity of effort and unity of command and degrades the units' effectiveness and efficiencies. Operational and administrative control is split for the detachments/teams provided to the joint forces and the service-retained units. According to Army doctrine, "the chain of command assists commanders at all levels to achieve their primary function of accomplishing the unit's assigned mission while caring for personnel and property in their charge."[19] However, the Army cyber force's command structure adds complexities to the key command elements and exacerbates the chain of command's challenges to serve its function.

Challenges

While units have administrative and operational requirements, they do not have enough training days to accomplish the requirements placed upon them—a challenge not unique to cyber forces.[20] Commanders, with the help of their staffs, make decisions and assume risks to balance competing requirements. For the nonservice retained teams, neither the commander nor the staff has administrative and operational control, nor are there structural mechanisms to prioritize and synchronize requirements. This oversight is reflected in resourcing and personnel. OPCON headquarters plan and direct operations the ADCON headquarters must fund. ADCON headquarters must also complete borrowed military manpower tasks that may directly conflict with operational requirements. Formally, no two headquarters simultaneously exercise the same command relationship on the unit. However, both headquarters effectively exert tactical control–like control, violating the principle of unity of command. Company commanders, detachment commanders/team leads, and battalion/brigade leaders can find ways to overcome these challenges and make missions happen. Based on individual personalities, their successes are achieved by overcoming structural impediments rather than being enabled by structure and processes.

Balancing operational and administrative requirements and having multiple headquarters imposing requirements is not unique to the Army's cyber forces. The scale of requirements, the echelons involved, persistence, and the evolving nature of cyberspace and the cyber force make it increasingly onerous. This imbalance manifests in two ways. First, the requirements of the administrative

[19] HQDA, *Army Command Policy*, AR 600-20 (Washington, DC: HQDA, July 2020), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN30074-AR_600-20-000-WEB-1.pdf.

[20] Leonard Wong and Stephen J. Gerras, *Lying to Ourselves: Dishonesty in the Army Profession* (Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2015), https://press.armywarcollege.edu/monographs/466.

headquarters exceed personnel support. While some units, like those supporting the National Security Agency, need only provide an administrative structure for detached personnel, Army cyber units must provide a mix of administrative and operational support. Cyber units must conduct individual and collective training for which the OPCON headquarters may have limited understanding, responsibility, or capacity. Additionally, the Cyber branch is small and continually evolving. As a result, the demands by operational forces for the continual development of capabilities, doctrine, organization, and training often fall to administrative headquarters. These practical demands exceed the scope and capacity intended for administrative headquarters and exacerbate the challenges of balancing requirements.

Second, cyber elements often lack intermediate supporting organizations like a division or corps staff. Enduring operational control of cyber detachments, typically led by a major or lieutenant colonel, is given to headquarters at echelons above corps, like a combatant command, while administrative control is retained by a brigade. In contrast to units like the 82nd Airborne Division, which might be operationally aligned to a combatant command, these cyber detachments lack the usual echelons of staff between a combatant commander and a detachment. In more typical force structures, these absent echelons would balance requirements across time and units. Instead, this responsibility falls to the team leads of cyber detachments with an authorized strength of around 39 personnel, though rarely fully manned, and with minimal redundancy in work roles. As a result, the persistently aligned detachments have little flexibility in how they allocate requirements to their personnel without deployment cycles or reset phases to provide time-based prioritization. Thus, the responsibility for balancing operational and administrative requirements has devolved to detachments lacking the capacity to do so, ensuring the problem persists.

This divided chain of command challenges normal Army processes. An administrative chain of command with no formal role in operations executes ratings, evaluations, awards, and other administrative processes. Contrary to the normal application of Army regulations, a line company commander is not the highest ranking regularly assigned officer. A company may have as many as five field-grade officers rated by the battalion or brigade commander and operationally controlled by a completely separate organization.

Soldier issues take on added complexity as the commander is less synchronized with operational requirements and must coordinate with multiple layers of leaders. The nuanced interplay of responsibility and authority between team leadership and company commander complicates the delegation and oversight of command responsibilities and can result in lieutenants and junior noncommissioned officers missing key developmental experiences. Supporting and enabling functions, already ill-defined for cyberspace, are further complicated by decisions regarding whether something is an ADCON or OPCON function and the differing channels for each. Further complicating the situation, most teams are externally controlled and actively on the mission, so there is no "garrison" time between deployments to complete ADCON requirements, leaving soldiers pulled between completing administrative tasks and executing the mission.

Most concerning are the operational challenges these command relationships impose. First, they can hinder organizational energy. Competing requirements and nonstandard processes require more communication and reporting and reduce the availability of personnel for operational requirements. Second, these relationships can reduce operational integration. Intent varies with commanders, making disciplined initiative across elements challenging. With convoluted chains of command, coordination may be slower or not happen because the correct information did not get to the right person. Since these command relationships lack support relationships or even full staffs, the command and operations (S3/G3/J3) channels provide the primary means of communication and often become overwhelmed. Similarly, it becomes less likely that the person making decisions and handling prioritization has all the information. This problem extends beyond the mission cycle into how we build and maintain combat power in the cyberspace domain.

Considerations for Mitigation

Cyberspace as a domain is constantly evolving, but many of these challenges are not. Artillery and logistics elements struggle with aligning by function or as integrated teams. Special forces frequently operate as independent small teams integrated with other organizations and headquarters with the goal to enable unity of effort, ultimately a matter of mission command. Commanders across the Army with complex command structures struggle to solve problems at the lowest echelon. The principles below can guide how we reassess our current force structures based on operational experiences to enable mission command in a modern cyber force.

Embrace the Principles of Unit Integrity

According to the Army's foundation doctrine for command and control, "[w]henever possible, commanders should task-organize based on standing headquarters and habitually associated groups."[21] For instance, if an operation requires two teams, those teams should be from the same company. This principle

[21] HQDA, *Mission Command: Command and Control of Army Forces*, ADP 6-0 (Washington, DC: HQDA, July 2019).

also applies to administrative tasks, which can reduce reporting requirements and ensure that nontasked units remain organically capable of accomplishing assigned missions; simplifying command and control; and reducing duplication, gaps in effort, and coordination requirements. We can use the command relationships of organic, assigned, and attached to preserve unit integrity but must carefully assess the long-term situation and costs to ensure the most effective structure is codified and unnecessary organizational chaos is not imposed.

Integrate Supporting and Enabling Functions

From property acquisitions to intelligence support, a variety of functions support cyberspace operations. These functions, however, cannot reside at every echelon. Instead, a clear process to coordinate and integrate support up and down echelons must be established. In conjunction with the previously recommended push toward unit integrity, clearly defined support relationships will ensure coordination for the gaps and overlaps in requirements.

Systemically Deconflict Requirements

Deployments provide clear transitions that shape unit priorities, distinguishing between training cycles, conducting operations, and synchronizing readiness cycles. While physical deployments might not be the right answer, time-based deconfliction measures (such as "mission windows," "long range training calendars," and "red, amber, green cycles") could be useful. The mechanism(s) should include the purpose, be acceptable to ADCON and OPCON, meet readiness and operational priorities, and clarify the responsibilities of the different headquarters, including operational support and reporting.

Provide Commander Latitudes in Execution

Unity integrity, clarity on roles and responsibilities, and channels for elevating support enable unit leaders to operate effectively. Units must also have the latitude to employ their resources optimally. Combining resources with latitude in execution, enables decentralized execution and the exercise of disciplined initiative. The emphasis on purpose in mission orders supports this principle. Providing units more time to complete requirements allows commanders to sequence priorities effectively and determine the force levels required to accomplish a mission, enabling more efficient use of personnel.

The Path Forward

The Cyber branch has grown in scope since its initiation and has not adjusted to meet the expanded needs of the Army, which now include electronic warfare, billets in the multi-domain task forces, billets in corps units and below, and the 915th Cyberspace Warfare Battalion. Military leadership should approach the recommendations made with a view toward the long-term growth of the Cyber branch to prevent repeating past mistakes. The Cyber branch must develop individuals with electronic-warfare knowledge, skills, and behaviors, and existing personnel should serve in units and on missions outside the 780th Military Intelligence Brigade and the Cyber Protection Brigade. Additionally, the Cyber branch must continue to recruit and integrate officers from other branches through the voluntary transfer incentive program. Acknowledging the manifest challenges in the existing cyber organizations can assist the successful development of the newly established portions of the branch.

With a broader scope, the potential to mismanage specialization increases. It becomes less plausible that officers can achieve competency in offensive, defensive, and electronic warfare mission sets, especially if they become cyber officers four or more years into their careers. For warrant officers and enlisted soldiers, growth represents additional specialization. A single billet, or even a limited number of billets, cannot bring mastery of all branch functions. Similarly, members of the branch cannot achieve advanced competency without specialized training and assignment. The branch must carefully consider its doctrine, organization, and training to ensure sufficient specialization and mastery while maintaining adequate integration across these specializations to deliver maximal effects.

The growth in the Cyber branch's scope will also have implications for the complex chains of command, introducing additional headquarters and longer coordination chains. The cyber billets have a relatively low density in the field Army and provide a limited set of organic capabilities for commanders at those echelons. Instead, capabilities will often be integrated or assigned from higher headquarters. Authorities, network ownership and visibility, and MOS density dictate that this integration must occur with the already complex chains of commands within Army Cyber Command, the 780th Military Intelligence Brigade, and the Cyber Protection Brigade. If unresolved, these complexities will affect combat power. Cyber personnel in noncyber units will duplicate capabilities available to other echelons or be unable to integrate and mass sufficient capabilities effectly. A revised modern cyber force structure that applies the principles outlined in this article will better equip the Army to meet the needs of multi-domain operations and beyond.

John Fernandes
Major John Fernandes, US Army, is a cyber officer and research scientist at the Army Cyber Institute. He holds a Master of Science degree in computer science from the University of Massachusetts.

Nicolas Starck
Major Nicolas Starck, US Army, is a cyber officer and research scientist at the Army Cyber Institute. He holds a Master of Science degree in electrical and computer engineering from Carnegie Mellon University.

Richard Shmel
Captain Richard Shmel, US Army, is a cyber officer and research scientist at the Army Cyber Institute. He holds a Master of Science degree in electrical engineering from the Naval Postgraduate School.

Charles Suslowicz
Major Charles Suslowicz, US Army, is a cyber officer and research scientist at the Army Cyber Institute. He holds a Master of Science in Computer Engineering from Virginia Tech.

Jan Kallberg
Dr. Jan Kallberg, US Army, is an assistant professor and research scientist in the Insider Threat Research Program, Department of Mathematical Sciences, at the United States Military Academy.

Todd W. Arnold
Lieutenant Colonel Todd W. Arnold, PhD, US Army, is a cyber officer and academy professor at the Army Cyber Institute and an assistant professor, Department of Electrical Engineering and Computer Science, at the United States Military Academy.

Select Bibliography

Center for Strategic Leadership. *Strategic Cyberspace Operations Guide*. Carlisle, PA: US Army War College, August 2021. https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf.

Chesney, Robert. "The Domestic Legal Framework for US Military Cyber Operations." Hoover Working Group on National Security, Technology, and Law. Aegis Series Paper No. 2003. Stanford, CA: Hoover Institution, July 2020. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3668463_code119080.pdf?abstractid=3668463&mirid=1.

Fernández-Salinero, Samuel, and Gabriela Topa. "Intergroup Discrimination as a Predictor of Conflict within the Same Organization: The Role of Organizational Identity." *European Journal of Investigation in Health, Psychology and Education* 10, no. 1 (May 2019): 1–9, https://www.mdpi.com/2254-9625/10/1/1/pdf?version=1585805094.

Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs,* September/October 2010, https://www-foreignaffairs-com.usawc.idm.oclc.org/articles/united-states/2010-09-01/defending-new-domain.

Pomerleau, Mark. "Cyber Command's Force Is Growing, in Part, to Support Space." FEDSCOOP (website). April 8, 2022. https://www.fedscoop.com/cyber-commands-force-is-growing-in-part-to-support-space/.

Wong, Leonard, and Stephen J. Gerras. *Lying to Ourselves: Dishonesty in the Army Profession*. Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2015. https://press.armywarcollege.edu/monographs/466.