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

RESEARCH ARTICLE

Evaluating Alternative Models for Organizing U.S. Cyber Forces

Nick Starck*, Todd Arnold

Army Cyber Institute, West Point, NY, USA

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

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

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

INTRODUCTION

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

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

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

This work is meant to provide such an outside-the-box evaluation, critical to designing the best way to generate cyber forces to compete with peer adversaries like China and Russia. Our analysis is grounded in the assumption that cyberspace is its own distinct domain (Lonergan and Montgomery 2024). This domain has been repeatedly defined as having its own operational logic (Alexander 2011; DoD 2022; Conti and Raymond 2017). We therefore

assume that it requires force generation distinct from other domains. This challenge includes competing for technical expertise that is in high demand elsewhere in the economy.

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

MODEL SELECTION AND ANALYTICAL CRITERIA

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

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

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

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

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

ANALYSIS OF MODELS

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

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

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

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

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

Table 1. Summary of Analysis of Organizational Models

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

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

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

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

Defense Combat Support Agencies

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

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

Like the PHSCC, CSAs offer a practical model for generating and employing a technical workforce that could integrate with popular proposals for cyber forces. As an existing model within the military, CSAs have a long history of successful support to and integration with the joint community in sustained, global operations. Additionally, they enable personnel management and the development of expertise in a tailored field. In particular, the NSA has demonstrated the capacity to develop and maintain a world-leading technical workforce that serves as the vital foundation and continued partner to USCYBERCOM. This success suggests

that the ratio of civilian to military employees within the cyber workforce may not need to reflect the military-heavy proportions typical of the existing armed services. Finally, CSAs have provided reliable support to both combatant commands and, in the case of the NSA, the enduring requirement for national intelligence collection.

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

Specialized Career Paths

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

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

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

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

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

Private Sector Approaches

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

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

Workforce development within private industry offers several significant lessons for military cyber force generation. The emphasis on strong relationships with academia to identify

and recruit students creates a robust pipeline for talent. Internship programs supplement scholarship with practical experience that can be leveraged as future employees. Further, the willingness of private companies to be highly selective, leaving positions unfilled rather than hiring someone who would be a bad fit, underscores the often-overlooked but negative impact on overall performance that can result from trying to grow a technical workforce without regard to talent, culture, and other factors.

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

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

CONCLUSION: DRAWING OUT LESSONS FOR MILITARY CYBER FORCE GENERATION DECISIONS

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

technical competence – both in initial selection and in continued professional advancement. The nature of that technical competence may evolve over the course of a career. Nevertheless, maintaining a strong technical foundation is instrumental to effective operations through shared organizational cultures.

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

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

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

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

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

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

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

ABOUT THE AUTHORS

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

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

ACKNOWLEDGMENTS

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

REFERENCES

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

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

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

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

DiCarlo, James. 2024. "Unveiling the Significance of the Army's Training with Industry Program," July 18, 2024. https://www.army.mil/article/277269/unveiling_the_significance_of_the_armys_training_with_industry_program.
DoD (Department of Defense). 2010. "Department of Defense Directive 5100.01: Functions of the Department of Defense and Its Major Components." https://dam.defense.gov/Portals/47/Documents/PDSD/510001p2.pdf.
DoD (Department of Defense, Joint Chiefs of Staff). 2022. *JP 3-12: Joint Cyberspace Operations.*
DoW (Department of War). 2025. "Department of War Establishes CYBERCOM 2.0 – Revised Cyber Force Generation Model," November 6, 2025. https://www.war.gov/News/Releases/Release/Article/4330204/department-of-war-establishes-cybercom-20-revised-cyber-force-generation-model/.
Freilich, Charles D., Matthew S. Cohen, and Gabi Siboni. 2023. *National Capacity Building, Israel and the Cyber Threat: How the Startup Nation Became a Global Cyber Power.* Oxford Academic.
King, Andrew. 2025. "Why America Needs a Dedicated Cyber Force Now | Opinion." Newsweek, April 2, 2025. https://www.newsweek.com/why-america-needs-dedicated-cyber-force-now-opinion-2053910.
Lonergan, Erica, and Mark Montgomery. 2024. *United States Cyber Force: A Defense Imperative.* Foundation for Defense of Democracies. https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf.
Luttrell, Morgan. 2024. "The time is right for a new military force to defend cyber space." Defense News, May 21, 2024. https://www.defensenews.com/opinion/2024/05/21/the-time-is-right-for-a-new-military-service-to-defend-cyber-space/.
Martin, Alexander. 2025. "British military drops basic training to fast track recruitment of 'cyber warriors'," February 10, 2025. https://therecord.media/british-military-drops-basic-training-to-fast-track-cyber-recruits.
Matishak, Martin. 2024. "After prodding from lawmakers, Cyber Command readies a plan for the future," October 22, 2024. https://therecord.media/cyber-command-2-0-project-progress-military-congress.
PHSCC (U.S. Public Health Service Commissioned Corps). n.d. "Officer and Student Training Programs." Accessed July 31, 2025. https://www.usphs.gov/students/.
Pomerleau, Mark. 2025. "DOD leadership asks for CYBERCOM 2.0 relook." DefenseScoop, May 20, 2025. https://defensescoop.com/2025/05/20/cybercom-2-0-relook-dod-leadership/.
Seffers, George I. 2025. "Cyber Command 2.0 Eyes Creation of a Cyber Innovation Warfare Center," April 2, 2025. https://www.afcea.org/signal-media/cyber-edge/cyber-command-20-eyes-creation-cyber-innovation-warfare-center.
Townsend, Kevin. 2018. "From IDF to Inc: The Israeli Cybersecurity Startup Conveyor Belt." SecurityWeek, February 28, 2018. https://www.securityweek.com/idf-inc-israeli-cybersecurity-startup-conveyor-belt/.
U.S. Air Force Institute of Technology. 2025. "Education With Industry Program," July 31, 2025. https://www.afit.edu/CIP/page.cfm?page=1567.
U.S. Air Force Public Affairs. 2022. "Career Intermission Program application window opens April 1, reduces service obligation," March 28, 2022. https://www.spaceforce.mil/News/Article/2980107/career-intermission-program-application-window-opens-april-1-reduces-service-ob/.
U.S. Army Talent Innovation Division. 2025. "Direct Commissioning." Accessed July 31, 2025. https://talent.army.mil/direct-commissioning/.
U.S. Code 10 § 101. https://www.law.cornell.edu/uscode/text/10/101.
U.S. Code 37 § 301(d). https://www.law.cornell.edu/uscode/text/37/301d.
U.S. Code 37 § 302. https://www.law.cornell.edu/uscode/text/37/302.
U.S. Code 42 § 209. https://www.law.cornell.edu/uscode/text/42/209.
U.S. Code 42 § 211. https://www.law.cornell.edu/uscode/text/42/211.
U.S. Congress. 2018. *National Defense Authorization Act for Fiscal Year 2019.* https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.
U.S. Congress. 2025. *Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Section 1544.* https://www.govinfo.gov/content/pkg/PLAW-118publ159/pdf/PLAW-118publ159.pdf.

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