Beyond USCYBERCOM: The Need to Establish a Dedicated U.S. Cyber Military Force

COL Jeffrey Couillard

ABSTRACT

This paper explores whether the United States should establish a separate Cyber Military Force. The article begins with a brief review of current cyber threats to the United States, followed by a review of historical precedent and great power competition. It then analyzes the current cyber military structure to help identify potential gaps within the current approach to offensive and defensive cyber operations. To provide a possible course of action in the context of a recommended framework, the article proposes using a well-known military framework called DOTMLPF-P (Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities, and Policy). The methodology used is a qualitative literature review, including journal articles, military doctrine, historical references, subject matter expert articles, U.S. Government Accounting Office reports, cyber industry reports, and legislation. The research aims to bring readers to the conclusion that it is time to establish a separate U.S. Cyber Force.

Keywords *– Cyber, Cyber Defense, Cyberspace, National Security Strategy, National Cyber Strategy, Cyber Domain, Department of Defense*

INTRODUCTION

In 1947, President Harry S. Truman signed the National Security Act.[1] This act made numerous changes to the nation's defense and intelligence organizations including the establishment of the Department of the Air Force. In 2019, President Trump signed the National Defense Authorization Act (NDAA)[2] establishing the U.S. Space Force as a component under the Department of the Air Force, after roughly twenty years

Colonel Jeffrey (Jeff) Couillard is a war college graduate of the College of Information and Cyberspace at the National Defense University. He started his Army career as an enlisted Infantryman in 1988. He received a direct commission to the Signal Corps in 2005. During his 35 years of service, he has commanded at the company level and led a Regional Cyber Center. In addition to his command and leadership assignments, Colonel Couillard has served on staff at Headquarters, Department of the Army, the Army National Guard Bureau, Multi-National Forces – Iraq, and Joint Task Force Guantanamo. Colonel Couillard has been deployed numerous times, in support of Operation Desert Shield/Storm, Operation Iraqi Freedom, and Operation Enduring Freedom. He earned a Bachelor of Business Administration degree from Davenport University; a Master of Arts from Webster University; and a Master of Science from the College of Information and Cyberspace.

of effort and a congressional report on Space Matters.[3] This aligned a dedicated organization to the Space Warfighting Domain. The FY23 NDAA directed a Department of Defense (DoD) report on Cyber Matters,[4] echoing an FY00 DoD report on Space Matters.[5] The topic of Cyber Matters within the NDAA covers a wide range of questions, including total force generation.[6]

The question of a Cyber Military Force is not new, although most studies lack practical solutions.[7] The research details multiple problems but falls short of proposing actionable solutions. This article explores the requirement to establish a separate U.S. Cyber Military Force, detailing threats, precedent, and current gaps. Finally, the author provides a framework for the DoD to recommend Congress establish a separate U.S. Cyber Military Force.

Some suggest, including the former Commander of U.S. Cyber Command (USCYBERCOM), General Paul M. Nakasone,[8] that there is no need to establish a separate Cyber Military Force. When asked by U.S. Representative Pat Fallon, during the House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems, if Gen. Nakasone would "...accept command of a cyber service?"[9] Gen. Nakasone responded with the following:

> So Congressman, I would offer that you know that is obviously as you said a policy decision, but let me just provide a thought on this in terms of how we model ourselves and I think as you asked a number of different who (is)...in charge of special operations? Special Operations is not run by any specific service yet it is the lead service and capability that our nation has. That's what we have modeled ourselves at U.S. Cyber Command (after). This idea of having special and unique authorities that we're able to train and man and equip our force and agility to maneuver.[10]

This article counters Gen. Nakasone's view by highlighting the distinct need for cyber defense. Unlike U.S. Special Operations Command's (USSOCOM) non-permanent defensive role, USCYBERCOM must continuously defend the Department of Defense Information Network (DoDIN), the world's largest network.[11] Additionally, USSOCOM specializes in small-group tactics, offensive operations, and providing specialized training. While small-group tactics may work for Cyber Protection Teams (CPTs) responding to cyber-related incidents, it is not applicable to defending a global network.

This article proposes using the DOTMLPF-P (Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities, and Policy) framework to analyze and develop a Cyber Military Force, not as a panacea but as a starting point.

Threats

In March 2022, the Federal Bureau of Investigation's (FBI) Internet Crime Compliant Center (IC3) released its 2021 Internet Crime Report[12] showing a year-over-year increase in Internet Crime between 2017 and 2021, roughly a 68% increase each year. The total reported losses for 2021 were $6.9 billion.[13] Applying that same 68% increase to 2022 and 2023, the anticipated losses could be $11.6 billion and $19.5 billion, respectively. A way to reduce those losses is by identifying those supporting internet crime and cyber-attacks. Within the FY22 National Defense Strategy, the Pentagon stated that "China remains the 'pacing challenge'" and "identifies Russia as an 'acute threat.'"[14] Additionally, the Cybersecurity & Infrastructure Security Agency (CISA), under the Department of Homeland Security (DHS), published to their website Alerts (AA22-110A)[15] and (AA22-279A)[16] pointing to Russian and Chinese state-sponsored cyber threats. Continuing to pull that thread, North Korea and Iran both rise in relevance as state sponsors in CISA Alerts (AA22-187A)[17] and (AA22-320A).[18]

However, it is not just state-sponsored actors conducting these attacks. Mieke Eoyang, the Deputy Assistant Secretary of Defense for Cyber Policy, is quoted as saying,

> But I think we've seen over time with the development of the non-state actor – the criminal cyber market – is that capabilities that were once reserved for state actors are available on the dark web for purchase."[19]

According to Eoyang, the criminals "...are motivated by money." She said. "They're in it for the ransom. They're not necessarily in it for harming [the United States.]"[20]

What does this mean to the cyber defense of the United States? According to a September 2022 U.S. Government Accountability Office (GAO) report on Opportunities and Threats to the DoD's National Security Mission, the GAO found:

> Given the ubiquitous nature of the information environment, both DoD and adversaries can conduct operations and activities in the information environment from anywhere in the world. Additionally, with DoD capabilities dependent on IT and the electromagnetic spectrum (EMS), its ability to conduct operations and activities in any of the physical domains (land, maritime, air, and space) is reliant on protecting the information environment.[21]

Specific to threat actors, the GAO report offered that "National and DoD strategies recognize that nation-states...have demonstrated that they are threat actors in the information environment..."[22] Of the institutional challenges, the GAO report continues with:

> The challenges include a lack of leadership emphasis, lack of resources, the implications of new technologies, and dated processes. DoD components identified personnel, funding, IT, organization, and training as the most important institutional challenges they face related to the information environment.[23]

From the GAO report, with the specific details above, one can understand that the DoD and its components are not focusing on the cyber domain as much as necessary, which is critical to the other four warfighting domains.

Precedent for Organizing the Cyber Mission in DoD

From the time of Brigadier General Billy Mitchell in World War I to the 1947 National Security Act, which established the U.S. Air Force, aviators had continuously struggled to convince the U.S. Army that Air Power was more than a supporting effort to the land warfighting domain. In his doctoral thesis Dr. James P. Tate, Lt. Col. U.S. Air Force (Retired) stated, "Within the Army it was the conflict over budget as much as anything else that fueled the Air Corp's drive for independence."[24] Tate also includes in his thesis the congressional testimony of several aviators stating:

> During the hearings, the points of the airmen's argument emerged. The flyers argued that there were military missions for the air arm independent of the surface forces; that the airplane had an almost unlimited potential as a weapon; that the full power of the airplane could be reached only by an air arm controlled by men with knowledge and interest in aviation; that the leadership of the Army, especially the General Staff, lacked interest and knowledge in aviation and had subordinated the needs of the air arm to those of other combat arms; that a separate air service would prevent expensive duplication by concentrating the government's aviation activities under central control; that such an independent air service had been successful in Britain; and finally, that development of aviation under an independent air service would provide support, direction, and encouragement for the country's aviation industry which depended so heavily upon the military market. The best way to take advantage of the new technology in aviation was to create a new military organization.[25]

Within the above quote, one could easily replace "air" and "airplane" with "cyber" and present the same compelling argument. Of note, for use later, is the concept of the Air Force supplying pilots and support to the U.S. commercial air sector. Again, replacing "air" with "cyber" is something to remember when talking about the deficit of cyber talent for positions available within the United States.

Lastly, from Tate's thesis, "Congress passed the National Defense Act of 1920, which gave permanent legislative authority to the Air Service..."[26] Additionally, "The Air Service received authority to procure equipment."[27] Similarly, as Mark Pomerleau details in a Defense Scoop article, the FY22 National Defense Authorization Act "granted Cybercom enhanced budget authority... to maintain the cyber mission force."[28] It appears USCYBEROM is already following the same steps the U.S. Air Force took to separate from the U.S. Army.

Some suggest that a Cyber Military Force should mirror the development of the U.S. Air Force before founding Cyber as a separate military service. Of significance, the U.S. Air Force was established after World War II (WWII). This was a time when the nation was recovering from the war and the world was generally at peace, so the focus turned to reorganizing defense and intelligence organizations, including establishing the U.S. Air Force. Today, there is no similar armistice or peace treaty to end the ongoing cyberattacks commonly described as operating just below the threshold of armed conflict.

Additionally, if one uses the FY00 NDAA as the starting point, it took nearly twenty years to establish the U.S. Space Force. The FY00 National Defense Authorization Act (NDAA) compelled the DoD to produce a Report of the Commission to Assess United States National Security Space Management and Organization.[29] This report detailed how to establish a U.S. Space Force. Similar to the request for the report on Space Matters in the FY00 NDAA, Congress included language in the FY23 NDAA compelling the DoD to address the question of cyber matters.

The U.S. is not the only nation to establish new cyber military organizations. The German government created its Cyber Military Force in 2017. They established the organization to counter challenges perceived within the cyber domain. According to a recent German report, the German Cyber Military Force includes Cyber Security, Infrastructure, Intelligence, Applications, IT Management, Project Management, and Enterprise Architecture.[30] The German Cyber Military Force also conducts the organize, train and equip mission, providing a cyber-specific career pipeline. In 2022, this force began an effort to restructure based on experiences gained from the previous five years of operations.

Similarly, on October 28, 2022, Singapore established its cyber-focused Digital and Intelligence Service (DIS). According to Mike Yoe, an Asia correspondent for *Defense News*, the intel directorate within DIS,

> will support Singaporean military decision-making and operations through research and analysis, doctrines, standards, and best practices...

The article continues,

> (t)he DIS will also have four separate commands, plus a digital operations technology center. The four commands are tasked with joint intelligence, C4 [command, control, communication, and computers] cybersecurity, digital defense and training.[31]

In 2015, China established the Strategic Support Force (SSF) to consolidate their space, cyber, and electronic warfare (EW) efforts under a single unified force. According to Elsa B. Kania and John K. Costello,

> ...the SSF has integrated the PLA's [People's Liberation Army] capabilities for cyber, electronic, and psychological warfare into a single force within its Network Systems Department, which could enable it to take advantage of key synergies among operations in these domains.[32]

Relative to China's cyber force, in 2017 RAND Corporation published a report on "The Creation of the PLA Strategic Support Force (SSF) and Its Implications for Chinese Military Space Operations."[33] While focusing on space, the RAND report highlights that "The SSF is charged with overseeing Chinese military space, cyber, and electronic warfare capabilities..."[34] Within the report, RAND interviewed former Second Artillery officer, Song Zhongping of the PLA who said, "... that the SSF is an independent service 'unique in the world'." Song continues, "The goal of the SSF is to achieve cyber and electromagnetic superiority."[35] If China is the main competitor in global power competition, the SSF already has an eight-year lead maturing tools and tactics.

The Wrong Structure for the Job

Information Technology systems evolve over time. Information Technology support groups have iteratively reinvented themselves to react to that evolution. The same is true of IT organizations within DoD. In the U.S. Army, IT organizations have included: Data Processing, Information Systems and Support, Department of Information Management, Network Enterprise Centers, Theater Network Operations and Security Centers, and Regional Cyber Centers (RCCs) to name a few. One could assume the same to be true of the other services within the DoD, as it certainly is with USCYBERCOM as shown on their website history page.[36] USCYBERCOM is a functional combatant command, like U.S. Strategic Command (USSTRATCOM) and U.S. Transportation Command (USTRANSCOM), but supports global cyber operations for all DoD and all combatant commands. The Commander of USCYBERCOM is also the Director of the National Security Agency (NSA). Within USCYBERCOM are the Cyber National Mission Force (CNMF) and Joint Forces Headquarters – DoDIN (JFHQ-DoDIN). The Commander of JFHQ-DoDIN is also the Director of the Defense Information Systems Agency (DISA), an agency within the DoD (Figure 1).[37]

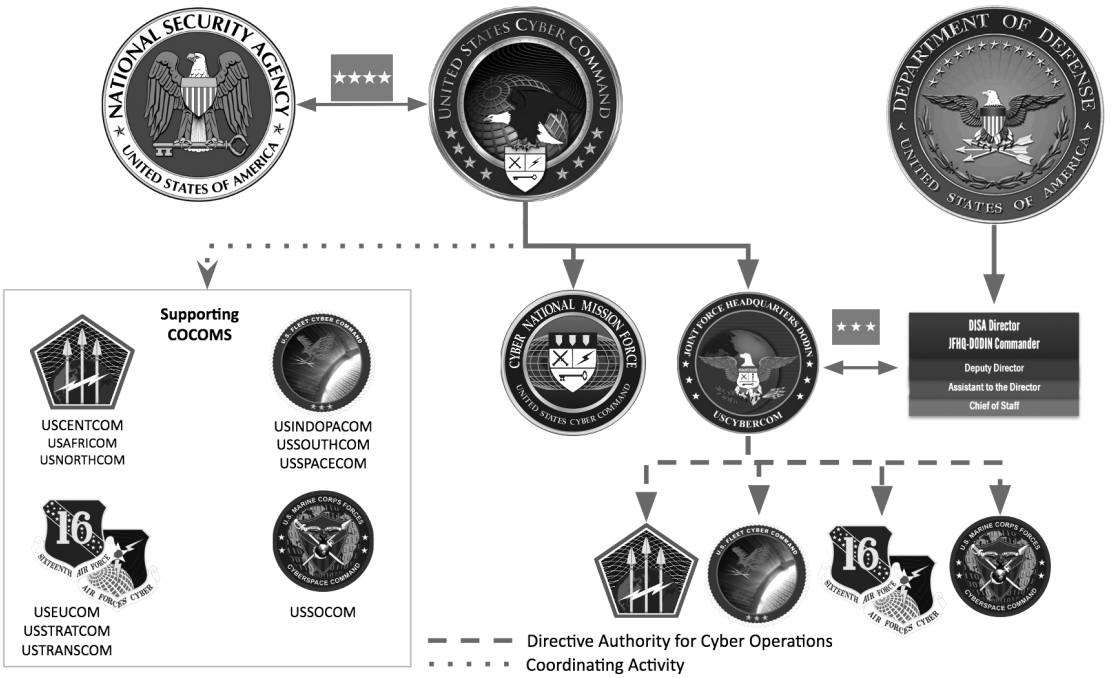

Figure 1: U.S. Army IT Organizations.

While the above figure shows some of the complexity, it is only the beginning. According to Maj. Eric Pederson, Maj. Don Palermo, Maj. Stephen Fancey, and Lt. Cdr. (Retired) Tim Blevins "The DoDIN is the biggest network in the world..."[38] and "...is composed of 44 different DoD components (and) constructed networks[39] across approximately 3,500 locations in 26 nations."[40] Just within the Army there are six RCCs, aligned with the Continental United States (CONUS), Europe, Pacific, Southwest Asia, Korea, and the National Guard. The RCCs support their portion of the DoDIN, including the Joint Regional Security Stacks (JRSS) provisioned by DISA. As shown in Figure 1, the various service Cyber Commands each support a Geographic Combatant Command. Although, even with that support, in 2023, U.S. Indo-Pacific Command (USINDOPACOM), according to the C4ISRNET website, "asked Congress for an additional $274 million to fund offensive and defensive cyber capabilities."[41] Of note, each service cyber command approaches its assigned combatant commands with different tools, methods, policies, and procedures.

Combatant Commanders rely on IT infrastructure to enable all aspects of operations and support (pay, health care, personnel actions, logistics, etc.). Each Combatant Commander's IT infrastructure becomes the defensive position the DoD must protect for orchestrating multi-domain operations. Additionally, that infrastructure is a regional portion of the global DoDIN. The greater the number of organizations charged with defending sections of that IT infrastructure, the greater the chances for holes in those defenses.

At some point, the scope of managing those defenses becomes clouded with bureaucracy. For example, suppose a security vendor discovers a new zero-day exploit. That security vendor alerts the producer of the product about the vulnerability. The producer then works to develop a patch. The producer alerts the public and, by proxy, the DoD. USCYBERCOM takes the lead and pushes an order to JFHQ-DoDIN. JFHQ-DoDIN then produces an order directing service agencies connected to the DoDIN to implement the patch. In the case of the Army, U.S. Army Cyber Command (ARCYBER) receives the order and produces a separate order to U.S. Army Network Enterprise Technology Command (NETCOM). NETCOM digests the ARCYBER order, issues any Requests for Information (RFIs) for clarification, then issues a NETCOM order to all six RCCs and Theater Signal Commands. The Theater Signal Commands in turn issue their own orders to subordinate Signal brigades, which manage the Network Enterprise Centers (NECs) at each base, post, camp, and station (collectively called posts). The NECs manage the IT infrastructure contained within each post.

When viewing defensive capabilities, the structure is inefficient and ripe for missing key linkages to ensure appropriately hardened enterprise defenses. Simply consolidating key elements, along with JFHQ-DoDIN, DISA, and the six Army RCCs into a single Cyber Military Force while properly aligning the budget to address the lifecycle requirement of equipment across the DoDIN, down to the customer edge equipment, could streamline operations and ensure a stronger defense.

Force Design

Congress compelled the DoD to answer "Cyber Matters" in the FY23 NDAA – specifically in section 1533.[42] This is probably one of the most challenging tasks to "compel" based on the complexity, dispersion, authorities, service requirements vs. domain requirements, and lexicon used across the services within the DoD. Yet this task is critical, as the previously discussed GAO report stated, "It's [the DoD's] ability to conduct operations and activities in any of the physical domains (land, maritime, air, and space) that is reliant on protecting the information environment."[43] This study will use the DOTMLPF-P framework to address the scope of this problem. Organizational change is hard. It is apparent from the above that the Air Force and Space Force broke away from their parent services to prioritize niche warfare capabilities. Both services have focused on doctrine, equipping, and funding, enabling them to fully explore and implement domain-specific capabilities.

Cyber Doctrine: The Challenge of Parent-service Bias

The U.S. Army writes doctrine specific to supporting operations in the land warfighting domain. With this focus, the U.S. Army should not be the primary entity responsible for developing cyber doctrine for the cyber warfighting domain. Similar to a statement offered in Dr. Tate's thesis, "The best way to take advantage of the new technology in aviation was to create a new military organization."[44] Cyber needs its own service to develop doctrine specific to warfighting in the cyber domain.

The U.S. Army has been developing doctrine for nearly 250 years, incorporating lessons learned from previous military engagements, as well as the theory and philosophy of warfare. The U.S. Army's capabilities and doctrine are forged to support its mission "To deploy, fight and win our nation's wars by providing ready, prompt and sustained land dominance by Army forces across the full spectrum of conflict as part of the joint force."[45] The Army also says its "mission is vital to the nation because we are the service capable of defeating enemy ground forces and indefinitely seizing and controlling those things an adversary prized most – its land, its resources and its population."[46] The emphasis on land warfare was another key factor in the Army Air Corps' need to separate from the Army, highlighting the specialized nature of each domain.

Currently, there is only one joint cyber doctrine manual for the cyber warfighting domain. This manual, influenced by the Army's focus on land warfare, provides only a basic understanding of cyber operations. A highly skilled team must actively analyze and integrate offensive and defensive capabilities specific to the cyber domain to support other warfighting domains and geographic combatant commanders while considering the actions of allies and adversaries. This approach mirrors the success achieved by the U.S. Air Force in developing air domain doctrine and provides a road map for cyber to do the same.

Organization

Establishing a cyber military service can be achieved with minimal personnel increases by consolidating existing organizations such as DISA, JFHQ-DoDIN, ARCYBER, parts of NETCOM, the six Army RCCs, and cyber staff from the Air Force, Navy, and Marines. However, current military services will still require organic cyber staff to meet their IT and cyber requirements and support for cyber activities. Additionally, non-cyber specialties like the Judge Advocate General (JAG), Intelligence, and Public Affairs, which focus on cyber aspects, must be integrated. These specialties, especially JAG, need a thorough understanding of their field's application in cyberspace, including national and international law relevant to U.S. defensive and offensive cyber operations.

The Department of the Army would be the most appropriate department to constitute this new cyber force. According to the U.S. Army Cyber Command website, "The Army was the first service to create cyber career fields for both Soldiers and Civilians."[47] Comparatively speaking, the Army has spent more time developing a greater cyber capability than other services. Additionally, the Department of the Air Force includes the the U.S. Space Force, and the Department of the Navy includes the U.S. Marine Corps. The Department of the Army does not currently have a similar military service component. However, like the U.S. Space Force, the new U.S. Cyber Force must have autonomy to allow for growth within the cyber domain.

The need for a separate cyber military force is not a new idea. James Stavridis, a U.S. Navy retired four-star Admiral, co-wrote an article with David Weinstein in 2014 on the need to establish a separate U.S. Cyber Force.[48] Stavridis makes several excellent points about the

reasons why there is a need for a separate cyber force, many included in this paper from other sources. However, Stavridis asserts that this separate force should remain constrained by the Posse Comitatus Act, like the U.S. Army. According to an article on the Brennan Center for Justice website, "The Posse Comitatus Act bars federal troops from participating in civilian law enforcement except when expressly authorized by law."[49] Domestic police activities are a key difference between U.S. Code Title 10 and Title 32 missions, where Title 10 is Federal and subject to Posse Comitatus, and Title 32 is a state National Guard mission.

A new U.S. Cyber Force, addressing national cyber threats across all sectors, must incorporate a National Guard component. In a cyber emergency, whether state or local government or private sectors, state or territory Governors could mobilize their National Guard Cyber forces upon request. These Guard units, equipped with the same training and tools as the full-time cyber force, offer the added benefit of being locally based in the states they serve.

The Guard Cyber force could offer immediate emergency response and support to local law enforcement. It could provide state-specific vulnerability assessments, reporting findings to the Governor. Additionally, these forces would aid their parent service's Title 10 missions, having the same training and equipment as the active-duty force, similar to the current Army and Air Guard. The Cyber National Guard could recruit volunteers from their local commercial industries. Some of these professionals are already part of state and territory-aligned CPTs. Integrating these CPTs into a separate cyber military force as the Cyber National Guard component would standardize training, equipment, and doctrine for both Title 32 and Title 10 missions.

Cyber Training: Lifelong Learning Culture

Training in today's military is generally based on the crawl-walk-run method to develop task-specific skills. For example, basic rifleman's marksmanship follows this construct. The crawl phase begins with fundamentals: body position and grip, sight picture, trigger squeeze, and breath control.[50] The walk phase covers disassembly, reassembly, a functions check, and dry-fire exercises. The run phase culminates with weapons qualification at a firing range.

Most skills-based training activities have applied the above training method. While designed for basic skills, this method fails to develop skills necessary for success in a dynamically evolving technical environment, like offensive and defensive cyber operations. In this case, the DoD should incorporate the concept of perishable skills. Reporter, Mark Gibson, references a book titled *A New Culture of Learning*, in which the authors Douglas Thomas and John Seely Brown suggest that "The half-life of a learned skill is 5-years."[51] With the continuous evolution of technology, half of what you learned 5 years ago is now obsolete.[52] However, in the basic rifleman's marksmanship example, firing a weapon system does not fundamentally change unless the basic weapon system changes. In the case of more technical

or professional-level skills, there must be a better way to address skill atrophy paired with the rapid evolution of technology and exploits in cyber.

Matthew J. Daniel, a principal consultant with Guild Education, described three distinct categories of skills, including: perishable skills (half-life of less than two and a half years), semi-durable skills (half-life of two and a half to seven and a half years), and durable skills (half-life of more than seven and a half years)."[53] This illustration provides a framework for building an adaptive training model.

This framework can be used to codify cyber training into durable, semi-durable, and perishable skills. Military history and traditions can be foundational and established as durable skills, giving new members the structure to identify with a specific military culture. The semi-perishable is equivalent to the basic rifleman's marksmanship skills – to maintain the "run" phase, you must continue to practice, but the skills will not become obsolete in short order. For perishable skills, there must be a revolution in training.

The DoD can revolutionize cyber training in two steps: First, teach cyber warriors essential skills for their specific roles. Second, provide biennial training to enhance and learn new skills. Initially, recruits attend a modified basic training on military conduct, history, performance, and expectations, coupled with six months of foundational cyber training. After their first 18-month assignment, they would attend a six-month study program, followed by another 18-month assignment. This four-year cycle would greatly enhance their technical skills. The cyber warrior could then progress from defensive to offensive operations, possibly reserving offensive training for those who re-enlist for another four years. Those leaving service after their first term would return home with substantial defensive cyber skills, enabling them to secure a well-paid career, indirectly bolstering the nation's cyber defense.

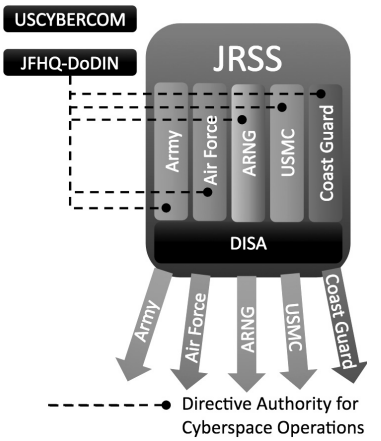

Figure 2: Multi-tenant Model.

Cyber Materiel: The DMARC

The current problems with Materiel include issues with both offensive tools and especially with defensive tools. In this context, “materiel” is the hardware or software solution provided to satisfy unit or mission requirements. For example, if the requirement is to view data crossing a network, the materiel solution might be packet capture software installed on a government-provided computer. In the FY22 NDAA, USCYBERCOM received enhanced budget authority.[54] This is a good start, but the U.S. military needs much more. Each of the services has procurement authority for both offensive and defensive cyber tools, leading to each service doing its own thing. For defensive tools, the cyber terrain is even more

complicated with the DISA providing Information Systems and Services to the various military branches.

A case in point is JRSS. DISA is currently working to replace JRSS with a project named Thunderdome.[55] The benefit of JRSS was the eventual capability of a rich suite of equipment and systems built specifically to secure the Non-Secure Internet Protocol Router (NIPR) portion of the DoDIN. The problem is the multi-tenant model (Figure 2)[56] DISA employes for its customers.

DISA retains advanced access to the systems within JRSS but does not manage them. DISA provisions virtual space for each customer within JRSS providing customers with a graphical user interface (GUI) to manage their virtual space across JRSS. This includes access to advanced tools for monitoring alerts, traffic volume, and troubleshooting traffic flow, immediately requiring each customer to have staff capable of using the DISA tools within JRSS. Those tools may be significantly different than what the military services had been using within their own environments. Additionally, DISA did not originally provide any formal training for the tools in JRSS. Further complicating JRSS was the cumbersome process used to gain access to manage JRSS.

Using JRSS as a model, a single cyber-service would excel by providing a single point of contact and standardized management across JRSS. Combining key defensive cyber elements from each of the military services, along with JFHQ-DoDIN and DISA, would allow for a single service to manage the DoDIN (using NIPR as the example) down to and including the customer edge router. Doing so would allow for a single service provider to have end-to-end visibility across the DoDIN with a team fully trained to use the defensive tools provided (Figure 3),[57] while dramatically reducing redundant support forces across the services.

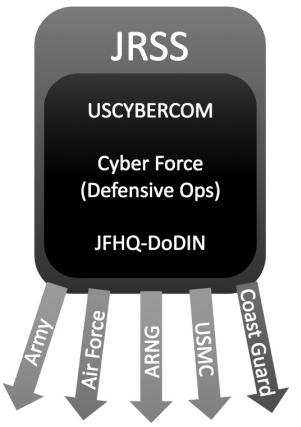

Figure 3: JRSS Model.

Additionally, this would allow for the rapid migration to future technology to enable greater capacity and throughput across the DoDIN. If a single service owned the security stacks across DoDIN, the circuits connecting each base, post, camp, station, state, ship, airbase, and customer edge router, that service could gain economies of scale when upgrading or migrating systems. This would enable the other military services to focus on their post, camps, stations, and domain-specific capabilities instead of each managing transport into and across the DoDIN.

Leadership & Education

The current single publication of cyber doctrine, produced by the Joint Staff,[58] generically addresses offensive and defensive operations and includes the structure of the U.S. Cyber

Command, a functional Combatant Command, and its subordinate and assigned organizations. When considering the land warfighting domain, the U.S. Army has sixteen different doctrinal references.[59] Additionally, the U.S. Army does not focus just on offensive and defensive operations; its doctrine describes a variety of capabilities to use in concert. This concept must extend to cyber to inform training and tactics required to achieve cyber dominance, both offensively and defensively.

The Cybersecurity & Infrastructure Security Agency (CISA) recently published the Workforce Framework for Cybersecurity,[60] based on the National Initiative for Cybersecurity Education (NICE) Framework. CISA outlined seven categories with thirty-three specialty areas and fifty-two work roles, all specific to cyber defensive roles.[61] The CISA categories do not apply to the DoD, but they highlight the complexity and broad skills required just for defense. Recently, the DoD published its Cyber Workforce Framework tool. This tool lists all the DoD cyber workforce roles, both offensive and defensive.[62] Each of these roles includes an exhaustive list of required skills, but no detail of that list is the minimum required for the achievement of expert status, signaling and guiding staff progression.

Personnel

Alternative manning options are currently not possible (or frowned upon) within the existing military services. Alternative generally refers to a person who would normally be physically or medically disqualified for service. A cyber-service would not be constrained by as those disqualifying factors. If the bulk of a cyber warrior's career will be sitting at a computer terminal doing some level of cyber activity, then many of the reasons other services use to exclude potential candidates become irrelevant, such as increasing the mandatory retirement age to bring in experienced talent, reducing physical fitness standards, changing medical requirements to allow for a greater number of approved disabilities, or following the U.S. Space Force's lead by using health monitoring instead of physical training tests.

Additionally, recruiting specifically for cyber will have a generative follow-on effect of increasing the cyber-skilled talent across the U.S. as trained cyber warriors transition back to the civilian workforce. History has proven this, as U.S. Air Force pilots transitioned from active service back to the commercial air industry.[63]

Facilities

Possible locations for the new Cyber Force could include the following. However, this list is not exclusive, and further research should be conducted to adequately capture the full requirement.

- Ft Meade, MD (USCYBERCOM / DISA / JFHQ-DoDIN)
- Scott Air Force Base, IL (DISA)

- Ft Eisenhower, GA (Army Cyber Command)
- Joint Base Lewis-McChord, WA (West coast point of presence)
- Guam – To establish a solid point of presence in the Pacific region

Policy

Very similar to doctrine, policy can help to drive the total force to gain dominance within the associated warfighting domain. Leaving cyber policy to a force built specifically to operate in cyber would allow for innovative changes to positively impact all warfighting domains and improve support to combat commanders. USCYBERCOM currently deals with at least four different sets of service policies specific to its assigned service members. Each service establishes policy specific to supporting its service members. This causes an unnecessary burden to offensive and defensive cyber operators working across mission sets.

For example, enlisted soldiers in the Army are required to complete certain activities to be eligible for promotion. Through these activities, they compete directly with their peer group across the Army, in rank and in their job category. These activities include the Army Combat Fitness Test, weapons qualification, professional military education (PME), civilian education, and annual evaluations.The results of these activities produce a rank-ordered list, by points, of those eligible for promotion. Each military service has a different process and requirements for enlisted promotions. To support the Army requirements, USCYBERCOM must allow Army enlisted soldiers the opportunity to complete these required activities, which may conflict with timing established by other services for their enlisted promotions, or ongoing operations. Establishing a single cyber military service would resolve this issue.

CONCLUSION

Considering the compelling arguments presented throughout this article, it is apparent that now is the time to establish a separate cyber military force under the Department of the Army. The current cyber threats facing the United States, the historical precedent set by the establishment of other military branches, and the existing gaps from of an overly complex and disjointed offensive and defensive cyber organization all point to the necessity of a dedicated cyber military force.

The evolving cyber threat landscape requires a robust response that can only be achieved through a dedicated cyber military force. The increasing frequency and sophistication of cyberattacks on U.S. infrastructure and systems echo similar risks to the DoDIN, demonstrating the need for a consolidated service to defend the nation's cyber domain. By centralizing resources, expertise, and command structure, a separate cyber military force will be better positioned to defend the United States from adversaries.

Moreover, the historical precedent of establishing separate military branches, such as the Department of the Air Force in 1947 and the U.S. Space Force in 2019, underscores the importance of a dedicated cyber military force. Furthermore, countries like Germany, Singapore, and China have also recognized the necessity of a separate cyber military force, leading them to establish dedicated branches. This global trend highlights the importance of the United States maintaining its competitive edge in the cyber domain. A dedicated cyber military force will enable the United States to develop the advanced cyber capabilities required to achieve dominance within the cyber domain, counter adversaries and maintain a technological edge in this ever-evolving domain.

Current gaps in both offensive and defensive cyber strategies further demonstrate the need for a separate cyber military force. As the thesis has shown, the disjointed multi-service model that exists today hinders the effectiveness and efficiency of our cyber operations, especially defensive cyber operations. A unified cyber military force could streamline the decision-making process, optimize resource allocation, and promote the development of advanced cyber capabilities that are essential to maintaining a competitive advantage in the cyber domain. Additionally, by reducing unnecessary redundancy, a separate cyber military force could have the added benefit of dramatically reducing costs currently expended by four different military branches all defending the same terrain.

Utilizing the DOTMLPF-P framework, the DoD can develop a comprehensive cyber military force structure that addresses the unique challenges and requirements of the cyber domain. This framework will also enable the DoD to avoid potential pitfalls and ensure the success of this new branch.

In conclusion, establishing a separate cyber military force under the Department of the Army is a critical and necessary step in addressing the evolving cyber threats facing the United States. By creating a dedicated force, the U.S. will be better positioned to defend its national interests in the cyber domain, develop advanced capabilities, and maintain a competitive advantage over potential adversaries. By using the DOTMLPF-P framework as a starting point, the DoD can ensure the successful development and implementation of this new branch, ultimately strengthening the nation's overall security posture.

NOTES

1. "Uslaw.Link," accessed February 3, 2023, https://uslaw.link/citation/us-law/public/80/253.
2. "Trump Signs Law Establishing U.S. Space Force," U.S. Department of Defense, December 20, 2019, https://www.defense.gov/News/News-Stories/Article/Article/2046035/trump-signs-law-establishing-us-space-force/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F2046035%2F-trump-signs-law-establishing-us-space-force%2F.
3. Donald H. Rumsfeld, "Report to the Commission to Assess United States National Security Space Management and Organization," January 11, 2001, https://aerospace.csis.org/wp-content/uploads/2018/09/RumsfeldCommission.pdf.
4. Peter A. DeFazio, "H.R. 7776, the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023," December 23, 2022, https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117HR7776EAS-RCP117-70.pdf.
5. Rumsfeld, "Report to the Commission to Assess United States National Security Space Management and Organization."
6. DeFazio, "FY23 NDAA," 509.
7. Winn, Jacob. "U.S. Can't Wait Any Longer for a Cyber Force." Nationaldefensemagazine.org. Accessed September 22, 2022. https://www.nationaldefensemagazine.org/articles/2022/4/22/us-cant-wait-any-longer-for-a-cyber-force.; Senate.gov, 2021. https://www.warner.senate.gov/public/_cache/files/f/2/f26e92ba-2b05-4e65-bbda-10d3a8dc-1c81/0CE82FCBF5172B642C7B6F9C2440B778.hainesnakasonewraywales-ssci-09feb21.pdf.; Aylward, Mary Kate. "The Air Force Isn't Doing Information Technology Right." *War on the Rocks,* December 20, 2021. https://warontherocks.com/2021/12/the-air-force-isnt-doing-it-right/.; Curley, Michael. "The US Military Needs a Seventh Branch: The Cyber Force." *The Hill.* September 2, 2021. https://thehill.com/opinion/cybersecurity/570634-the-us-military-needs-a-seventh-branch-the-cyber-force/.
8. "U.S. Cyber Command Leadership," U.S. Cyber Command, accessed April 26, 2023, https://www.cybercom.mil/Leadership/.
9. *Pat Fallon Supports a Cyber Service | C-SPAN.Org,* mp4, Senior Military Officials Testify on Cyber Operations (Washington, D.C., 2023), https://www.c-span.org/video/?c5064510/user-clip-pat-fallon-supports-cyber-service.
10. *Pat Fallon Supports a Cyber Service | C-SPAN.Org.*
11. Eric Pederson et al., "DoD Cyberspace: Establishing a Shared Understanding and How to Protect It," Air Land Sea Space Application (ALSSA) Center, January 1, 2022, https://www.alsa.mil/News/Article/2891794/DoD-cyberspace-establishing-a-shared-understanding-and-how-to-protect-it/.
12. "Federal Bureau of Investigation Internet Crime Report 2021," March 22, 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.
13. "Federal Bureau of Investigation Internet Crime Report 2021."
14. Eleanor Watson, "Pentagon Reviews: China Is 'Pacing Challenge' and Russia Poses 'Acute Threat' - CBS News," CBS News, October 27, 2022, https://www.cbsnews.com/news/pentagon-reviews-say-china-poses-greatest-security-challenge-to-u-s-while-russia-is-acute-threat/.
15. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA," April 20, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.
16. "Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors | CISA," October 6, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-279a.
17. "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector | CISA," July 6, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-187a.
18. "Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester | CISA," November 16, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-320a.
19. C. Todd Lopez, "DoD: It's Not Just State Actors Who Pose Cyber Threat to U.S.," U.S. Department of Defense, May 20, 2022, https://www.defense.gov/News/News-Stories/Article/Article/3039462/DoD-its-not-just-state-actors-who-pose-cyber-threat-to-us/.
20. Lopez, "DoD: It's Not Just State Actors Who Pose Cyber Threat to U.S.,".
21. Joseph W. Kirschbaum, "Information Environment: Opportunities and Threats to DoD's National Security Mission," U.S. Government Accountability Office, September 2022, https://www.gao.gov/assets/gao-22-104714.pdf, 2.

NOTES

22. Kirschbaum, 3.
23. Kirschbaum, 3.
24. Dr James P Tate, "The Army and Its Air Corps: Army Policy toward Aviation 1919-1941" (Maxwell Air Force Base, Alabama, Air University Press, 1998), https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0062_TATE_ARMY_AIR_CORPS.pdf, 187.
25. Tate, 12.
26. Tate, 20.
27. Tate, 20.
28. Mark Pomerleau, "US Cyber Command Releases First Full Budget," *DefenseScoop* (blog), March 13, 2023, https://defensescoop.com/2023/03/13/us-cyber-command-releases-first-full-budget/.
29. Rumsfeld, "Report to the Commission to Assess United States National Security Space Management and Organization."
30. Bundeswehr, The Cyber and Information Domain Service, accessed March 3, 2024 at https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service, translated by google.
31. Mike Yeo, "Singapore Unveils New Cyber-Focused Military Service," *Defense News*, November 2, 2022, https://www.defensenews.com/global/asia-pacific/2022/11/02/singapore-unveils-new-cyber-focused-military-service/.
32. Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* 3, no. 1 (Spring 2018), 105.
33. Kevin L. Pollpeter, Michael S. Chase, and Eric Heginbotham, "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations | RAND," 2017, https://www.rand.org/pubs/research_reports/RR2058.html.
34. Pollpeter, Chase, and Heginbotham, iii.
35. Pollpeter, Chase, and Heginbotham, 16.
36. "Command History," accessed April 7, 2023, https://www.cybercom.mil/About/History/.
37. "Command History."
38. Pederson et al., "DoD Cyberspace."
39. Pederson et al.
40. Pederson et al.
41. Colin Demarest, "US Indo-Pacific Command Seeks Extra $274 Million for Cyber," C4ISRNet, March 27, 2023, https://www.c4isrnet.com/cyber/2023/03/27/us-indo-pacific-command-seeks-extra-274-million-for-cyber/.
42. DeFazio, "FY23 NDAA."
43. Kirschbaum, "Information Environment: Opportunities and Threats to DoD's National Security Mission.", 2.
44. Tate, "The Army and Its Air Corps: Army Policy toward Aviation 1919-1941."
45. "U.S. Army Mission - The Army's Vision and Strategy | The United States Army," accessed October 19, 2022, https://www.army.mil/about/.
46. "U.S. Army Mission - The Army's Vision and Strategy | The United States Army."
47. "About Army Cyber," U.S. Army Cyber Command, accessed April 23, 2023, https://www.arcyber.army.mil/About/About-Army-Cyber/#:~:text=The%20Army%20was%20the%20first,into%20Cyberspace%20Operations%20Officer%20underway.
48. James Stavridis and David Weinstein, "Time for a U.S. Cyber Force," *U.S. Naval Institute* 140, no. 1 (January 1, 2014), https://www.usni.org/magazines/proceedings/2014/january/time-us-cyber-force.
49. Joseph Nunn, "The Posse Comitatus Act Explained | Brennan Center for Justice," October 14, 2021, https://www.brennancenter.org/our-work/research-reports/posse-comitatus-act-explained.
50. David R. James and Jean L. Dyer, "Rifle Marksmanship Diagnostic and Training Guide:" (Fort Belvoir, VA: Defense Technical Information Center, May 1, 2011), https://doi.org/10.21236/ADA544533.
51. Mark Gibson, "The Half Life of a Learned Skill Is 5 Years - Toward a New Culture of Learning," Why Change Selling, April 11, 2015, https://www.whychangeselling.com/inbound-marketing-messaging-sales-performance-blog/bid/113040/the-half-life-of-a-learned-skill-is-5-years-toward-a-new-culture-of-learning.

NOTES

52. Gibson, "The Half Life of a Learned Skill Is 5 Years - Toward a New Culture of Learning,".
53. Matthew J. Daniel, "Skills Aren't Soft or Hard — They're Durable or Perishable," October 29, 2020, https://www.chieflearningofficer.com/2020/10/29/skills-arent-soft-or-hard-theyre-durable-or-perishable/.
54. Rick Scott, "Text - S.1605 - 117th Congress (2021-2022): National Defense Authorization Act for Fiscal Year 2022 | Congress.Gov | Library of Congress," Congress.gov, December 27, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1605/text.
55. Alexandra Lohr, "Thunderdome Hits Its Targets, DISA Moves to next Phase of Zero Trust," Federal News Network, February 20, 2023, https://federalnewsnetwork.com/defense-news/2023/02/thunderdome-hits-its-targets-disa-moves-to-next-phase-of-zero-trust/.
56. Jeffrey A Couillard, Image produced by the paper's author from several years of experience managing the Army National Guard's portion of the DoDIN, including the Joint Regional Security Stacks (JRSS), to provide a high-level conceptual image of the complexity and redundancy in managing JRSS, January 22, 2023.
57. Couillard, Image produced by the paper's author to conceptualize the efficiency and economies of scale gained by establishing a separate Cyber Military Force, January 22, 2023.
58. "Joint Publication 3-12 Cyberspace Operations," Joint Chiefs of Staff, June 8, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
59. "Army Doctrine Publications," Army Publishing Directorate, access April 26, 2023, https://armypubs.army.mil/ProductMaps/PubForm/ADP.aspx.
60. "Workforce Framework for Cybersecurity (NICE Framework) | NICCS," accessed December 1, 2022, https://niccs.cisa.gov/workforce-development/nice-framework.
61. "Workforce Framework for Cybersecurity (NICE Framework) | NICCS."
62. "DoD Cyber Workforce Framework – DoD Cyber Exchange," accessed April 3, 2023, https://public.cyber.mil/wid/dcwf/.
63. Meredith Metsker, "Three Reasons Why the U.S. Is Running Out of Pilots," June 26, 2019, https://stradaeducation.org/adult-learners/three-reasons-why-the-u-s-is-running-out-of-pilots-2/.