A CASE FOR AN INDEPENDENT CYBER FORCE

Ian C. Heffron
Mark G. Reith
James Dean

Although cyberspace is considered the newest warfighting domain, military analysts and scholars have opined the United States remains woefully behind its peers in cyberspace and have called for the creation of a separate cyber service component. Yet a cohesive and robust discussion on this topic has yet to emerge. This article proposes a general framework that builds on the Joint doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) analysis to address questions of sufficiency and necessity. Such analysis reveals DoD cyber operations do not maximize the United States' ability to fight a cyber war, especially when compared against near-peer and peer threats such as China and Russia. A separate cyber force would position the United States to meet these challenges head on.

Since the 1990s, cyberspace has been part of the United States' combat mission, dating back to the creation of Joint Task Force (JTF)-Computer Network Defense in 1998.[1] Within the Department of Defense, this mission set has evolved throughout the years, culminating in US Cyber Command (USCYBERCOM). The purpose of the mission has remained relatively unchanged: defend and maintain US networks and crafting and launch offensive cyber operations against US adversaries. Throughout the years, US military and government analysts and scholars have discussed creating a military branch solely dedicated to cyber warfare.[2] Despite their

Captain Ian Heffron, USAF, a network operations officer at Joint-Base Anacostia-Bolling in Washington, DC, holds a master of science in computer science from the Air Force Institute of Technology.

Dr. Mark G. Reith is an assistant professor of computer science and adjunct assistant professor of systems engineering at the Air Force Institute of Technology.

Lieutenant Colonel James Dean, USAF, PhD, is an assistant professor of computer engineering at the Air Force Institute of Technology.

1. US Cyber Command, "Our History," US Cyber Command (website), n. d., accessed October 31, 2022, https://www.cybercom.mil/.

2. David Barno and Nora Bensahel, "Why the United States Needs an Independent Cyber Force," War on the Rocks, May 4, 2021, https://warontherocks.com/; Anthony S. Caristi, "Ignoring a Revolution in Military Affairs: The Need to Create a Separate Branch of the Armed Forces for Cyber Warfare" (master's thesis, US Army Command and General Staff College, Leavenworth, KS, 2017); and James Stavridis and David Weinstein, "Time for a U.S. Cyber Force," *Proceedings* 140, no. 1 (January 2014), https://www.usni.org/.

many opinions, ranging from forming a separate military branch to a small civilian cyber force, a clear framework from which to determine when and why such a new military unit may be justified has yet to emerge.[3]

Several articles have attempted to discuss the issue by applying Joint doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) analysis to determine what a distinct cyber service component should entail based on the assumption that a cyber service component *should* exist.[4] This article attempts to tackle this assumption directly with a similar, but distinct approach to provide senior leaders with a framework that may inform their decision-making. The specific composition of a distinct cyber force, however, is beyond the scope of this article.

The US Space Force is the newest branch of the Department of Defense. It took 58 years from the first manned space flight for the United States to create the US Space Force. Past leaders determined the warfighting capabilities of the space domain must be separated from the other services to achieve maximum effectiveness of US combat forces.

Will cyber be the next branch of US military power? And what factors drive the decision to establish a new military branch? This article proposes a framework to determine the arguments for and against a distinct cyber service component and to examine the gaps within this framework to demonstrate the need for the United States to create a separate service dedicated to cyber operations.

Distinct Service Component Analysis Framework

The proposed framework focuses on questions of necessity and sufficiency—specifically, whether a change to the current system is necessary, and whether a new service component would sufficiently address the identified problems.

Table 1 introduces the framework and outlines a set of questions and concerns relative to necessity/sufficiency (columns) across the DOTMLPF-P elements (rows). This framework extends DOTMLPF-P with additional rows to address internal signaling, or how the US public will receive and perceive the change in force structure, and external strategic signaling, or how foreign entities will receive and perceive this change.

The DOTMLPF-P analysis framework is a well-accepted concept from the Joint military community. DoD staff typically use DOTMLPF-P analysis, defined in the Joint Capabilities Integrations Development System Process, to assist in designing administrative changes, acquisition efforts to fill a capability need, or course of action

3. Zachary M. Smith, "Airpower History and the Cyber Force of the Future: How Organization for the Cyber Domain Outpaced Strategic Thinking and Forgot the Lessons of the Past" (master's thesis, Air Command and Staff College, Maxwell AFB, AL, June 2016).

4. Caristi, "Ignoring a Revolution"; and Lynn Scott et al., *Human Capital Management for the USAF Cyber Force* (Santa Monica, CA: RAND Corporation, 2010).

development.[5] Though it is hardly new, any discussion about the creation of a new service to fill a domain need would be remiss without including it. A full treatment of DOTMLPF-P can be found at the Defense Acquisition University.[6]

Internal signaling focuses on the response of the American public to a change in force structure. Will they look at it from a cost-saving or cost-generating perspective? Will they trust in the new organization to protect them and represent their best interests, or will they just see it as more governmental bureaucracy? In contrast, external signaling focuses on the potential responses of foreign governments. Will this change be perceived as a threat? Does the United States feel it necessary to demonstrate its resolve in each domain? Before the creation of a service or other governmental organization dedicated to a particular mission set can occur, the pros and cons of such an action must be weighed.

Not all sections of the proposed framework are equal and some may not apply at all. Decisionmakers themselves must decide which elements are priorities, and to what extent. A specific threshold is intentionally omitted because the topics are complex and nuanced and data that informs these questions may not be accessible. The framework is rather intended to prompt the reader to question the current state of military operations within a domain to encourage productive community discussion. No "correct" conclusion should come from DOTMLPF-P or strategic signaling analysis alone. Moreover, the framework omits the potentially contentious issue of funding because it focuses on long-term strategy. Ultimately, this analysis is intended to spark conversation that may help determine if a better method for implementing national power in an emerging military domain exists.

Table 1. Distinct Service Component Analysis Framework

Distinct Service Component Analysis Framework		
	Necessary	Sufficient
Doctrine	Does current doctrine fail to answer capabilities gaps and can it be tweaked slightly, or does it need significant changes to be effective?	Does the proposed system use resources to enable its forces to maneuver and incorporate a diverse mission set?
Organization	Does the current organizational structure fail to address the inability of the military to fill the capabilities gap?	Will the new force be organized in a coherent manner to fight in the domain?
Training	Is the given training coherent, with a logical progression, and does it cover the material necessary to ensure US forces are trained to fight in the domain?	Will US forces be properly trained to fight in the domain in question?

5. Chairman of the Joint Chiefs of Staff (CJCS), *Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System*, CJCS Instruction (CJCSI) 5123.01I (Washington, DC: CJCS, October 30, 2021), https://www.jcs.mil/.

6. Defense Acquisition University (DAU), "DOTMLPF-P Analysis," DAU (website), n. d., accessed May 1, 2023, https://www.dau.edu/.

Distinct Service Component Analysis Framework		
Materiel	Is US equipment aging or inadequate? Is there enough quantity of US systems to fight?	Will US fighters in the domain be properly equipped to match peer and nonpeer adversaries?
Leadership and Education	Is leadership inadequately prepared to tackle the problems facing US forces in the domain? Are domain leaders focused on and adequately prepared to tackle problems facing US cyber forces? Are domain leaders caught up in noncyber, service-related issues to the detriment of the defense of the domain?	Will the leadership understand the problems they are facing? Will they have the necessary resources to correct the problems? Will leadership be placed properly to affect change?
Personnel	Is there a lack of qualified individuals in key areas? Are the wrong people placed in the wrong areas?	Is there proper staffing to deal with any issues that may arise and are the right people in the right places?
Facilities	Are facilities causing issues for operators? Does equipment maintenance keep up with mission demand?	Will maintenance operations and facilities allow operators to carry out the mission?
Policy	Does US policy limit any of the previously discussed areas? Can one of them not be solved solely due to existing DoD or service-level policy?	Will the new policy allow the previously discussed seven areas to be addressed properly?
Internal Signaling	Is it important for the Department to demonstrate how dedicated it is to the defense of the domain to the American people? Does the Department of Defense care more about defending the domain than it does about potential civilian backlash at the creation of a separate service component?	Will the creation of a separate service send the wrong message to the American people? Will this cause protests or uproar? Are tools necessary to accomplish the mission already in place?
External Signaling	Is it important enough to show that the United States deems the domain critical to defending its interests to the point that the creation of a service component is warranted? Does the United States want the world to know that it intends to be the best in the domain?	Will the creation of the service escalate conflict? Will US adversaries and Allies condemn the act?

The necessity column in the table elicits a discussion on why the Department of Defense might be motivated to make changes to the status quo, while the sufficiency column elicits a discussion on why the new military service will better address the needs of the nation.

Application of Framework: US Space Force

The framework can be validated by examining the establishment of the US Space Force in December 2019. In this case, the United States determined it had reached a point at which the current paradigm from which space operations were conducted

was inadequate. It based this decisions on criteria that identified a warfighting domain and the associated organizational restructuring.

Space Force

The creation of the US Space Force focuses on certain framework criteria: doctrine, materiel, facilities, and strategic signaling were the only major framework factors that seemingly played a large part in the decision to form the US Space Force. By 2015 US peer-and near-peer- threat adversaries, namely Russia and China, had branches in their militaries dedicated to full-spectrum space operations.[7] But before 2019, doctrinally, the US military used space capabilities as a force enabling tool or for defensive threat detection. The United States and NATO did not view space as a warfighting domain.[8]

Prior to the establishment of US Space Force, the services did not recognize space as a full-spectrum warfighting domain. The US Navy used space for ballistic missile defense, and the US Army and US Air Force used space for early warning missile defense, positioning for troop movements, GPS-guided missile strikes, and intelligence collection. A new service was necessary for the United States to pool space operators in one service and focus on building up space as a warfighting domain, not simply as an enabler or a defensive tool against long-range threats.[9]

Additionally, with the Chinese and Russian governments combining military branches with their civilian space agencies to create the People's Liberation Army Strategic Force Support and the Russian Aerospace Forces respectively, the United States needed to signal to its Allies and adversaries that it would take any action in space to protect its interests. Materiel and facilities were lacking as well. Despite the fact the United States employed top-tier technologies, many of those technologies were created by the commercial sector and many had to be carried into space on the backs of Russian-made Soyuz rockets, limiting the US ability to use space in a warfighting capacity should the need arise.[10] The Space Force has since shifted to using SpaceX vehicles to launch capabilities into space, removing the reliance on Russia.[11]

---

7. John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, vol. 13 (Washington, DC: National Defense University Press, 2018); and Matthew Bodner, "Russian Military Merges Air Force and Space Command." *Moscow Times*, April 3, 2015, https://www.themoscowtimes.com/.

8. Kevin Pollpeter and Elizabeth Barrett, *NATO Ally Contributions to the Space Domain* (Arlington, VA: Center for Naval Analyses, 2021).

9. Barbara Barrett, *Department of the Air Force [DAF] Report to Congressional Committees: Comprehensive Plan for the Organizational Structure of the U.S. Space Force* (Washington DC: DAF, February 2020), https://velosteam.com/; and US Space Force, *United States Space Force* (Washington, DC: Department of Defense (DoD), 2019), https://media.defense.gov/.

10. Jonathan O'Callaghan, "The Last Soyuz - NASA Ends Reliance on Russia with Final Launch before Crew Dragon," *Forbes*, April 9, 2020, https://www.forbes.com/; and Michelle Cordero and Dean Cheng, "Does the United States Need A Space Force?," July 27, 2018, in *Heritage Explains*, produced by Michelle Cordero and Tim Doescher, podcast, 12:59, https://www.heritage.org/.

11. Theresa Hitchens, "A Space Force Dozen: SpaceX, ULA Awarded Contracts to Launch 12 New Satellites," Breaking Defense, June 8, 2023, https://breakingdefense.com/.

As for internal signaling, the creation of the US Space Force told Americans that the United States was going to deter and defeat its adversaries in the space domain. This was an important message as many in the United States feared space threats from China and Russia.[12] The United States and the Department of Defense took space-based military operations seriously enough to work together in a single service to outperform enemies and support Allies and partners around the world.

Application of Framework for a Separate US Cyber Force

Now that the framework has been demonstrated, it is necessary to validate the need for a US cyber force. A well-designed cyber force can remedy the inadequacies of current US cyber operations.

Doctrine

Necessary: Does current doctrine fail to answer capabilities gaps and can it be tweaked slightly, or does it need significant changes to be effective? One researcher argues the creation of US Cyber Command preceded the full development of military cyberspace doctrine.[13] With each service creating its own cyber forces, a lack of overarching cyber theory and doctrine led to the Air Force applying airpower theory to cyber operations. Yet airpower and cyber power are not the same; in fact, this employment strategy of the Air Force and the other services has led to strategic mistakes.[14]

Joint Publication 3-12, *Cyberspace Operations*, is intended to provide Joint doctrine to plan, execute, and assess cyberspace operations.[15] This publication, however, does not remove the service-based lens and employment strategies. In order to remove these, there must be a service component that solely focuses on cyber operations. Research shows that three factors are necessary for cyber to be successful: autonomy, mastery, and purpose.[16] But the way the services treat cyber is not conducive to autonomy.

Sufficient: Does the proposed system use resources to enable its forces to maneuver and incorporate a diverse mission set? Cyber operations could greatly benefit from giving operators autonomy to train in laboratory environments and lowering the decision-making level. Higher-level leaders would need only request an end product or a required level of competency to be demonstrated. To more effectively employ cyber capabilities there must be new doctrine. A new service component with the ability to

12. Loren Thompson, "Secret Pentagon Space Program Driven by Fear of China," *Forbes*, September 12, 2019, https://www.forbes.com/; and Robert A. Wood, "The Threats Posed by Russia and China to Security of the Outer Space Environment," U.S. Mission to International Organizations in Geneva, August 18, 2021, https://geneva.usmission.gov/.

13. Smith, "Airpower History."

14. Colin Gray, *Airpower for Strategic Effect* (Maxwell AFB, AL: Air University Press, 2012), 35–36.

15. CJCS, *Cyberspace Operations*, Joint Publication (JP) 3-12 (Washington, DC: CJCS, 2018).

16. John Chezem, "Air Force Cyber Mission Success Depends on Cultural Change," AFCEA International, October 1, 2015, https://www.afcea.org/

draft doctrine, focusing on enabling autonomy rather than one bogged down by existing force employment strategies, may be key to building a cyber force that is more prepared to deter and defeat our peer-level adversaries. Further issues within the military cyber community exist in the culture of box-checking and leadership appeasement.[17] This prevents individuals from being able to effect change, update broken processes, and deeply evaluate which policies and procedures are serving as barriers to mission needs. A separate service employing cyber-minded personnel may also be able to create new policies and procedures that can remove some of these bureaucratic barriers.

Organization

Necessary: Does the current organizational structure fail to address the inability of the military to fill the capabilities gap? The US military presents its cyber forces in the form of 133 cyber mission force teams. Each of these teams has one of four distinct assignments: Cyber National Mission Teams (CNMTs), Cyber Combat Mission Teams (CCMTs), Cyber Protection Teams (CPTs), and Cyber Support Teams (CSTs). These mission teams consist of members of all services. Currently, the services present their forces to USCYBERCOM, which in turn presents the teams to the geographic and other functional combatant commanders.[18] This structure means different services are developing capabilities separately.

In many cases, this may be beneficial, but because cyber operations weapons systems are expensive and time-consuming to develop, a lack of unity of effort can lead to duplicate capabilities, costing taxpayer money and stifling the ability to create diverse, top-of-the-line cyber weapons. As the Air Force's chief software engineer, Nicholas Chaillan, remarked in 2021, DoD cyber had "silos within silos" and "people reinventing the wheel," which reduced the effectiveness of US cyber forces. He stated, "we're very behind in cyber, to the point that it was very scary when it comes to critical infrastructure and the lack of security."[19]

Sufficient: Will the new force be organized in a coherent manner to fight in the domain? With the creation of a US Cyber Force, the format of the teams would not change; however, the key difference would be that the majority of presented forces would be sourced from the same service. Creating a new service to combine cyber professionals under one roof should lead to greater communication and help ensure that newly developed technology is shared within the entire cyber community and should result in greater cyber strength within the Defense Department.

---

17. Greg Hadley, "Air Force Leadership Needs to 'Walk the Walk' in Baking Security into Cyber, Software Boss Says," *Air & Space Forces Magazine*, August 12, 2021, https://www.airandspaceforces.com/.

18. CJCS, Cyberspace Operations.

19. *CITI Hearing: The Future of War: Is the Pentagon Prepared to Deter and Defeat America's Adversaries?* House Armed Services Committee (2023) (statement of Rear Admiral [Ret.] Mark Montgomery, senior director, Center on Cyber Technology and Innovation Foundation for Defense of Democracies), https://armedservices.house.gov/.

Training

Necessary: Is the given training coherent, with a logical progression, and does it cover the material necessary to ensure US forces are trained to fight in the domain? Currently there is no Joint technical skills school to ensure consistent training for all DoD cyber personnel. Retired Rear Admiral Mark Montgomery states that this has resulted in a cyber force that is inconsistent in training, readiness, and organization.[20]

Sufficient: Will US forces be properly trained to fight in the domain in question? A new service would be able to bring in the best aspects of each technical school and provide consistent and advanced training for all cyber individuals. Further, with current cyber training conducted by noncyber service components, even highly trained and specialized cyber operators will inevitably approach cyber problems from the perspective of their own service. A new training pipeline within a single service for all DoD cyber would help remove the service-specific view that hinders cyber operators and help enable greater standardization across the US cyber force.

Leadership and Education

Necessary: Is leadership inadequately prepared to tackle the problems facing US forces in the domain? Are there domain-minded DoD leaders in high enough positions to effectively advocate on behalf of the domain? USCYBERCOM leadership currently comprises general officers with experience in their service component's cyber units. While this is a reasonable Joint approach, it may not be enough to resolve differences in how cyber is employed as a full-spectrum capability. More importantly, the shifting of leadership from the various service components—that is, with each service taking a turn—may induce significant and frequent policy changes that degrade organizational performance.

Furthermore, it requires a significant commitment from service components to grow leaders with appropriate backgrounds in order to maintain a pool of viable candidates. The Army, Navy, Air Force, Space Force, and Marine Corps operate differently, as they have different doctrine and perspectives on how to win wars. This is seen in Joint task forces, as they are led by the commander from the component that provides the most forces to the operation. As a result, Army doctrine is most prevalent in JTFs.[21] This results in the Air Force, Navy, and Marine Corps following unfamiliar Army structure and processes to conduct operations. This issue extends to most Joint forces as there will always be a need for a Joint force commander from one of the existing services. Joint forces will likely never be rid of this unfortunate byproduct of having the commander coming from a single service.

Sufficient: Will the leadership understand the problems they are facing? Will they have the necessary resources to correct the problems? Will leadership be placed prop-

20. Daniel R. Walker, "The Organization and Training of Joint Task Forces" (master's thesis, Air University, 1996).

21. Walker.

erly to affect change? USCYBERCOM can benefit from a US Cyber Force as its leadership will be brought up within the cyber community—which means they will likely approach cyber as a force-projection capability instead of simply as a force multiplier—and will be brought up in cyber doctrine, exercising leadership through a purely cyber lens.

Personnel

Necessary: Is there a lack of qualified individuals in key areas? Are the wrong people placed in the wrong areas? Two major issues face US military cyber right now. The loss of qualified personnel to private industry and a lack of high-ranking cyber leadership to advocate for cyberspace.[22] Regarding the loss of talent, many cyber professionals rightly believe they can make more money working in information technology (IT) for a private company. Additionally, the size of the cyber mission forces each service contributes has not increased appreciably since 2012 despite the *National Security Strategy* directly calling for the United States to secure cyberspace.[23]

Sufficient: Is there proper staffing to deal with any issues that may arise and are the right people in the right places? To incentivize and retain cyber professionals, a US Cyber Force could distinguish itself from private industry, demonstrating that cyber defense and offense are different careers than IT. This distinction may help bring in talented individuals with a desire to operate in a warfighting capacity. Further, a separate branch would bring with it new general officer positions at the highest levels that could better advocate for the domain. This should lead to better educated cyber leaders that understand the domain and how to organize the force to remove barriers that frustrate personnel and lead them to separate from the US government.

Appearance standards are one area that provide an example of needed changes in the personnel arena related to recruitment and retention of cyber professionals.

Several individuals have called for changes to appearance standards for US military cyber operators. They have referred to requirements concerning hair color, tattoos, weight, and fitness level that would normally disqualify someone from becoming a cyber warrior.[24] Yet a relaxing of standards within existing military branches has led to morale issues in the British Army.[25] These morale issues are likely due to changing standards within existing branches. A distinct cyber component may permit a culture that emphasizes cyber skills over physical strength and endurance, preventing such a morale issue. The relaxed standards could simply be part of service branch rivalry. More research regarding relaxed standards within the US military could be useful in determining how beneficial a change like this could be.

22. Stavridis and Weinstein, "U.S. Cyber Force."

23. Montgomery, *Future of War*; and Joseph R. Biden, *United States National Security Strategy* (Washington, DC: The White House, 2022).

24. Caristi, "Ignoring a Revolution"; and Stavridis and Weinstein, "U.S. Cyber Force."

25. Caristi.

Internal and External Signaling

Necessary: Internally, does the public understand the need for the creation of the domain? Is it important for the United States to state the importance of the domain and to show its citizens it takes the threat and the domain seriously? Externally, is it important to show that the domain is critical, and the US is resolute in this area? Does the United States want the world to know that it intends to be the best in the domain? Care must be taken to ensure that US adversaries do not see a cyber force as escalatory; however, the United States must also weigh the need to demonstrate how seriously it takes cyberspace both to adversaries and to the American people. The 2018 DoD *Cyber Strategy* outlined a new term called "defending forward," which is a shift from active defense defined in its *Strategy for Operating in Cyberspace* in 2011.[26]

Sufficient: Internally, will the creation of a separate service send the wrong message to the American people? Will this cause protests or uproar? Are tools necessary to accomplish the mission already in place? Externally, will the creation of the service escalate conflict? Will US adversaries and Allies condemn the act? The United States is often critical of China and Russia and their cyber tactics, calling out Russia for meddling in the 2016 presidential election and China for hacking into the Office of Personnel Management and stealing the personal files of millions of Americans with security clearances.[27] Yet China and Russia have both reacted to the defending forward strategy with criticism. Both nations state their cyber operations are limited to defense and retaliatory strikes.[28]

Releasing more aggressive strategy or establishing a new service will likely always elicit responses from near-peer and peer adversaries. After the creation of the US Space Force, for example, China and Russia issued statements condemning the US action.[29] The Chinese government accused the United States of turning space into a battlefield and the Russians echoed the sentiment. Yet actual actions in retaliation have been few and far between with continued cooperation between the Russian and US space agencies.[30]

---

26. DoD, *Summary: Department of Defense Cyber Strategy* 2018 (Washington, DC: DoD, 2018), 4, https://media.defense.gov/; DoD, *DoD Strategy for Operating in Cyberspace* (Washington, DC: DoD, 2011), 6, https://csrc.nist.gov/; and Lyu Jinghua, "A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward,' " *Lawfare* (blog), October 31, 2019, https://www.lawfareblog.com/.

27. Josh Fruhlinger, "The OPM Hack Explained: Bad Security Practices Meet China's Captain America," CSO United States, February 12, 2020, https://www.csoonline.com/.

28. Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare* (Washington, DC: Center for Naval Analyses, March 2017); and Jinghua, "Chinese Perspective."

29. Reality Check team, "Russian President Warns over Expansion of US Space Force," BBC News, December 4, 2019, https://www.bbc.com/; and "China Attacks US Space Force as Threat to Outer Space Peace," Associated Press, December 23, 2019, https://apnews.com/.

30. Kenneth Chang and Anton Troianovski, "In Space, U.S.-Russian Cooperation Finds a Way Forward," *New York Times*, July 15, 2022, https://www.nytimes.com/.

Similarly, cyber often ends up serving a de-escalatory rather than escalatory function.[31] Cyber can alter the battlefield to force an adversary into disadvantageous situations, thus decreasing the desire to fight in that moment. On the other hand, by not creating a separate force in a new domain or surrounding a new capability, the United States may signal to Americans and adversaries that it views the domain with little or no significance.

The creation of the National Artificial Intelligence Initiative (NAII), while not a separate service, signaled to the American public, partners, and adversaries that the United States was taking the advent of artificial intelligence (AI) seriously by prioritizing AI research for purposes of national security and economic prosperity.[32]

If the United States decides that it wants to become the world leader in a new technology or domain, then due consideration must be made regarding the creation of an organization dedicated to developing this technology. As with NAII, the United States decided that AI is of key importance to national security. While some capabilities may be more effectively governed in a national organization such as the NAII, other capabilities should have a dedicated warfighting service. Cyberspace is one of those. By establishing a separate cyber force, the United States is signaling cyber is on par with the other warfighting domains.

Counterarguments to a Separate US Cyber Force

The arguments made thus far highlight key aspects of the proposed framework. This section identifies not only counterarguments but also potential gaps in the framework, namely the historical coupling of the intelligence and cyber communities, as well as the argument that USCYBERCOM should model itself after US Special Operations Command (USSOCOM) instead of forming a separate service component.

Relationship between Intelligence and Cyber

Intelligence operations have been closely linked to cyber and cyberspace operations since their inception. Cyber was spawned through intelligence with ciphers and cryptographic machines such as Enigma in World War II. Following the war, cyber became a tool for organizations to gain intelligence on adversaries' computing devices.[33] Computing devices transitioned from the means to conduct intelligence to intelligence targets.

The creation of an independent US Cyber Force would likely see the split of USCYBERCOM and the National Security Agency (NSA), two organizations that currently are highly intertwined, with one leader dual-hatted as the commander of

31. Christopher Whyte and Brian M. Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy* (Abingdon, UK: Routledge, 2023).

32. National Artificial Intelligence Initiative (NAII) Act of 2020, Pub. L. No. 116-283 (2021); and NAII Office (NAIIO), "About," NAIIO, accessed June 21, 2023, https://www.ai.gov/.

33. Whyte and Mazanec, *Understanding Cyber Warfare*.

USCYBERCOM and NSA director. This close connection between the two organizations has been controversial for years, with some calling for the separation of the two.[34] Still, the coordination ability between the cyber domain and the Intelligence Community is of paramount importance when considering the capabilities of US adversaries and the speed in which decisions can be made when unity of command exists. The cooperation between the NSA and USCYBERCOM is beneficial in coordinating offensive and defensive cyber operations. One command structure enables greater sharing of ideas and capabilities, and the creation of innovative solutions for mutual operations.[35] This innovation is critical when dealing with adversaries such as Russia and China that have developed and are developing their own internet standards. China already has developed the Great Firewall that censors traffic deemed inappropriate by its government, and Russia is developing its own domain name system, capable of redirecting users and internet traffic as the government sees fit.[36] These efforts by near-peer and peer adversaries underpin the need for a close relationship between intelligence and cyber. Yet despite the current arrangement, this need for closeness does not require the NSA and USCYBERCOM be led by a single individual.

In fact, US Congress decided this connection could be terminated in the future, but only once Cyber Command was able to stand on its own. Congress recognized the mission sets of the NSA and Cyber Command are large enough in their own right to justify each needing its own commander. In 2016, the National Defense Authorization Act established a set of criteria that USCYBERCOM and the NSA would have to meet in order to separate. These criteria mainly revolve around creating a command-and-control structure, operational infrastructure, and capabilities to enable intelligence collection and cyber operations as well as training for cyber operators.[37] Cyber Command has not yet developed a robust enough system of command and control or operational infrastructure to break free from the NSA, but creating a US Cyber Force will help to realize these conditions for separation.

The link between cyber and intelligence will likely remain; however, one of the criteria for separating NSA and USCYBERCOM is that capabilities must be established to enable intelligence collection and operational preparation of the environment—that is, the highly technical requirements—for cyber operations. Placing intelligence liaisons, perhaps even intelligence personnel staffed from a newly created US Cyber Force, in cyber teams or within the cyber operations center is a simple way of furthering the integration of cyber operations and intelligence. This can even be extended to

34. Chris Demchek, "Five Reasons Not to Split Cyber Command from the NSA Any Time Soon – If Ever," War on the Rocks, March 5, 2021. https://warontherocks.com/.

35. Paul Nakasone, "CYBERCOM and NSA Chief: Cybersecurity Is a Team Sport," *Defense News*, August 19, 2022. https://www.defensenews.com/.

36. "Russia: Growing Internet Isolation, Control, Censorship," Human Rights Watch (website), October 28, 2020. https://www.hrw.org/; and Yaqiu Wang, "In China, the 'Great Firewall' Is Changing a Generation," *Politico*, September 1, 2020, https://www.politico.com/.

37. National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328 (2016).

liaisons from other mission sets, such as other forms of nonkinetic or kinetic operations personnel, further strengthening the ties of US cyber operations to noncyber missions.

Following the USSOCOM Model and a Duplicative Service

Many have stated, as far back as 2007, that a US Cyber Force should be modeled after the example set by US Special Forces.[38] Similarities between cyber operations and special operations include the need for an agile acquisition process for capabilities as well as the ability to leverage different authorities and work across service lines as USCYBERCOM, like USSOCOM, is a functional combatant command instead of a geographic combatant command.[39] Further, if the services are providing highly specialized forces to USSOCOM to enable special operations, and the services are providing highly technically proficient forces to USCYBERCOM for cyberspace operations, then why is the USSOCOM model not sufficient for US military cyberspace operations? Many also argue that each of the services are growing their cyber components in ways to support their services, with the US Army prioritizing the integration of cyberspace operations with their land forces and the US Navy prioritizing cyberspace for fleet defense operations.[40] This parallels the idea of each service providing special operations forces with expertise in their respective domains.

Drawing such parallels between the two commands, however, is problematic. USSOCOM must function in multiple domains, where USCYBERCOM only functions in one domain: cyberspace. Echoing a similar sentiment, Vice Admiral Craig Clapperton, commander of Fleet Cyber Command, said that a distinct cyber force would be a duplicative force, as the Navy's Fleet Cyber Command would still work to carry out cyberspace operations necessary for fleet defense, and similar cyberspace operations would be needed within the Army.[41] While this paper does not deign to guess whether a cyber branch would or would not assume those functions for the services, the argument against a duplicative service falls flat when considering the current state of US military aviation assets.

Nearly all services have aviation capabilities despite the existence of the US Air Force. The US Air Force could not serve the unique aviation functions of the other services as well as the individual services themselves. This may be true as well for a future cyberspace service component. Perhaps there will still be need of cyberspace operators in key roles in each of the existing services. The argument that a cyber service might be duplicative does not negate the value of a service component dedicated

38. John Sakellariadis, "For Future of Cyber Command, Look to SOCOM," *Politico*, January 9, 2023, www.politico.com/; Mark Pomerleau, "Many Believe It's Time for an Independent Uniformed Cyber Service. Here's What It Could Look Like." DefenseScoop, May 15, 2023, https://defensescoop.com/; and Joe Gould, "Former NSA Chief: Follow SOCOM Model for Cyber," *Defense News*, August 19, 2022, https://www.defensenews.com/.

39. Pomerleau, "Uniformed Cyber Service."

40. Stavridis and Weinstein, "U.S. Cyber Force."

41. Pomerleau, "Uniformed Cyber Service."

to organizing, training, and equipping multicapable cyberspace operators, capable of working throughout the domain in support of multidomain operations.

Conclusion

Whether cyber becomes a separate branch of the military is yet to be determined; however, the case can be made that the current system is inadequate if the United States is to continue to compete at the highest levels with its peer and near-peer adversaries. The United States must find a way to develop a cohesive cyber organization that can be organized to thwart these ever-present and potentially existential threats. This force must be appealing to a new generation of fighters in a way that the current services are not, allowing for potentially different standards to allow for the best talent. There must be a change in doctrine and leadership styles if the US military is to cultivate a lethal and effective cyber force.

The current way of thinking about cyber limits the nation's ability to scale cyber operations. The United States will need to increase the number of cyber competent leaders in the higher echelons of government. This line of thinking follows for any future service or capability. Warfare solely focused on air and naval superiority and land occupation is a concept of the past. Today's militaries must be able to think in new and creative ways and leverage technologies such as cyber and artificial intelligence in innovative manners. *Æ*