MITIGATING CYBER VULNERABILITY

A Proposal for an Independent Cyber Force Within the DAF

Marco Catanese

As the United States confronts the challenges of intensified competition with China and other peer adversaries, its focus on exquisite platforms potentially overlooks the increasing cyber vulnerability of US forces, resulting in a poorly organized and resourced cyber force vis-à-vis China.[1] With its relatively small size, synergies with the US Space Force, and innovative culture, the Department of the Air Force is the ideal organization to house a larger and independent cyber force that would address current threats and develop unique cyber doctrine and education.

China's kinetic and nonkinetic forces have dramatically increased in size and capability, posing a broad threat to the United States and its Allies.[2] These forces, coupled with China's heightened aggression—such as prepositioning destructive malware on United States critical infrastructure in case of a conflict—form the impetus for the Department of Defense to continue optimizing for great power competition.[3] Such efforts are wide-ranging, including reoptimizing core capabilities and

Major Marco Catanese, USAF, chief of the strike branch at the Office of the Secretary of the Air Force Studies and Analysis, has a master of science in industrial engineering from New Mexico State University and a master of military operational art and science from the Air Command and Staff College.

1. The author would like to thank Dr. C. J. Horn, Dr. Heather P. Venable, and Major Julia Catanese for their help and contributions to this article.

2. Robert Haddick, *Fire on the Water: China, America, and the Future of the Pacific*, 2nd ed. (Naval Institute Press, 2022), 25.

3. *Department of the Air Force* [*DAF*] *Posture Statement Fiscal Year* [FY] *2024, Hearing Before the Senate Armed Services Committee on the Posture of the Department of the Air Force in Review of the Defense Authorization Request for FY 2024 and the Future Years Defense Program* [*Posture Statement*], 118th Cong. (2023), (statements of Secretary of the Air Force Frank Kendall, Chief of Staff of the Air Force Charles Q. Brown Jr., and Space Force Chief of Space Operations B. Chance Saltzman), 2–3, https://www.armed-services.senate.gov/; *The CCP Cyber Threat to the American Homeland and National Security*, *Hearing Before the Select Committee on Strategic Competition Between the United States and the Chinese Communist Party United States House of Representatives on the CCP Cyber Threat to the American Homeland and National Security,* 118th Cong. (2024) (statement of Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security), 2, https://selectcommitteeontheccp.house.gov/; and Secretary of the Air Force Public Affairs, "Air Force, Space Force Announce Sweeping Changes to Maintain Superiority amid Great Power," US Air Force (USAF), 12 February 2024, https://www.af.mil/.

organizational structures and developing exquisite weapon systems to better compete with China.[4] Yet, these efforts potentially overlook the increasing cyber vulnerability of the United States forces.

In fact, based on the testimony of each service secretary to the Senate Armed Services Committee, none of the services' top modernization priorities are cyber-related.[5] Recently, however, the services have made some strides with improving their cyber postures. The Air Force has elevated Air Forces Cyber into a standalone service component command.[6] The Navy has released a new cyber strategy, and after prompting from Congress, it created dedicated separate cyber roles for its officers and enlisted personnel.[7] By early 2024, the Army and Marines had accepted the US Government Accountability Office's recommendation to add active-duty service obligations for Interactive On-Net training, a lengthy and expensive advanced cyber training.[8] Yet these efforts by the services are not fully assuaging congressional concerns, leaving the United States with its currently poorly organized and resourced cyber force.[9]

With no service adequately prioritizing this issue, Congress directed in the Fiscal Year 2025 National Defense Authorization Act (NDAA) that the Defense Department evaluate the need for an independent cyber force "as a separate Armed Force in the Department of Defense dedicated to operations in the cyber domain."[10] This assessment would be performed by the National Academies of Science, Engineering, and Medi-

---

4. Ronald O'Rourke, *Great Power Competition: Implications for Defense—Issues for Congress*, R43838 (Congressional Research Service [CRS], 28 February 2024), 9, 10, 27, https://crsreports.congress.gov/.

5. *DAF Posture Statement FY 2025*, 118th Cong. (2024), (statements of Secretary of the Air Force Frank Kendall, Chief of Staff of the Air Force David W. Allvin, and Space Force Chief of Space Operations B. Chance Saltzman), https://www.armed-services.senate.gov/; *Department of the Army Posture Statement FY 2025*, 118th Cong. (2024), (statements of Secretary of the Army Christine E. Wormuth and Chief of Staff of the Army Randy A. George), https://www.armed-services.senate.gov/; and *Department of the Navy Posture Statement FY 2025*, 118th Cong. (2024), (statement of Secretary of the Navy Carlos Del Toro), https://www.armed-services.senate.gov/.

6. Mark Pomerleau, "What Will the Elevation of Air Forces Cyber Look Like?," *DefenseScoop*, 5 April 2024, https://defensescoop.com/; and "Rapid Loss of Talent Contributing to DOD [Department of Defense] Cyber Shortfalls: Pentagon's Chief Weapons Tester," *DefenseScoop*, 23 January 2023, https://defensescoop.com/.

7. Justin Katz, "Navy Publishes First Cyber Strategy, Prioritizing Defense of 'Information Ecosystem,' " *Breaking Defense*, 21 November 2023, https://breakingdefense.com/; and Mark Pomerleau, "After Prodding from Congress, Navy Creates Dedicated Cyber Work Roles to Boost Readiness," *DefenseScoop*, 28 June 2023, https://defensescoop.com/.

8. Brenda S. Farrell et al., *Military Cyber Personnel: Opportunities Exist to Improve Service Obligation Guidance and Data Tracking*, GAO-23-105423 (US Government Accountability Office [GAO], 21 December 2022), https://www.gao.gov/.

9. See, for example, Mark Pomerleau, "What Will the Elevation of Air Forces Cyber Look Like?," *DefenseScoop*, 5 April 2024, https://defensescoop.com/; Pomerleau, "Rapid Loss"; and Justin Katz, "Navy Publishes First Cyber Strategy, Prioritizing Defense of 'Information Ecosystem,' " *Breaking Defense*, 21 November 2023, https://breakingdefense.com/.

10. National Defense Authorization Act (NDAA) for FY 2025, Pub. S. no. 118–159 (2024), 377, https://www.congress.gov/; and see, for example, Greg Hadley, "Is a Cyber Force Next? Lawmakers Want Independent Study," *Air & Space Forces Magazine*, 30 May 2024, https://www.airandspaceforces.com/.

cine. The draft included a proposal for an outside organization to evaluate the feasibility of an independent cyber force. The fiscal year 2024 Senate version of the NDAA included a similar proposal but it was removed after pushback from the Defense Department; the 2025 proposal has encountered similar pushback.[11] In arguing against the creation of a new cyber force, DOD leaders and others rationalize that US Cyber Command (CYBERCOM) has not been allowed enough time to utilize its new budgetary authorities to drive changes and that with no evidence an independent cyber force will be a more effective option, moving all cyber forces to a new service would be detrimental to the parent services.[12]

This article contends that the most effective way to remedy the cyber shortfall is to create a dramatically larger and independent cyber force to address current threats and develop unique cyber doctrine and education. Such a change would not necessarily be costly, as costs in cyber are inherently lower than other defense expenditures. In fiscal year 2024, such expenses were allocated to be $13.5 billion, or just 2 percent of the DOD budget.[13]

Additionally, such a cyber force should be created within the Department of Defense. Recent analyses have covered the debate on whether such a new force should be housed within the Defense Department or external to it, with one analysis supporting the latter camp offering alternatives "better suited to the unique demands of cyber," such as modeling a cyber service after the US Coast Guard or the US Public Health Services Commissioned Corps.[14] Yet while the creation of a cyber force outside the Department of Defense may improve the ability of the federal government to respond to domestic cyberattacks, it is neither cost effective nor beneficial in terms of timeliness, given the urgent need for cyber capabilities in the current strategic environment.

This article further contends that the Department of the Air Force (DAF) would be the best department to house a new cyber force due to its synergies with the US Space Force and the DAF's relatively small size and innovative culture. The Cyber Force, like the Space Force, would be relatively small and agile and would mesh well with the highly technical branches of the Air and Space Force.[15]

---

11. Martin Matishak, "Pentagon Gives Thumbs-down to Cyber Service Proposal in Defense Bills," *The Record from Recorded Future News*, 27 September 2024, https://therecord.media/.

12. See for example, Mark Pomerleau, "Many Believe It's Time for an Independent Uniformed Cyber Service. Here's What It Could Look Like," *DefenseScoop*, 15 May 2023, https://defensescoop.com/; and Alan Brian Long Jr. and Alex Pytlar, "An Argument Against Establishing a U.S. Cyber Force," *DefenseScoop*, 11 July 2024, https://defensescoop.com/.

13. Mark Pomerleau, "US Cyber Command Releases First Full Budget," *DefenseScoop*, 13 March 2023, https://defensescoop.com/.

14. Michael Kreuzer, "A Better Cyber Service," *War on the Rocks*, 4 January 2024, https://warontherocks.com/; see also Pomerleau, "Many Believe"; and Erica Lonergan, Todd Arnold, and Nick Starck, "The Case for a Prospective US Cyber Force," *War on the Rocks*, 22 May 2024, https://warontherocks.com/.

15. David Barno and Nora Bensahel, "Why the United States Needs an Independent Cyber Force," *War on the Rocks*, 4 May 2021, https://warontherocks.com/.

Creating a new service under the DAF does not mean that every service's cyberspace operations forces and capabilities should be transferred to the DAF. Rather, only each service's cyber warfare personnel and capabilities that they currently provide to CYBERCOM's Cyber Mission Force (CMF) should be transferred. This article thus envisions a cyber force comprising initially of the existing personnel and capabilities transferred from the services with plans to rapidly grow the force to better posture the United States for offensive and defensive operations in peer competition, crisis, and conflict. This would overcome one of the main arguments against an independent cyber force as the services and agencies would retain most of their cyber workforce.

Information Dominance in the United States and China

Although both China and the United States view information dominance as essential to future warfare, only China has reoriented and prioritized its cyber-related military forces.[16] After Desert Storm, China identified that information dominance would be critical in any future conflict.[17] Later in the 1990s, China emphasized "network-centric warfare" and started organizing cyber units, which by the 2000s were conducting espionage and cyberattacks.[18] China has routinely used cyberattacks over the last 10 years to steal military technology and conduct economic espionage, resulting in an economy and military roughly equivalent to the United States'.[19]

China's emphasis on information and cyber warfare is further demonstrated by its 2015 military reorganization, which established a Strategic Support Force that elevated the Chinese cyber force as one department within that unit along with its space force.[20] In 2024, China reorganized its forces again, dividing the Strategic Support Force into separate information support, cyber, and space forces, all directly subordinate to the Central Military Commission.[21] Initial analysis suggests the division was implemented to improve President Xi Jinping's visibility into each force.[22] In any case, these efforts further China's goal for "intelligentized warfare"—or "the

16. Thomas L. Cantrell, "JADC2 Culture at the Operational Level of War," *Air & Space Operations Review* 2, no. 1 (2023): 45, https://www.airuniversity.af.edu/; *Military and Security Developments Involving the People's Republic of China 2023: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2000, as Amended* (DOD, 2023), 40, 93, https://media.defense.gov/; and "Command History," US Cyber Command, accessed 11 December 2023, https://www.cybercom.mil/.

17. Michael V. Smith, "Are We Gaining or Losing the High Ground of Space?" (lecture, Air Command and Staff College, 11 December 2023).

18. Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges* 7, no. 2 (2011), https://www.jstor.org/; and Jonathan Racicot, "The Past, Present and Future of Chinese Cyber Operations," *Canadian Military Journal* 14, no. 3 (2014), http://www.journal.forces.gc.ca/.

19. *Military and Security Developments*; and Robert D. Blackwill and Jennifer M. Harris, *War by Other Means: Geoeconomics and Statecraft*, 1st Harvard paperback ed. (Belknap Press, 2017).

20. Caitlin Campbell, *China's Military: The People's Liberation Army (PLA)*, R46808 (CRS, 4 June 2021), 24, https://crsreports.congress.gov/; and *Military and Security Developments*, 93.

21. Nectar Gan, "Xi Shakes Up China's Military in Rethink of How to 'Fight and Win' Future Wars," *CNN*, 27 April 2024, https://www.cnn.com/.

22. Gan.

expanded use of AI and other advanced technologies at every level of warfare"—and its belief that information technologies are a key vulnerability of the United States.[23] As such, China is investing in capabilities to attack systems used in command and control and logistics.[24]

The United States also perceives information dominance as vital but has yet to make the requisite organizational structure changes or investments to reflect the new strategic environment. In the late 1990s and the early 2000s, the United States initiated a series of organizations to conduct defensive and offensive operations. CYBERCOM was then established in 2010 as a sub-unified command and later in 2018 as a unified combatant command. Today CYBERCOM is largely the same size and has the same structure as projected in the early 2010s.[25]

Information connectivity is the core of Joint All-Domain Command and Control, which plans to interconnect existing and new systems—including the B-21 Raider—to deliver transformational capabilities in all domains using meshed sensor-to-shooter networks.[26] If the United States recognizes that information and cyber are essential to its core capabilities and acknowledges that China believes it can exploit that vulnerability, then it is logical that the United States would dramatically increase capabilities to defend and attack in cyberspace.[27] Yet, it has pursued only limited investments due partially to other priorities such as the Global War on Terror but also to service parochialism, with the services prioritizing their domain or mission ahead of other services or the Joint force.[28] This in turn has restricted the number and quality of personnel assigned to the cyber mission. A separate cyber force will be essential to ensure the United States can compete with China in the cyber domain.

The Cyber Mission Force cannot counter China with the low quantity of forces with mixed readiness levels currently provided by the services. In 2012, three years before China created its cyber force under its Strategic Support Force, the United States created CMF with an authorized force of 133 teams and 6,200 personnel.[29] It took six years for the CMF to reach full operational capability of 5,000 military and civilian personnel in 133 teams, and today the force has about 6,200 personnel with mixed readiness levels.[30] At the same time that the CMF declared full operational capability, CYBERCOM was elevated to a unified combatant command.[31] In 2022,

23. *Military and Security Developments*, VIII.

24. *Military and Security Developments*.

25. "Command History."

26. Cantrell, "JADC2 Culture," 44.

27. "Command History."

28. S. Rebecca Zimmerman et al., *Movement and Maneuver: Culture and the Competition for Influence Among the U.S. Military Services* (RAND Corporation, 2019), https://www.rand.org/.

29. "Command History."

30. "Command History"; and Mark Pomerleau, "Senate Armed Services Committee Looks to Tackle Cyber Mission Force Readiness—Again," *DefenseScoop*, 11 July 2023, https://defensescoop.com/.

31. Cantrell, "JADC2 Culture," 44.

CYBERCOM announced that over the next few years the CMF would increase 11 percent to 147 teams.[32]

Yet even though the number of teams has increased, improving readiness levels remains a challenge.[33] Some cyber officers allege that official readiness statistics are inflated, with proficient cyber operators double-counted to show that CMF teams are at full-strength when they are in fact filled at only 67 to 75 percent capacity.[34] The Navy in particular has had difficulty with readiness; yet in early 2024, training was improved and Congress mandated the Navy create specific cyber roles for enlisted personnel and officers.[35]

Clearly, the size of the CMF has not kept pace with threat actors—individuals or groups who pose a threat to cybersecurity—nor the increase in missions assigned. Since 2012, China and others such as Russia, North Korea, Iran, and nonstate actors have expanded their cyber capabilities.[36] In addition to the greater number of threat actors, the CMF has recently been increasingly tasked to conduct missions not traditionally assigned to the military, including supporting election security and securing the defense industrial base.[37] Given the greater number and capability of cyber threat actors, the additional missions required of the CMF, and the exponential growth of internet connectivity and devices, the United States logically should have significantly increased the number of its cyber forces and associated readiness to counter these threats, but unfortunately it has not.[38]

While the services have recently claimed they are now committed to intensifying efforts to improve the readiness and capacity of cyber forces, it is unlikely that their parochial practices would suddenly end and they would shift significant resources and personnel to the cyber domain when they assert they are currently ill-equipped to confront China in their own domain.[39] China's cyber force cyber operators outnumber the CMF almost 10:1 and are assessed as very capable; the additional increase in the

32. Martin Matishak, "Cyber Command Reshuffles Force Expansion Due to Navy Readiness Woes," *The Record*, 14 June 2023, https://therecord.media/.

33. Erica Lonergan and Mark Montgomery, *Cyber Force: A Defense Imperative* (Foundation for Defense of Democracies Press, March 2024), 6, https://www.fdd.org/.

34. Lonergan and Montgomery, 23.

35. Mark Pomerleau, "Following Reforms, Navy Seeing Cyber Mission Force Readiness Improvements," *DefenseScoop*, 22 February 2024, https://defensescoop.com/.

36. Lloyd J. Austin III, *2022 National Defense Strategy of the United States Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (DOD, October 2022), 6.

37. "Cyber Panel" (Air Command and Staff College, Maxwell AFB, AL, 5 December 2023).

38. Amy B. Zegart, *Spies, Lies, and Algorithms: The History and Future of American Intelligence* (Princeton University Press, 2023).

39. Haddick, *Fire on the Water*, 145; and Mark Pomerleau,"Prospective Service Chiefs Pledge to Address Cyber Mission Force Readiness Concerns of Congress," 15 September 2023, https://defensescoop.com/.

CMF to 147 teams will improve the ratio only to 9:1.[40] Although quantity does not always lead to operational success, defending against or attacking an opposing force of the same quality that is nine times larger is not conducive to success. Although it may improve readiness in some areas, recent efforts that have provided CYBERCOM with the enhanced budget authority akin to a special operations command will not result in changes to its capacity, because the services have still retained control over manpower and a majority of the cyber-related funding.[41]

The Case for a DAF Cyber Force

Today, the only warfighting domain that does not have a separate service is cyber.[42] Only an independent cyber force will provide the requisite autonomy to develop service-unique doctrine, education, and training to compete against China.

One benefit of a separate cyber force is that there will be a single organization that will prioritize that mission as much as the other services prioritize their own. Currently, the services have not promoted officers with technical competency to senior levels, with only 5 out of 45 general officers working cyber jobs having any technical experience.[43] An independent cyber force could promote personnel based on cyber competency rather than Army, Air Force, Space Force, Marine, or Navy experience.[44] It could also standardize training and incentives to develop and retain the right personnel; for example, an independent cyber force could provide more bonuses to personnel who have a higher number of certifications or greater technical proficiency.[45] CYBERCOM, with enhanced budget authority, could set the training standards; however, in the end, the services would be the ones that promote and retain cyber personnel based on their own domain-specific requirements. Thus, only as an independent service can a cyber force advocate to increase its size dramatically and readiness levels accordingly.

Additionally, a separate cyber force can develop service-centric doctrine, strategy, and professional military education to create leaders who have an innate understanding of cyber operations and who can best employ them. This stance echoes historical arguments for an independent Air Force from the 1920s, when leaders advocated that only an air-minded person could best implement airpower.[46] Such perspectives, coupled with the belief that the United States was losing its qualitative edge in space, led

40. Pomerleau, "Cyber Command"; Meredith Roaten, "JUST IN: China Flexes Cyber Strength in India," *National Defense*, 3 March 2021, https://www.nationaldefensemagazine.org/; and Mark Pomerleau, "Russia and China Devote More Cyber Forces to Offensive Operations Than US, Says New Report," *C4ISRNet*, 15 February 2022, https://www.c4isrnet.com/.

41. Lonergan and Montgomery, *Cyber Force*, 11, 12.

42. Lonergan and Montgomery, 7.

43. Lonergan and Montgomery, 20.

44. Lonergan and Montgomery, 6, 14; and Jeffrey Couillard, "Beyond USCYBERCOM: The Need to Establish a Dedicated U.S. Cyber Military Force," *Cyber Defense Review* 9, no. 1 (Spring 2024): 68.

45. Lonergan and Montgomery, *Cyber Force*.

46. William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military* (University of Alabama Press, 2009), 221.

to the Space Force's creation.[47] With the looming threat of war with China, the United States cannot afford to wait until after a conflict to justify an independent cyber force, as it did with the Air Force in 1947.[48]

While a separate cyber department would be ideal, political objections to establishing additional bureaucratic overhead would likely call for the creation of a cyber force under an existing department.[49] Wisconsin Representative Mike Gallagher, the former chairman of the House Armed Services Committee's cyber, innovative technologies, and information systems subcommittee, has expressed hesitancy to create extra bureaucracy without a clear cyber benefit.[50]

As argued, the DAF would be the best department for this new force due in part to its small size—the smallest number of forces across the services. Even with its recently created Space Force and a notional cyber force of 30,000 personnel—which would be five times the current CMF size—a DAF cyber force would still represent an active-duty force smaller than either the Department of the Army or the Navy by more than 82,500 personnel and 144,800 personnel, respectively.[51] As mentioned earlier, such a cyber force would be initially comprised of the 6,000 personnel and capabilities transferred from the services, with plans to rapidly grow the force. The services and agencies would thus retain most of their cyber workforce, since only 2.6 percent of the over 225,000-strong DOD cyber workforce would be transferred.[52]

Some have argued that the Department of the Army would be a logical fit for a cyber force since it has only one service; for a busy congressperson, that is a simple and easy argument to understand.[53] Others have noted that Army officials have been making the right decisions regarding cyber, and the Army provides capable cyber forces like the Air Force and a majority of the resources.[54] Yet, even though the Army comprises only one service, it is the largest service with 445,000 active-duty members.[55] Additionally, while the Army has focused on cyber in recent years, its efforts center on the integration of cyber and electronic warfare to support land

47. Smith, "High Ground."

48. William P. Head, "The Berlin Airlift: First Test of the US Air Force," *Air Power History* 68, no. 3 (Fall 2021): 23, https://www.jstor.org/.

49. Margaret A. Best et al., *Defense Efficiency Initiatives: Observations on DOD's Reported Reductions to Its Headquarters and Administrative Activities* (GAO, 24 September 2018), https://www.gao.gov/; and Jaspreet Gill, "Lawmaker 'Definitely' Considering Value of Independent Cyber Force but Wants More Study," *Breaking Defense*, 10 February 2023, https://breakingdefense.com/.

50. Gill.

51. NDAA for FY 2025, 189.

52. DOD News, "DOD Releases Plan for Implementing Cyber Workforce Strategy," DOD, 3 August 2023, https://www.defense.gov/.

53. Military Cyber Professionals Association (MCPA), "HammerCon 2023: US Cyber Force Panel (Schafer, Cleary, Franz, and Montgomery)," 18 May 2023, uploaded 13 June 2023, YouTube video, 47:25, https://youtu.be/.

54. MCPA.

55. NDAA for FY 2025, 89.

operations.[56] In fact, the top priority for the Army's Cyber Center of Excellence is an electronic warfare systems pack for tactical Army units.[57] The Army's tactical focus on integrating cyber and electronic warfare thus seeks to support the land domain versus strategic cyber operations. While the Air Force has announced it is now also building tactical cyber capabilities to support air superiority, it has not identified this effort as its main cyber priority.[58]

While size is one aspect that warrants placing the cyber force in the DAF, a flexible and innovative culture is another factor where the Air Force comes out ahead. Culturally, the Air Force is the best department for a cyber force. Despite some initial growing pains, the addition of the Space Force demonstrates the Air Force has already shown it can foster an innovative culture. On the other hand, the Army and Navy both tend to adhere to a sense of orthodoxy and set of beliefs that their respective domains are the most important, with the Army maintaining the centrality of the land domain since its founding in 1775, and the Navy seeing itself as an institution older than the United States.[59] Conversely, from 2005 to 2021, the Air Force mission statement included air, space, and cyberspace, demonstrating the importance the service has ascribed to the cyber domain.[60] The DAF also was one of the first services to recognize the importance of cyber, creating a separate dedicated career field in 2010, almost four years before the Army did.[61] Air Force culture also emphasizes technical competence and flexibility, traits that experts argue would be well-suited for a cyber force.[62]

Additionally, as former Secretary of the Air Force Frank Kendall has testified, the DAF has given wide latitude to the Space Force to create a modern talent management framework that includes eliminating episodic physical fitness testing.[63] Similar to the Space Force, experts also believe that new talent management policies will be required to recruit cyber force personnel who may not fit the traditional view of what a service member

56. Lauren C. Williams, "Preparing for Electronic Warfare Is the Army's Top Cyber Priority in 2024," *Defense One*, 22 March 2024, https://www.defenseone.com/.

57. Williams.

58. Mark Pomerleau, " 'This Is Overdue'—Air Force Creating Tactical Cyber Capabilities to Ensure Air Superiority," *DefenseScoop*, 23 May 2024, https://defensescoop.com/.

59. Zimmerman et al., *Movement and Manuever*, xiv, xv; and Oriana Pawlyk, "Air Force Drops 'Space,' 'Cyber' from Mission Statement as Space Force Gains Momentum," Military.com, 8 April 2021, https://www.military.com/.

60. Zimmerman et al., xv ; and Joshua Dewberry, "Air Force Unveils New Mission Statement," Nellis AFB (website), 8 April 2021, https://www.nellis.af.mil/.

61. Susan Griggs, "New Officer Course Boosts Cyberspace Transformation," Air Education and Training Command, 16 June 2010, https://www.aetc.af.mil/; and Federal News Radio Custom Media, "Army to Recruit Next Generation of Cyber Workers Through New Career Field," *Federal News Network*, 18 September 2014, https://federalnewsnetwork.com/.

62. Zimmerman et al., *Movement and Maneuver*, 77; and Lonergan and Montgomery, *Cyber Force*.

63. *DAF Posture Statement FY 2024*, 8.

should look like.[64] Thus, the DAF would culturally be the best fit for the proposed cyber force, allowing it the freedom to innovate a new force construct.

Conclusion

China is developing cyber capabilities that, if left unchecked, will allow it to gain a competitive advantage in the cyber domain, negating any advantages the United States may have in other domains, including those created by improved kinetic strike capabilities.[65] All of the planned upgrades to kinetic systems will likely be integrated into Joint All-Domain Command and Control that only present additional vulnerabilities if they are not defended.[66] The current approach that increases the Cyber Mission Force by a modest 11 percent but keeps cyber professionals subordinate to their own respective services will not result in the force required to confront a well-equipped and well-trained force that is nine times larger, no matter what changes are made to readiness or cyber strategy. Only an independent cyber force can leverage service parochialism to its benefit in order to dramatically increase its size and innovate new doctrine and education. A separate department would likely best employ those capabilities, but political pushback on creating additional bureaucratic overhead would force the service to be created under a current department. Clearly, the Department of the Air Force is the best choice. *Æ*

64. Henry L. Sims, "Enacting the U.S. Cyber Force: The Key to Winning the Great Cyber Competition with China" (thesis, Naval War College, 23 February 2023), 10, https://apps.dtic.mil/.

65. John A. Tirpak, "Kendall: Ratio of Fighters to Bombers May Shift Toward Bombers in the Future," *Air & Space Forces Magazine*, 2 May 2023, https://www.airandspaceforces.com/.

66. Tirpak.