STUDENT NOTES

Outsourcing the Cyber Kill Chain: Reinforcing the Cyber Mission Force and Allowing Increased Contractor Support of Cyber Operations

Homer A. La Rue*

* Homer A. La Rue is a J.D. candidate at Georgetown University Law Center, Class of 2022, and currently serves the U.S. Department of Defense as a warranted contracting officer. He would like to express deep gratitude to Professor Mary B. DeRosa for her generous feedback and guidance. In addition, the author would like to extend special thanks to the Journal of National Security Law & Policy Managing Editors, Staff Editors, and LLMs who contributed such thoughtful edits to this paper. Disclaimer: This article represents the opinions of the author, and does not represent the opinions, views, or policy of his agency, the Department of Defense or any component thereof, or the United States Government.

INTRODUCTION

The United States is under persistent and increasing threat of cyberattack.[1] As the successful attacks against SolarWinds,[2] Microsoft,[3] and Colonial Pipeline[4] indicate, the U.S. is still working to secure critical supply chains and infrastructure against future attacks.[5] In addition to efforts to make the U.S. more resilient to attack, the United States has responded to the growing cyber threat by committing U.S. Cyber Command to more assertive and persistent peacetime confrontation of cyber adversaries.[6]

This more-assertive U.S. cyber strategy will require the Department of Defense (DoD) Cyber Mission Force (CMF) to conduct more cyber operations.[7] However, the CMF force structure and size were not designed with this new

1. A Proclamation on Cybersecurity Awareness Month, 2021, WHITE HOUSE, (Sept. 30, 2021), https://perma.cc/P3JJ-NMF5. This paper uses the term 'cyber-attack' as it is defined by the U.S. National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC). The CRSC defines a 'cyber-attack' as "[a]n attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." *Cyber Attack*, NAT'L INST. OF STANDARDS & TECH., (Dec. 2, 2021), https://perma.cc/3MW7-WWZR.

2. Robert Morgus, *The SolarWinds Breach Is a Failure of U.S. Cyber Strategy*, LAWFARE BLOG (Dec. 18, 2020, 8:01 AM), https://perma.cc/6FFV-S7HD.

3. Thomas Brewster, *Warning: 'Extremely Serious' Microsoft Vulnerabilities Hacked By Ransomware Criminals*, FORBES (Aug. 23, 2021, 6:33 AM), https://perma.cc/Q2FD-P2DV.

4. David E. Sanger & Nicole Perlroth, *F.B.I. Identifies Group Behind Pipeline Hack*, N.Y. TIMES (May 10, 2021), https://perma.cc/KR8F-5B7P.

5. This task is made more difficult by the fact that so much of U.S. critical infrastructure is owned and controlled by private industry. INT'L INST. FOR STRATEGIC STUD., CYBER CAPABILITIES AND NATIONAL POWER - A NET ASSESSMENT, 16 (2021), https://perma.cc/4MVE-W656.

6. Paul M. Nakasone, *A Cyber Force for Persistent Operations*, 92 JOINT FORCE Q. 10 (2019), https://perma.cc/9VKD-XJQG. *See also* Vishnu Kannan, *What Really Happened in the Cyber Command Action Against Iran?*, LAWFARE BLOG (July 11, 2019, 10:15 AM), https://perma.cc/6DCN-65MT; Robert Chesney, *Persistently Engaging TrickBot: USCYBERCOM Takes on a Notorious Botnet*, LAWFARE BLOG (Oct. 12, 2020, 3:53 PM), https://perma.cc/M8TA-BLUH.

7. This paper uses the term "cyber operations" to refer to "the employment of cyber capabilities to achieve objectives in or through cyberspace." TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 564 (Michael N. Schmitt ed., 2017), [hereinafter Tallinn Manual 2.0]. That definition is sufficient for the purposes of this paper, though DoD distinguishes offensive cyber operations from defensive cyber operations. *See* CATHERINE A. THEOHARY, CONG. RSCH. SERV., IF10537, *DEFENSE PRIMER: CYBERSPACE OPERATIONS* 1 (2021), https://perma.cc/3ABC-TT63.

operational strategy or threat picture in mind.[8] Thus, as some members of the Cyberspace Solarium Commission have suggested, the DoD will need to provide the CMF with the "resourcing, force size and capability mix" appropriate to its new operational responsibilities.[9] This paper argues that the best way to reinforce the CMF, in the short term, is to allow greater private-contractor participation in support of Cyber Command's gray-zone cyber operations.[10]

This paper proceeds in four parts. Part I describes the urgent need to reinforce the CMF in light of the persistent and increasing threat of cyberattacks against the U.S. and the CMF's increased deterrence responsibilities. Part II uses the Cyber Operation Kill Chain model[11] to examine the current role contractors play in supporting Cyber Command's operations. Cyber Command only utilizes contractor personnel in the initial phases of its cyber operations but should reinforce the CMF with more liberal utilization of contractor support throughout the rest of the kill chain.

Part II also discusses two important scope limitations related to this paper's primary recommendation. First, increased contractor participation in cyber operations will not solve the systemic issues impacting the nation's ability to recruit and retain an adequate cyber workforce.[12] That is a long-term challenge that will require smart policy choices and significant investment by both the private and public sectors.[13] Second, this paper's recommendation is also scope-limited in that it applies only to gray-zone cyber operations.[14] History suggests, private participation in high-intensity international conflict makes command and control more

8. Erica D. Lonergan & Shawn W. Lonergan, *To Defend forward, the U.S. Must Strengthen the Cyber Mission Force*, LAWFARE BLOG (Mar. 13, 2020, 8:00 AM), https://perma.cc/PNY5-H4LZ.

9. *Id.*

10. Geopolitical competition includes an increasing amount of conduct, including some cyber operations, that exist beyond the threshold of conventional diplomacy but fall short of conventional war. This liminal space is often referred to as the "Gray Zone." *See* Nakasone, *supra* note 6; KATHLEEN H. HICKS, ALICE HUNT FRIEND, JOSEPH FEDERICI, HIJAB SHAH, MEGAN DONAHOE, MATTHEW CONKLIN, ASYA AKCA, MICHAEL MATLAGA & LINDSEY SHEPPARD, BY OTHER MEANS, PART II: ADAPTING TO COMPETE IN THE GRAY ZONE (2019), https://perma.cc/33AB-UURH; Robert Chesney, *Covert Military Information Operations and the New NDAA: The Law of the Gray Zone Evolves*, LAWFARE BLOG (Dec. 10, 2019, 5:03 PM), https://perma.cc/9N8G-SN7N.

11. The kill-chain model segments cyber operations into models where overall operational success depends on successfully completing each model in turn. *See* ERIC HUTCHINS, MICHAEL CLOPPERT & ROHAN AMIN, INTELLIGENCE-DRIVEN COMPUTER NETWORK DEFENSE INFORMATION BY ANALYSIS OF ADVERSARY CAMPAIGNS AND INTRUSION KILL CHAINS (2011), https://perma.cc/473U-RK7S.

12. *See, e.g.*, INT'L INFO. SYS. SEC. CERTIFICATION CONSORTIUM, (ISC)^2 CYBERSECURITY WORKFORCE STUDY, 2021 (2021), https://perma.cc/34V3-9CGG; DEP'T OF COM. & DEP'T OF HOMELAND SEC., Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce, 2-3 (2017), https://perma.cc/AY3D-SW44; *See* BORIS GRANOVSKIY, CONG. RSCH. SERV., IF10654, CHALLENGES IN CYBERSECURITY EDUCATION AND WORKFORCE DEVELOPMENT 3 (2017), https://perma.cc/U5KL-RF3S.

13. This paper's recommendation may even exacerbate some of the cyber workforce challenges by increasing the demand for scarce private sector talent. Indeed, as discussed *infra* in Part II and Part IV, there are serious risks associated with a permanently augmenting U.S. cyber operations with increased contractor participation.

14. *See* HICKS ET AL., *supra* note 10.

challenging and introduces the potential for unwanted escalation.[15] In addition, more aggressive cyber operations—those analogous to an armed attack or coincident to actual armed conflict—will likely implicate the international law of war.[16] Therefore, as explained in Part II, contractors should only be granted an expanded role in those cyber operations that fall below the use of force threshold.[17]

Part III explains the advantages of increased contractor support to U.S. cyber operations. The first is that it is one of the only ways—at least in the immediate term—to reinforce the CMF that would not require any new legal or regulatory authority. Additionally, it would allow cyber command to fully leverage its access to the cybersecurity talent in the U.S. technology sector. This Part also describes the ways that this proposal would minimize the command-and-control risks presented by other public-private collaboration models targeting the cyber threat.

Lastly, Part IV addresses two of the main risks associated with expanding the scope of contractor participation in U.S. cyber operations. The first is that aggressive outsourcing of cyber operations by the United States may further normalize the long-term global use of third-party proxy forces. This risk must be taken seriously because not all of the United States' rivals will (or can) exert the same level of control over their cyber proxies as Cyber Command does over its contractors. Additionally, increased outsourcing may make it harder for the CMF to recruit and retain cyber operators by growing the private market for cybersecurity professionals. These are real risks, but they can be lessened if Cyber Command reduces its use of contractor support once the conventional CMF achieves an adequate force size and capability mix.

I. THE U.S. NEEDS TO REINFORCE ITS CYBER MISSION FORCE

A. The United States is Under Persistent and Increasing Threat of Cyber-Attack

On the eve of 2021 Cybersecurity Awareness Month, President Biden asserted that the United States is "under a constant and ever-increasing threat from malicious cyber actors."[18] At least three factors support his conclusion. First, many of the sophisticated tools, techniques, and personnel that birthed U.S. cyber supremacy are now regularly weaponized against U.S. targets.[19] Second, Russia, Iran, and other rivals have made information operations and gray-zone cyber confrontation central to their strategies for peacetime international competition. That propensity towards cyber aggression amplifies the threat posed by those countries' growing technical sophistication. Finally, ransomware presents a critical and persistent threat to the U.S. because it is a highly profitable criminal enterprise with very low barriers to entry.

---

15. *See, e.g.*, WILLIAM R. CASTO, FOREIGN AFFAIRS AND THE CONSTITUTION IN THE AGE OF FIGHTING SAIL, 91-102 (2006) (discussing the Citizen Genêt Affair and the prizes profit-motivated U.S. privateers took in defiance of President Washington's 1793 Proclamation of Neutrality).

16. *See* Oona A. Hathaway, Rebecca Crootof, Philip Levitz & Haley Nix, *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 821 (2012).

17. *See* Irving Lachow & Taylor Grossman, *Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations*, *in* BYTES, BOMBS, AND SPIES 382 (Herbert Lin & Amy Zegart eds., 2018).

18. A Proclamation on Cybersecurity Awareness Month, 2021, *supra* note 1.

19. *See, e.g.*, Nicole Perlroth, *How the United States Lost to Hackers*, N.Y. TIMES (Feb. 6, 2021), https://perma.cc/25LU-QAR8.

First, although the U.S. was once the world's sole cyber superpower, it no longer has a monopoly on the tools, techniques, and personnel that birthed its cyber supremacy.[20] In fact, many of the most powerful digital weapons in the U.S. arsenal were leaked online in 2017[21] and now regularly appear as components of cyberweapons used against the U.S. and its allies.[22] Additionally, cyber talent is now a global resource and foreign companies (some of them poorly concealed fronts for foreign intelligence services) are increasingly recruiting U.S. talent to serve their own interests.[23] In one infamous incident, a former NSA analyst working on a CyberPoint contract for the United Arab Emirates, participated in a hack against former First Lady Michelle Obama.[24] In short, the threat actors have become more sophisticated and dangerous[25] through a combination of new tools, techniques, and other resources.

Second, perhaps deterred from direct confrontation with conventional U.S. military forces, many rival nations have turned to gray-zone cyberspace operations as a form of day-to-day competition with the United States.[26] These countries weave cyber-enabled influence and subversion operations into their strategies for everyday international competition.[27] These relatively aggressive cyber campaigns compound the threat posed by a rise in global technical sophistication.[28] The U.S. has been slow to contest this strategy. As described by IISS in their report on Cyber Capabilities and National Power, "[t]he US and its closest allies have the most technically sophisticated tools . . . but their use of those tools is highly constrained."[29] In contrast, countries like Russia, China, and Iran are

20. *See, e.g.*, Perlroth, *supra* note 19 ("Three decades ago, the United States spawned, then cornered, the market for hackers, their tradecraft, and their tools. But over the past decade, its lead has been slipping, and those same hacks have come boomeranging back on us"); *but see* INT'L INST. FOR STRATEGIC STUD., *supra* note 5, at 15 (arguing that offensive cyber capability is merely one of seven interrelated measures of cyber power and that the U.S. is still "the only country with a heavy global footprint in both civil and military uses of cyberspace").

21. Perlroth, *supra* note 19; Brian Krebs, *WikiLeaks Dumps Docs on CIA's Hacking Tools*, KREBS ON SEC. (Mar. 8, 2017), https://perma.cc/E4QH-RVXW.

22. *See, e.g.*, Brian Krebs, *'Petya' Ransomware Outbreak Goes Global*, KREBS ON SEC. (June 27, 2017), https://perma.cc/2FYU-ALL6 (describing the discovery that the WannaCry ransomware – widely attributed to North Korea – and certain strains of the Petya malware that devastated Ukraine in 2017 contained a digital weapon believed to have originated within the U.S. National Security Agency called "Eternal Blue").

23. *See* Perlroth, *supra* note 19.

24. *Id.*

25. Christopher Wray, Dir., Fed. Bureau of Investigation, Remarks at the Boston Conference on Cyber Security: Tackling the Cyber Threat Through Partnerships and Innovation (Mar. 4, 2020), https://perma.cc/S92T-SABQ.

26. DEP'T OF DEF., OFF. OF THE CHIEF INFO. OFFICER, 2018 DOD CYBER STRATEGY AND CYBER POSTURE REV. (2018).

27. Iran, for example, learned well the force multiplying potential of a sophisticated hacking program when the U.S. and Israel destroyed a fifth of its nuclear centrifuges with the Stuxnet bug. In response, Tehran built a world-class cyber program, from scratch, for the approximate cost of three F-35 stealth bombers. *See* NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS 270 (2021).

28. *See, e.g.*, Gary Corn, *Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses*, JUST SECURITY (Feb. 11, 2020), https://perma.cc/GC5T-DECG.

29. INT'L INST. FOR STRATEGIC STUD., *supra* note 5, at 172.

able to "punch above [their] cyber weight" through a willingness to make "more extensive use of less technically sophisticated capabilities."[30] To be sure, U.S. cyber policy under "defend forward" is now more overtly aggressive with respect to launching gray-zone cyber operations.[31] But that doctrinal shift only moves U.S. policy closer to that of its rivals. The growing international inclination towards gray-zone competition suggests that the threat to U.S. networks and infrastructure will persist.

Finally, ransomware presents a critical and persistent threat to the United States because it is a highly profitable criminal enterprise with very low barriers to entry.[32] The FBI received nearly 2,500 ransomware complaints in 2020 alone.[33] The increasing prevalence of cryptocurrency and cyber insurance may be contributing to the profitability of ransomware attacks by indemnifying victims and facilitating payments.[34] Further, "the barriers to entry into this lucrative criminal enterprise have become shockingly low."[35] For example, the attack at Colonial Pipelines did not require the resources or sophistication of a nation-state actor like China or Iran, it was an act of extortion perpetrated by a criminal gang of hackers.[36] Worse, the explosive growth in Ransomware-as-a-Service (RaaS) attacks in 2020 ensures that any sufficiently resourced threat actor, even those lacking any malware-development sophistication, can still launch ransomware attacks against American targets.[37]

The rise of ransomware, the growing number of sophisticated threat actors, and the increasing number of national governments pursuing cyber and

30. *Id.* at 172-173.

31. *Id.*

32. Ransomware refers to "the use of malicious software to deny users access to data and information systems to extort ransom payments from victims." PETER G. BERRIS & JONATHAN M. GAFFNEY, CONG. RSCH. SERV., R46932, RANSOMWARE AND FEDERAL LAW: CYBERCRIME AND CYBERSECURITY (Oct. 5, 2021).

33. *Id.*

34. INST. FOR SEC. AND TECH. COMBATING RANSOMWARE: A COMPREHENSIVE FRAMEWORK FOR ACTION, 13 (2021). Yet, this is not to say that cyber insurance is valueless. Eligibility for cyber insurance often requires the insured to assess their cyber controls and harden themselves against known cyber risks like ransomware. Scott J. Shackleford, *Wargames: Analyzing the Act of War Exclusion in Insurance Coverage and Its Implications for Cybern security Policy*, 23 YALE J. L. & TECH. 362, 386–87 (2021). Further, because cyber insurance can be prohibitively expensive, insurers incentivize investment by offering premium discounts to organizations with sophisticated cyber security programs. *Id.*

35. COMBATTING RANSOMWARE, *supra* note 34, at 5.

36. Sanger and Perlroth, *supra* note 4. To be sure, Cyber Command may not have as clear a role in addressing purely criminal conduct, especially where the ransomware originates from a domestic threat actor or targets a purely private entity unrelated to U.S. critical infrastructure. However, nation-state actors like North Korea also launch ransomware and other complex digital extortion schemes that do implicate Cyber Command's core mission. INT'L INST. FOR STRATEGIC STUD., *supra* note 5, at 126.

37. COMBATTING RANSOMWARE, *supra* note 34, at 16 (explaining that RaaS "is a business model that provides ransomware capabilities to would-be criminals who do not have the skills or resources to develop their own malware . . . [It] follows similar evolutions in the mainstream software and infrastructure industries, which have seen success from "software as a service" and "infrastructure as a service" business models."). By at least one count, two-thirds of the ransomware attacks in 2020 used this model. *Id.*

information operations to advance their strategic interests are not the only factors contributing to the near-constant barrage of cyber attacks against the U.S. The inherent vulnerability of U.S. critical infrastructure[38] and lack of internationally-recognized cyber norms[39] also present persistent and critical challenges.

B. Cyber Command Will Conduct More Cyber Operations

The U.S. has responded to the intensifying cyber threat, in part, with an increased appetite for low-level conflict in cyberspace.[40] The "defend forward" and "persistent engagement" doctrines, advanced by the 2018 Department of Defense Cyber Strategy, reflect this more assertive posture.[41] Defend forward describes efforts to preempt, defeat, or deter cyber-attacks at their source and before they reach U.S. targets.[42] As the Solarium Commission observed, defending forward in cyber mirrors the U.S. military's strategic posture after World War II.[43] There, the U.S. and allied forces positioned themselves at or near the potential epicenters of the "next war."[44] The Cyber Strategy's pledge of "persistent engagement" describes a renewed commitment to constant competition with adversary cyber operators in defense of national interests.[45] Both doctrines indicate that the U.S. is moving away from the more restrained and conservative cyber policies of the last decade,[46] and will engage in a greater number of gray-zone cyber operations.[47]

---

38. *See* Sanger and Perlroth, *supra* note 4.

39. Michael P. Fischerkeller, *Initiative Persistence and the Consequence for Cyber Norms*, LAWFARE BLOG (Nov. 8, 2021), https://perma.cc/6FUF-YDZR.

40. Warren P. Strobel, *Bolton Says U.S. Is Expanding Offensive Cyber Operations*, WALL ST. J. (June 11, 2019, 1:59 PM), https://perma.cc/Q4RH-ZFBD.

41. U.S. DEP'T OF DEF., SUMMARY DEPARTMENT OF DEFENSE CYBER STRATEGY (2018) [hereinafter 2018 Department of Defense Cyber Strategy].

42. *Id.* at 2.

43. U.S. CYBER SPACE SOLARIUM COMM'N, SOLARIUM COMMISSION FINAL REP. 182 (Mar. 2020). The Cyberspace Solarium Commission is a bipartisan, intergovernmental body created by the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to develop a strategic approach to defense against cyberattacks. The CSC delivered its final report in March of 2020 which embraced the DoD's defend forward approach and build upon it to recommend a whole of nation approach to cyber security. *Id.*

44. *Id.* at 26.; Through proximity and commitment of resources, forward deployment was meant to detect Soviet aggression and impose deterrent costs in real-time. *Id.*

45. INT'L INST. FOR STRATEGIC STUD., *supra* note 5, at 16.

46. *See* Karen Parrish, *Lynn: Cyber Strategy's Thrust is Defensive*, AMERICAN FORCES PRESS SERV. (July 14, 2011), https://perma.cc/PY3H-CWYL; *see also* Michael Warner, *U.S. Cyber Command's First Decade*, LAWFARE BLOG (Dec. 8, 2020, 10:53 AM), https://perma.cc/N33N-JWJE (detailing Cyber Command's initial years and early defensive focus); Press Release, Robert Gibbs, White House Press Secretary, Statement by the Press Secretary on Conclusion of the Cyberspace Review, (Apr. 17, 2009), https://perma.cc/ZU4D-FEHX (discussing a Whitehouse cyber-policy review that prioritized "building a reliable, resilient, trustworthy digital infrastructure for the future").

47. Dustin Volz, *Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive*, WALL ST. J, (Aug. 16, 2018, 11:36 PM), https://perma.cc/AHC8-SCQG; Paul McLeary, *Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff*, BREAKING DEF. (Sept. 17, 2018, 5:30 PM), https://perma.cc/VB3R-NCVG; Mark Pomerleau, *New Authorities Mean Lots of New Missions at Cyber Command*, FIFTH DOMAIN (May 8, 2019), https://perma.cc/7WGU-VQ3V.

To be sure, the U.S. government classifies the details (and in many cases, the existence) of many of its cyber operations.[48] Nevertheless, several U.S. cyber operations have made the news in recent years. These include actions against: the Russian power grid,[49] Iranian hackers seeking to disrupt the 2020 Presidential Election,[50] Iranian weapons systems in retaliation for the downing of a U.S. drone,[51] and the world's largest botnet.[52] As these operations suggest, the U.S. has responded to the growing cyber threat by adopting a more bellicose attitude towards gray-zone cyber competition and operations against digital adversaries.[53]

C. The CMF was not Designed for Defend Forward or Persistent Engagement

The CMF is tasked with efforts to "counter, disrupt, and impose costs for malicious adversary behavior in cyber space."[54] Organized under the authority of the U.S. Cyber Command, the CMF includes more than 6,000 individuals organized into 133 mission teams.[55] But the CMF's structure, force size, and capability mix were determined in 2013, before the U.S. began to signal its increased appetite for gray-zone cyber operations.[56] As some members of the Solarium Commission have argued, to conduct the volume of routine cyber operations required to defend forward successfully, the U.S. must strengthen and reinforce the CMF.[57] A number of workforce development issues—many of them common to the broader cybersecurity labor market—make it a challenge to recruit and retain workers for the CMF.

First, the CMF must draw talent from the broader "cybersecurity workforce"[58] where cybersecurity professionals are globally scarce and in high demand.[59] A

48. As a matter of policy and to protect operational security, the Pentagon and Cyber Command do not typically discuss cyber operations. *See, e.g.*, Kannan, *supra* note 6 (discussing unanswered questions about a previous action launched by Cybercom against Iranian targets in 2019). Incidentally, this is also why this paper focuses on cyber operations conducted by U.S. Cyber Command as opposed to the Central Intelligence Agency or the U.S. Intelligence Community (IC). CIA cyber operations may (or may) not be more numerous but the IC is relatively less likely to publicly state its strategic initiatives or avow individual operations. INT'L INST. FOR STRATEGIC STUD., *supra* note 5, at 22.

49. David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid*, N.Y. TIMES (Jun. 15, 2019), https://perma.cc/BC3D-B63Y.

50. Ellen Nakashima, *U.S. Undertook Cyber Operation Against Iran as Part of Effort to Secure the 2020 Election*, WASH. POST, (Nov. 3, 2020), https://perma.cc/99PN-MZV8.

51. *US Launched Cyberattacks on Iran Weapons Systems,* AL JAZEERA (Jun. 23, 2019), https://perma.cc/CN2E-HEPV.

52. Chesney, *supra* note 6.

53. Strobel, *supra* note 40.

54. Lonergan and Lonergan, *supra* note 8.

55. Theohary, *supra* note 7.

56. Lonergan & Lonergan, *supra* note 8.

57. *Id.*

58. *Strategic Plan*, NAT'L INST. OF STANDARDS AND TECH. (2016), https://perma.cc/4U7A-V6S8 (defining the members of the cybersecurity workforce as any workers "whose primary focus is on cybersecurity as well as those in the workforce who need specific cybersecurity-related knowledge and skills in order to perform their work in a way that enables organizations to properly manage the cybersecurity-related risks to the enterprise.").

59. (ISC)^2 CYBERSECURITY WORKFORCE STUDY, 2021, *supra* note 12, at 4 (2021).

staggering number of cybersecurity positions go unfilled every year because of a shortage in qualified talent. By one estimate, U.S. organizations (public and private) would need an additional 377,000 cybersecurity professionals to adequately defend their critical assets.[60] The increasing threat of nation-state cyber intrusions and destructive ransomware attacks suggests that the demand for cybersecurity professionals will continue to outpace supply for the foreseeable future.[61]

In addition to the existing cybersecurity workforce shortage, there are also pipeline issues that will make it difficult to grow the CMF at pace. There are many unfilled cybersecurity leadership positions that require advanced technical degrees, multiple certifications, and significant managerial experience.[62] But ensuring the long-term health of the cybersecurity workforce in the U.S.—and by extension, the pool of candidates for the CMF—will require fixes to several critical challenges at the entry levels too. For example, U.S. cybersecurity education suffers from a scarcity of skilled secondary-school teachers, university faculty, and training instructors.[63] This limits the number of new entrants to the cybersecurity workforce and presents a barrier to retraining candidates willing to convert from non-cybersecurity positions.[64]

The relative lack of diversity in the field stands as an additional challenge to growing a strong pipeline of U.S. cybersecurity professionals. Women make up more than half of the U.S. population but barely 14% of the cybersecurity workforce.[65] Similarly, only 3% of U.S. cybersecurity professionals identify as Black or African American.[66] Diversity and inclusion issues in cyber are thorny and have multiple root causes. For one, the previously-mentioned issues hindering access to quality cybersecurity education may well be more acute in minority communities.[67] The wider tech industry also has a well-documented history of hostility towards women, racial minorities, and LGBTQ professionals in the workplace.[68] Whatever the ultimate drivers, the lack of diversity in cybersecurity represents a critical and unresolved barrier to closing the cybersecurity workforce gap.

Finally, in addition to various issues already discussed which affect the broader U.S. cybersecurity workforce, the federal government and CMF face certain particularized challenges in recruiting and retaining cybersecurity professionals.

60. *Id*. at 26.

61. *Id*. at 20.

62. NAT'L INST. OF STANDARDS AND TECH., SUPPORTING THE GROWTH AND SUSTAINMENT OF THE NATION'S CYBERSECURITY WORKFORCE: BUILDING THE FOUNDATION FOR A MORE SECURE AMERICAN FUTURE, 1 (2017) [hereinafter NIST Workforce Report 2017].

63. *Id*. at 2.

64. *Id*.

65. Taavi Must, *How to Address The Lack of Diversity in Cybersecurity*, FORBES (Apr. 23, 2021), https://perma.cc/FBS8-PEYH.

66. *Id*.

67. *Id*.; NAT'L INST. OF STANDARDS AND TECH Y, *supra* note 58; *see generally Diversity, Equity, and Inclusion Resource Center*, INT'L INFO. SYS. SEC. CERTIFICATION CONSORTIUM, https://perma.cc/7MXT-4WCC.

68. *See, e.g*., KAPOR CTR. FOR SOC. IMPACT, TECH LEAVERS STUDY, (Apr. 17, 2017).

Researchers often cite the government's antiquated pay structure, opaque and inefficient hiring processes, and the higher salaries for comparable private-sector work as significant obstacles to growing the cybersecurity workforce.[69] Additionally, and depending upon the position to be filled, the security clearance process can be lengthy and complicated.[70] While programs that might strengthen the CMF in the long term already exist,[71] outsourcing a larger portion of gray-zone operations to private contractors might be a viable short-term solution to the current workforce gap.

II. CYBER COMMAND SHOULD REINFORCE THE CMF WITH CONTRACTOR SUPPORT

A. Background: The Cyber Operation Kill Chain and Current Levels of Outsourcing

Researchers from Lockheed Martin introduced their cyber kill-chain model in 2011, which they described as a "systematic process to target and engage an adversary to create desired effects."[72] The model suggested that cyber intrusions have a common modular structure and that the ultimate success of a cyber operation (from the intruder's perspective) depended on achieving success at each individual stage of the chain.[73] This paper adopts the kill chain model to illustrate the scope of current contractor support of U.S. cyber operations and to assess the opportunities for increased participation.[74]

1. The Cyber Operation Kill Chain

Under the cyber operation kill chain model, a cyber operation will have seven steps. These steps include Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives. To complete

69. Granovskiy, *supra* note 12.

70. *Investigations and Clearance Processes at a Glance*, DEF. AND COUNTERINTEL. AGENCY, https://perma.cc/P95G-LFKR; OFF. OF THE DIR. OF NAT'L INTEL., SECURITY EXECUTIVE AGENT DIRECTIVE-4, NATIONAL ADJUDICATIVE GUIDELINES 6 (Jun. 8, 2017).

71. *See, e.g.*, *What is CyberPatriot?*, AIR FORCE ASSN CYBERPATRIOT WEBSITE, https://perma.cc/378A-NVER; *National Collegiate Cyber Defense Competition*, NAT'L COLLEGIATE CYBER DEF. COMPETITION (2020), https://perma.cc/L6AC-QU25; *Inspiring the Next Generation of Cyber Stars,* GENCYBER, https://perma.cc/F8WF-A4BD.

72. ERIC HUTCHINS, MICHAEL CLOPPERT & ROHAN AMIN, INTELLIGENCE-DRIVEN COMPUTER NETWORK DEFENSE INFORMED BY ANALYSIS OF ADVERSARY CAMPAIGNS AND INTRUSION KILL CHAINS 4 (2011).

73. Irving Lachow & Taylor Grossman, *Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations*, *in* BYTES, BOMBS, AND SPIES 381 (Herbert Lin & Amy Zegart eds., 2018), https://perma.cc/9ZAA-QDQ2.

74. The Lockheed Martin model has been augmented, adapted, and critiqued by other researchers since 2011. *See, e.g.*, MITRE ATT&CK, https://perma.cc/372R-MXC2; Ioan-Cosmin Mihai, Stefan Pruna & Ionut-Daniel Barbu, *Cyber Kill Chain Analysis*, 3 INT'L J. INFO. SEC. & CYBERCRIME 37, 42 (2014); Pete Cooper, *Cognitive Active Cyber Defense: Finding Value Through Hacking Human Nature*, 5 J.L. & CYBER WARFARE, 57–172, 98 (2016), https://perma.cc/B4S9-FRWD. But as Irv Lachow and Taylor Grossman noted in *Cyberwar Inc*., whatever its practical limitations, the basic Lockheed Martin kill-chain model is "a useful construct" for presenting the anatomy of an offensive cyber operation. *See* Lachow & Grossman, *supra* note 73 at 381.

a given cyber operation, the entity initiating the operation must successfully traverse each step of the kill chain in turn. The table below generally describes the seven steps of a typical cyber kill chain.[75]

Phase	Step	Description
Pre-Launch	1. Reconnaissance	Pre-planning, target selection, vulnerability assessments, and exploit development.
	2. Weaponization	Exploit combined with malware to create a deliverable payload of malicious code.
Launch	3. Delivery	Cyber weapon transmitted to its targeted system.
	4. Exploitation	Malicious code activates, taking advantage of the system vulnerability to gain access.
Post-Launch	5. Installation	Weapon installs the payload in the defender's trusted environment.
	6. Command and Control (C2)	Malware opens a channel to the attacker allowing the attacker to send instructions to the defender's system.
	7. Actions on Objectives	Attacker now able to achieve cyber operation mission objectives within the targeted system(s).

As Hutchins, Cloppert, and Amin point out, the steps may be organized "into three broad phases: pre-launch, launch, and post-launch."[76] The Pre-Launch phase includes the Reconnaissance and Weaponization steps of the operation.[77] The Launch phase includes Delivery and Exploitation. And the Post-Launch phase—the ultimate in-network activity of the operation—includes the Installation, Command and Control, and Actions on Objectives steps.[78] As discussed in the next section, private contractors primarily participate in the early phases of U.S. Cyber operations, sometimes up to and including the exploitation step.[79]

75. The chart is based upon Irv Lachow's articulation of the Lockheed Martin model. *See* Irving Lachow, *The Private Sector Role in Offensive Cyber Operations: Benefits, Issues and Challenges*, 1 (2016), https://perma.cc/BK9D-NXKY. It may not fully describe the anatomy of every successful hack, or the weight of resources required at each step.

76. Lachow & Grossman, *supra* note 73 at 382.

77. *Id.*

78. *Id.*

79. *Id.* at 387.

2. Pre-Launch – Current Contractor Participation in the Cyber Kill Chain

The DoD and Intelligence Community (IC) utilize civilian contractor Intelligence, Surveillance, and Reconnaissance (ISR) support in conducting cyber operations. These activities fall within the first step of the kill-chain model and the Pre-Launch phase of the operation. Typical activities delegated to a private contractor include mapping target networks, surveilling users, identifying system vulnerabilities, and bulk data compilation duties.[80] Several companies, even boutique firms, advertise sophisticated signal intelligence services that were once the "near-exclusive domain of government intelligence agencies."[81] And as off-the-shelf spyware tools become more ubiquitous,[82] the barriers to entry for this market segment will continue to fall.

U.S. firms also provide weaponization services. Weaponization is the second step in the kill chain and an element of an offensive cyber operation's (OCO) pre-launch phase. It uses the intelligence gathered through previous ISR efforts to develop an effective payload that is deliverable to the target system. These offensive cyber tools and services often exist in a gray market and are more likely to be offered in secret in response to classified government solicitations.[83] Thus the number of U.S. firms that publicly advertise cyber-weaponization services is understandably smaller. But however clandestine, the market for cyber weapons is substantial and growing.[84] As Nicole Perlroth documented in *This is How They Tell Me the World Ends*, the U.S. government has long paid top dollar to companies, independent hackers, and middlemen willing to sell zero-day exploits and vulnerabilities in secret.[85] And as Tim Maurer noted in *Cyber Mercenaries*, "unlike the development of conventional weaponry, which usually requires substantial investment and manufacturing capabilities, the development of malware for offensive cyber operations has much lower barriers to entry."[86]

C. The Recommendation: Moving Down the Kill Chain

1. Contractors Should Support Every Phase of the Kill Chain

Several legal and prudential considerations currently limit private contractor involvement in U.S. Government cyber operations to the Pre-Launch phase. Private contractors provide ISR support, and in some cases, weaponization services, but are not currently "hands-on-keyboard" for the launch and post-launch phases of offensive cyber operations.[87] For example, although ManTech publicly

80. *Id.* at 383.

81. *Id.*

82. *See, e.g.*, DJ Pangburn, *This Powerful Off-the-Shelf Phone-Hacking Tool is Spreading*, FAST CO. (Sept. 18, 2018), https://perma.cc/F3QS-8NDB.

83. *See* PERLROTH, *supra* note 27, at 41-52 (describing the U.S. Government's early entrée and continued presence in the secretive cyberweapons market); TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER 16-18 (2018) (same).

84. *See* PERLROTH, *supra* note 27 at 137-141.

85. *See generally Id.*

86. MAURER, *supra* note 83, at 75.

87. Lachow & Grossman, *supra* note 73, at 382.

advertises "full-spectrum" cyber operation support and "cyber operations" services, we should not understand this to mean that ManTech employees are actually delivering malicious code into adversary networks or extracting data from targeted systems.[88] A better understanding of their cyber operation support is likely that ManTech employees participate in more *indirect* cyber operation activities like reverse engineering malware or researching vulnerabilities in adversary systems.[89]

But as previously discussed, to successfully conduct the volume of routine cyber operations required to defend forward, the U.S. must strengthen and reinforce the CMF.[90] A number of workforce development issues will make that difficult in the short term. This paper's central argument is that private contractors can help augment the CMF by playing a more central role in U.S. cyber operations. Cyber Command should, in effect, move contractor support down the kill chain into the Launch and Post-Launch phases. In the short term, ManTech, Booz Allen Hamilton, and similarly situated private firms can and should provide support at every phase of the kill chain, at least for those cyber operations normally conducted in the gray-zone as part of routine cyber competition.

2. Scope Limitations: Short Term and Gray-Zone Operations Only

This paper's recommendation is not without risk. Two limits on the scope of expanded contractor participation in U.S. cyber operations will help minimize these risks. First, Cyber Command should expand its use of private contractors only until such time as it determines that the CMF has achieved adequate resourcing, force size, and capability to meet its newly expanded mission. Indeed, there are already a number of efforts in place to develop the CMF and federal cybersecurity workforce.[91] By not allowing this practice to become another one-way ratchet,[92] the U.S. can minimize the risk that its expanded outsourcing will further normalize the use of cyber-proxy forces internationally or that an overheated contract-labor market will inhibit Cyber Command's conventional recruitment efforts.[93]

---

88. *ManTech Cyber Overview*, https://perma.cc/A39B-MJ8C (advertising "full-spectrum cyber" services including "Cyber Network Operations (CNO)" support).

89. *See* MAURER, *supra* note 83, at 74.

90. Lonergan and Lonergan, *supra* note 8.

91. *See Cyber Command Steps Up Recruiting Efforts with Special Hiring Authority*, U.S. DEP'T OF DEF. (Jun. 7, 2018), https://perma.cc/J9HM-3YBJ.

92. *See, e.g.*, Hamdi v. Rumsfeld, 542 U.S. 507, 521-522 (2004) (authorizing the extraordinary practice of detaining enemy combatants, including U.S. citizens, indefinitely and without trial, so long as hostilities in Afghanistan persisted. Presumably the Court did not foresee hostilities, and thus this extraordinary Presidential authority, would persist for another 17 years); *see also* Elizabeth Goitein, *Congress Is Ready for FISA Reform – Will the House Judiciary Committee Rise to the Occasion?*, JUST SECURITY (Feb. 25, 2020), https://perma.cc/3HQK-KPH7 (describing the way that "[t]he politics of fear that underlie most national security debates generally create a one-way ratchet" where seemingly short-term and scope-limited government authorities grow and calcify).

93. See *infra* Part IV for a more detailed discussion of these risks.

This paper's recommendation is also scope-limited in that it applies only to gray-zone cyber operations—the roughly triangulated range of activities that exceed ordinary low-level statecraft but fall below the level of active hostilities.[94] Contractors should only be granted an expanded role in those cyber operations that fall below the use of force threshold, and this prohibition should include barring contractor participation in the type of cyber countermeasures that might trigger armed conflict.[95] To be sure, the threshold for when a cyber operation constitutes an act of war or becomes analogous to the use of force is somewhat of a moving target.[96] In fact, Rule 69 of the Tallinn Manual all but concedes that there is no consensus definition of use of force, even for kinetic operations.[97]

Professor Oona Hathaway and her colleagues may have provided one of the clearest articulation of the threshold in their 2012 paper, *The Law of Cyber Attack*.[98] There they "conclude that the best test of when a cyber-attack is properly considered cyber-warfare is whether the attack results in physical destruction —sometimes called a "kinetic effect"—comparable to a conventional attack."[99] This description of the threshold is not universally accepted and is almost certainly underinclusive.[100] However, it is sufficient for the purposes of this paper and contains the added virtue of a bright-line-rule. Cyber operations below this threshold —for example, missions to penetrate foreign networks, extract specific information, temporarily disrupt network capabilities, or prepare for future operations—are the primary focus of this paper recommendation.

Significantly, many cybersecurity roles and skillsets are interchangeable.[101] The same personnel capable of conducting below-the-threshold operations will generally have sufficient capability to participate in the more destructive,

94. *See* Chesney, *supra* note 10.

95. *See generally* Ashley Deeks, *Defend Forward and Cyber Countermeasures*, 1 (Hoover Working Group on Nat'l Sec., Tech., and Law, Aegis Series Paper No. 2004, Aug. 4 2020), https://perma.cc/E4GZ-DKCJ (emphasizing the importance of "anticipat[ing] the responses that . . . cyber activities may trigger from other states").

96. Michael Schmitt, *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law*, JUST SECURITY (Dec. 21, 2020), https://perma.cc/URQ6-8UYC; Yevgeny Vindman, *Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is*., LAWFARE BLOG (Jan. 26, 2021, 1:24 PM), https://perma.cc/RM7F-4E85.

97. TALLINN MANUAL 2.0, *supra* note 7, at 331 ("There is no authoritative criteria of, or criteria for, 'threat' or 'use of force'.").

98. Hathaway et al., *supra* note 16, at 817. Even this definition is likely under inclusive, since one can imagine non-kinetic cyber operations that are nonetheless so disruptive or debilitating that a victim nation might be justified in considering the operation equivalent to an armed attack. For example, some have argued that the Russian Solar Winds breach "may well constitute a *casus belli* under international law." Yevgeny Vindman, *Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is*., LAWFARE BLOG (Jan. 26, 2021, 1:24 PM), https://perma.cc/H9PR-MR6X.

99. *Id.*

100. For example, the drafters of the *Talinn Manual 2.0* were divided as to whether 2010 Stuxnet operation which caused physical damage in an Iranian nuclear fuel processing plant, met the definition of armed conflict. Tallinn Manual 2.0, *supra* note 7, at 384.

101. *See* MAURER, *supra* note 83, at 39 (noting that it is "relatively easy for actors who usually focus on defense (for example, penetration testers or reverse engineers) to deploy their skills for offensive purposes").

combatant-oriented operations. Through this fungibility of skills, even contractor participation in less belligerent cyber operations will still, at minimum, help reinforce the CMF by freeing up the Department's uniformed and civilian personnel for its above-the-threshold cyber operations.[102]

III. THE ADVANTAGES OF INCREASED CONTRACTOR SUPPORT

A. No Need for New Domestic Legal Authorities

As discussed in this section, Cyber Command's legal authority to conduct cyber operations with contractor support is well established. Yet because under current law and longstanding Executive Branch policy, certain tasks under some cyber operations will constitute Inherently Governmental Functions (IGF), Congress and DoD may need to clarify which components of common cyber operations may be delegated to private parties. This will provide certainty to contracting officers and private industry. Additionally, this section addresses the Computer Fraud and Abuse Act (CFAA) as it relates to outsourced cyber operations. In other contexts, the CFAA is one of several laws that may proscribe unauthorized out-of-network operations conducted by private parties. As discussed below, the CFAA is unlikely to bar increased contractor participation in Cyber Command's operations because private contractors are protected by Cyber Command's existing immunity to CFAA liability. In sum, current domestic legal frameworks likely provide sufficient legal authority to expand contractor participation in Cyber Command's cyber operations.

1. Cyber Command's Legal Authority to Conduct Cyber Operations

Cyber Command's current authority to conduct out-of-network operations flows both from the President's Article II war powers and from statutory grant.[103] The Executive Branch's longstanding view is that the President's Article II powers provide sufficient unilateral authority to conduct cyber operations when "the anticipated nature, scope, and duration of the operations do not rise to the level of war under the Constitution."[104] Under this rationale, "the domestic legal authority for the DoD to conduct cyber operations is included in the broader authorities of the President . . . to conduct military operations in defense of the nation."[105]

And indeed, the Executive often enjoys the last word on the scope of presidential national security powers. The Supreme Court has long assumed that the President has at least some limited, unilateral authority under Article II to protect

102. *See* THEOHARY, *supra* note 7.

103. In spite of this position, a number commentators argue that cyber operations alone are "rarely exercises of constitutional war powers" and thus need no constitutional basis of war power authority. *E.g.*, Mathew C. Waxman, *Cyberattacks and the Constitution* 2, (Hoover Working Group on Nat'l Sec., Tech., and Law, Aegies Series Paper No. 2007, Nov. 10, 2020), https://perma.cc/E6LW-LUA8.

104. Hon. Paul C. Ney, Jr., General Counsel, Dep't of Def., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://perma.cc/L34D-B4WK.

105. *Id.*

U.S. persons, property, and interests.[106] Additionally, the federal courts often infer congressional support for larger-scale Executive use of force from related appropriations and other indirect manifestations of support.[107] Failing that, the courts may simply find other grounds to avoid ruling on the scope of Executive power.[108] Importantly, the Executive's claimed unilateral authority to conduct military operations includes the authority to conduct, at least in the short term, operations that rise above the international law threshold for the use of force.[109] As stated previously, this paper does not contemplate increased contractor participation in such operations, but the authority to use force in cyberspace almost certainly includes the authority to conduct cyber operations below that threshold.

Ultimately Cyber Command's operations need not rely on the Executive's Article II authority alone. Congress answered the question of whether it supported Cyber Command's operations when it passed the John McCain National Defense Authorization Act (NDAA) in 2019. Section 1642 expressly authorized Cyber Command to "take appropriate and proportional action in foreign cyberspace" consistent with the defend-forward concept.[110] Finally, consistent with defend forward and persistent engagement, Cyber Command now has greater delegated authority to launch and manage Cyber Operations without presidential pre-approval.[111]

2. Inherently Governmental Functions

National Security is traditionally understood as a public good provided by sovereign states to their populace.[112] Accordingly, citizens expect the state security

106. *See, e.g.*, The Prize Cases, 67 US 635 (1863); *In re* Neagle, 135 U.S. 1, 63-64 (1890). The Court also has a longstanding (and somewhat controversial) doctrine of deference to the Executive in matters of national security. The courts also have a longstanding (and somewhat controversial) doctrine of deference to the Executive in matters of national security. *See* Shirin Sinar, *Courts Have Been Hiding Behind National Security for Too Long*, BRENNAN CTR. FOR JUST. (Aug. 11, 2021), https://perma.cc/CKY2-HRJC.

107. *See, e.g.*, Orlando v. Laird, 443 F.2d 1039, 1043 (2d. Cir. 1971) (holding that congressional support and authorization for armed conflict may be inferred, even without a formal declaration of war or authorization for use of force, where Congress appropriates funds with the understanding that the executive will use them to support the armed conflict).

108. *See, e.g.*, Dellums v. Bush, 752 F. Supp. 1141, 1152 (D.D.C. 1990) (avoiding the question of George H.W. Bush's authority to send troops to Kuwait prior to the Iraqi invasion on the basis of ripeness); Campbell v. Clinton 203 F.3d 19, 24-25 (D.C. Cir. 2000) (avoiding question of Clinton's authority for air strikes on the basis of standing).

109. *See, e.g.*, John Bellinger, *President Biden's Inaugural War Powers Report*, LAWFARE BLOG (Mar. 1, 2021, 9:18 AM), https://perma.cc/5AEB-9DKW (noting that President Biden relied only on his constitutional authority under Article II when reporting to Congress on the February missile strikes he ordered in eastern Syria and that he did not cite any new statutory authority for the strikes or attempt to justify them under the 2001 or 2002 Congressional Authorizations to Use Military Force (AUMF)).

110. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1642, 132 Stat. 1636, 2132-2133 (2018). Cyber Command may also rely on either AUMF, where appropriate, for authority to conduct a cyber operation. *See* Robert Chesney, *The Domestic Legal Framework for U.S. Military Cyber Operations*, LAWFARE BLOG (Aug. 5, 2020, 11:42 AM), https://perma.cc/AG78-NGM9.

111. *See* Pomerleau, *supra* note 47.

112. *See* U.S. CONST. art. IV, § 4; *see also* P.W. SINGER, CORPORATE WARRIORS: THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 226 (2003).

organs to orchestrate, direct, and execute the nation's core national security missions in a manner consistent with American values and public accountability.[113] U.S. military policy follows that tradition. Thus, Cyber Command's authority to carry out cyber operations does not necessary include the authority to outsource every aspect of every operation to private actors. Several laws, regulations, and executive branch policies prohibit contractor performance of "inherently governmental functions" (IGF).[114] And because it is possible to construe the later phases of a cyber operation as more "inherently governmental" than the Pre-Launch phases, some argue that IGF considerations could hinder full contractor participation in cyber operations.[115]

To start, in 2011, the Office of Federal Procurement Policy (OFPP) issued Policy Letter 11–01, which established Executive Branch policy addressing the performance of inherently governmental functions.[116] It was intended to assist agencies in ensuring that only Federal employees perform IGF.[117] The policy letter adopted the Federal Activities Inventory Reform Act (FAIR Act) definition of IGF as "a function that is so intimately related to the public interest as to require performance by Federal Government employees."[118] The letter also provided a non-exhaustive list of functions that should be considered to be IGF. Although Cyber Command's operations were not on this list, one could reasonably argue that they are implicitly covered because they are conducted by a component of the U.S. military in support of U.S. national security interests.[119]

Further, Cyber Command is a combatant command subject to the Defense Federal Acquisition Regulation Supplement (DFARS), which is the principle set of regulations governing procurements by DoD. The DFARS, at Subpart 207.5, echoes much the substance of OFPP Policy Letter 11-01, but also incorporates the requirements of Department of Defense Instruction (DoDI) 1100.22.[120] DoDI 1100.22 describes the functions that DoD considers to be IGF and therefore not performable by contractors.[121] DoDI 1100.22 expressly designates participation in the cyber components of Combat Operations as inherently governmental.[122]

113. P.W. SINGER, CORPORATE WARRIORS: THE RISE OF THE PRIVATIZED MILITARY INDUSTRY 226 (2003).

114. James R. Lisher II, *Outsourcing Cyberwarfare: Drawing the Line for Inherently Governmental Functions in Cyberspace*, J. CONT. MGMT., Fall 2014, at 7.

115. *Id.*

116. Performance of Inherently Governmental and Critical Functions, 76 Fed. Reg. 56227 (proposed Sept. 12, 2011) (Office of Federal Procurement Policy, Policy Letter 11-01).

117. *Id.* at 56227.

118. *Id.*

119. *Id.* at 56234.

120. 48 CFR § 207.5 (2005).

121. U.S. DEP'T. OF DEF., INSTRUCTION NO. 1100.22 POLICY AND PROCEDURES FOR DETERMINING WORKFORCE MIX 19 (2010), https://perma.cc/9A4G-UBV3.

122. *Id.* at 19 (The instruction defines a combat operation as "deliberate destructive and/or disruptive action against the armed forces or other military objectives of another sovereign government or against other armed actors on behalf of the United States.").

However, it provides no explicit guidance on which activities in support of below-the-threshold cyber operations DoD considers inherently governmental.

In summary, neither OFPP Policy Letter 11–01 nor DoDI 1100.22 expressly proscribe full contractor participation in gray-zone cyber operations. To be sure, the general doctrine of IGF raises weighty prudential questions about how much destructive cyber power and operational authority should be delegated to contractors.[123] But it is much less clear that moving contractors into the launch and post-launch phases of a cyber operation will actually violate any IFG policy or regulations. DoD could clarify the matter by reissuing DoDI 1100.22 to more expressly state which activities might constitute IGF in a given cyber operation.

3. The Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) of 1986 criminalizes seven activities related to gaining unauthorized access to computer systems.[124] The CFAA, codified as 18 U.S.C. § 1030, is the domestic law most cited for the proposition that Cyber Command cannot legally expand the role of private parties in cyber operations. Those who believe that the CFAA might bar contractor participation in the post-launch stages of Cyber Command's cyber operations argue that tasking contractors with these activities would require a private actor to access, alter, or execute code on a computer network without authorization and thus violate the CFAA. This contention is likely incorrect as applied to Cyber Command-contracted cyber operations. As explained below, the CFAA does not apply to Cyber Command's out-of-network activities. Perhaps more importantly, private contractors performing on behalf of Cyber Command could be "deputized" and obtain proxy authorization to participate in cyber operations under Section 1030(f) of the CFAA. This would likely make those contractors immune to prosecution under the CFAA.

To start, the CFAA does not apply to Cyber Command's cyber operations. Under 18 U.S.C. § 1030(f), the CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."[125] As former Department of Defense General Counsel, Paul Ney, Jr. stated in 2020, "[c]ommon sense and long-accepted canons of statutory interpretation suggest . . . that the CFAA will not constrain appropriately authorized DoD cyber operations."[126] And as discussed above, Section 1642 of the 2019 NDAA leaves little remaining doubt that Cyber Command cyber operations are "lawfully authorized" activities and therefore not subject to CFAA restrictions.[127]

123. Lisher, *supra* note 114, at 18-19 (noting concerns that private actors, only accountable to the U.S. government and citizenry by commercial contract, could undertake actions in cyberspace that impact U.S. policy and public interest).

124. Computer Fraud And Abuse Act (CFAA), 18 U.S.C. § 1030.

125. *Id*.

126. Ney, *supra* note 104.

127. *See* Chesney, *supra* note 10.

It is likely that contractors are similarly shielded from liability under the statute. One interpretation of the immunity to CFAA liability granted to Cyber Command under 1030(f) is that Cyber Command may effectively "deputize" its contractors and grant them similar immunity.[128] Such relationships are far from unprecedented. The government often tasks private parties with activities that might be legally perilous if performed absent a grant of government authority. For example, a a private party that builds or acquires surface-to-air missiles might be held criminally liable under 18 U.S.C. § 2332g, which makes it unlawful to "produce, construct, or possess" incendiary rockets. But no one would argue that Raytheon should be subject to prosecution under Section 2332g for producing Javelin and Stinger missiles under contract with the Department of Defense. To be sure, the statute includes exemption for government contractors at Section 2332g(3).[129] But as the statutory exception expressly states, the key point here is that Raytheon is acting "under the authority of the United States" or "pursuant to the terms of a contract with the United States."[130] That is the true shield from liability.

Here, there is no express carve-out in the CFAA for cyber operations conducted by private parties under contract. But as stated, Section 1030(f) exempts Cyber Command from the CFAA.[131] Common sense and analogous practice suggest that private contractors are similarly immune from CFAA liability so long as they "act under the authority of the United States" and "pursuant to the terms of a contract." Certainly, it might be prudent for private contractors to obtain an explicit grant of authority from Cyber Command—either within individual contracts or by separate charter—before participating in cyber activities that might otherwise violate the CFAA. Alternatively, Congress could amend the CFAA to expressly authorize contracted cyber operations under Section 1030(f). But as some scholars and practitioners have already asserted, the statutory exemption under Section 1030(f) is very likely delegable to private actors as is.[132]

4. Legal Obstacles Presented by Other Public-Private Collaboration Models

Layered, whole-of-nation cybersecurity will necessarily require any number of public-private collaborations that fall outside the scope of this paper.[133] Contractor participation in gray-zone cyber operations must be integrated into a larger strategy for public-private collaboration that includes initiatives like hardening critical infrastructure, increased investment in private-sector cyber education, modernizing the U.S. electric grid. And indeed, moving contractors down the kill chain is not even the only policy proposal with the potential to further

128. Anthony Glosson, *Active Defense: An Overview of the Debate and a Way Forward*, MERCATUS CENTER 11-12 (2018), https://perma.cc/4PZE-3JWZ.

129. 18 U.S.C. § 2332(g).

130. 18 U.S.C. § 2332g(a)(3).

131. Computer Fraud And Abuse Act (CFAA), 18 U.S.C. § 1030(f).

132. Glosson, *supra* note 128, at 11-12.

133. *Id.*

leverage private sector capabilities in U.S. cyber operations. For example, "hack-back" proponents argue that hacking victims should be permitted to conduct their own independent, out-of-network operations to deter, disrupt, and attribute cyber intrusions.[134] Taken a step further, one lesser-known proposal makes analogy to the days of fighting sail to argue that Congress should revive the nascent prize system to certify "Cyber Privateers."[135] This is perhaps a more extreme version of hackback because cyber privateers would not act in response to intrusions into their networks. They would act as a mercenary force and launch proactive cyber operations against a government-supplied list of adversaries.[136] But these proposals share two major drawbacks relative to simply expanding the current scope of outsourcing in cyber operations.

First, because every conceivable version of hacking back or privateering would require private actors to engage adversaries outside their own networks, their activities would invite criminal (and possibly civil liability) under the CFAA.[137] Under these models, the relationship between the government and the private party conducting the operation is likely far too attenuated to be covered under Section 1030(f). Thus in practical terms, enacting either regime would require Congress to amend or repeal the CFAA.[138] As discussed above, no such legislative action is necessary to allow contractor personnel to actively participate in post-launch phases of Cyber Command's operations. This fact would make moving private contractors down the kill chain much less burdensome than these alternative proposals.

Second, the proposal advanced by this paper has the advantage of simplicity in at least one other way. Hacking back and privateering are both on the riskier end of Maurer's cyber-proxy spectrum, raising the possibility of unwanted escalation with international rivals and the risk that private actors would act contrary to U.S. interests.[139] Thus for either regime, the U.S. would need to develop and enact new frameworks to select, certify, and manage the private actors authorized to conduct cyber operations.

However, no new regulatory infrastructure would be needed to expand the scope of contractor support on Cyber Command's operations. Observers often cite challenges that the DoD faced overseeing contractors during the early years of the Iraq and Afghanistan conflicts as evidence that DoD cannot successfully administer contracts for cyber operations.[140] But the Department invested billions

134. Robert Chesney, *Hackback Is Back: Assessing the Active Cyber Defense Certainty Act*, LAWFARE BLOG (June 14, 2019, 5:31 PM), https://perma.cc/SRR5-D2GQ; *see also* James Rundle, *Cyber Private Eyes Go After Hackers, Without Counterattacking; see also* James Rundle, *Cyber Private Eyes Go After Hackers, Without Counterattacking*, WALL ST. J. (Oct. 18, 2021, 5:30 AM), https://perma.cc/K7VD-DSE6.

135. Forrest B. Hare, *Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy?*, 15 ASIAN SEC. 93, 93-102 (2019); Florian Egloff, *Cyber Privateering: A Risky Policy Choice for the United States*, LAWFARE BLOG (Nov. 17, 2016, 9:30 PM), https://perma.cc/98X3-HCUH; Nathaniel Garrett, *Taming the Wild Wild Web: Twenty-First Century Prize Law and Privateers as a Solution to Combating Cyber-Attacks*, 81 U. CIN. L. REV. 683 (2012).

136. Hare, *supra* note 135.

137. *See* Chesney, *supra* note 134.

138. *Id.*

139. MAURER, *supra* note 83, at 30-36, 144

140. Lisher, *supra* note 114, at 10-13.

in remaking its acquisition workforce, policies, and processes in just the last two decades.[141] Though still imperfect, the existing DoD procurement system evolved over the course of decades and will likely manage command and control risk better than any new system erected to administer hackback or privateering.[142]

B. Cyber Command Can Fully Leverage the U.S. Technology Sector

Reinforcing the CMF through outsourced cyber operations would allow Cyber Command to fully leverage the United States' world-leading Information and Communications Technology (ICT) capabilities.[143] The U.S. already exploits global consumer dependence on U.S. ICT products like Oracle databases and iPhones for a competitive advantage in cyber.[144] As New York Times reporter Nicole Perlroth asserted, the NSA spent the early 2000s implanting backdoors and malware "into every major make and model of internet router, switch, firewall, encryption device, and computer on the market."[145] Those successes[146] were possible because the NSA recognized its proximity and access to U.S. ICT capabilities as an opportunity.[147]

However, Cyber Command could more fully leverage its unrivaled access to U.S. ICT capabilities—and reinforce its CMF with experienced cybersecurity professionals—by more aggressively outsourcing aspects of its cyber operations to private actors. In other contexts, the DoD regularly relies on staff augmentation contracts to supplement its uniformed and civilian workforce. Cyber Command itself awarded its $460 million omnibus contract in 2015 to pull outside expertise, tools, and administrative services from the private sector.[148] Indeed that contract explicitly solicited contractor support for activities in the ISR and weaponization stages of the cyber operation kill chain.[149] The next step would be to acknowledge

---

141. *See* MOSHE SCHWARTZ, KATHRYN A. FRANCIS & CHARLES V. O'CONNOR, CONG. RSCH. SERV., R44578, THE DEPARTMENT OF DEFENSE ACQUISITION WORKFORCE: BACKGROUND, ANALYSIS, AND QUESTIONS FOR CONGRESS (July 29, 2016); *see also* 2008 National Defense Authorization Act, Pub. L. No. 110-181, 122 Stat. 3 (2008).

142. It bears repeating that Cyber Command is already utilizing contractor support on its cyber operations. MAURER, *supra* note 83, at 77.

143. INT'L INST. FOR STRATEGIC STUD., *supra* note 5, at 18. ("The [United States] remains the most powerful country in terms of ICT capability, whether gauged by the size of its digital economy, its leading role in global innovation or the unrivalled partnership between industry, government and academia.").

144. *See generally* PERLROTH, *supra* note 27, at 58-63 (detailing some of the National Security Agency's early efforts to purchase bugs and exploits in common commercial tech products).

145. *Id.* at 112.

146. These were, at minimum, technological successes. Though one can easily question the long-term wisdom of compromising so much U.S. technology. *See* Krebs, *WikiLeaks*, *supra* note 21; Krebs, *Petya Ransomware Outbreak Goes Global*, *supra* note 22.

147. *See* INT'L INST. FOR STRATEGIC STUD., *supra* note 5, at 18 (detailing the unrivaled levels of ICT collaboration between U.S. private industry, government, and academia); *but cf.* PERLROTH, *supra* note 27, at 102-116 (To be sure, the sheer scale of the NSA's digital exploitation does suggest that much of the "collaboration" was one-way or nonconsensual.).

148. MAURER, *supra* note 83, at 77.

149. Aliya Sternstein, *$460M CYBERCOM Contract Will Create Digital Munitions*, DEFENSE ONE (Oct. 10, 2015), https://perma.cc/GAR5-Q5WT.

that the private sector possesses adequate expertise to support every other phase of the kill chain too.

According to public reporting, at least some private entities already conduct illicit, out-of-network operations that are similar in scope to the gray-zone cyber operations conducted by Cyber Command. Few companies admit to conducting offensive cyber operations because, as discussed previously, the Computer Fraud and Abuse Act (CFAA) essentially bars private actors from conducting unauthorized out-of-network actions.[150] But notwithstanding the provisions of the CFAA, these operations do occur.[151] Further, because they are likely unlawful, every phase and function of these hacks—from reconnaissance to actions on objectives—is necessarily conducted by private actors without government assistance. This suggests that there is ample expertise in the private sector capable of supporting all phases of a CMF operation. Indeed, because cyber operators regularly migrate back and forth between government and private industry jobs, the private sector may contain as much modern technical cyber capability as all but the most elite groups within the U.S. government.[152]

There is some evidence that the U.S. is beginning to better recognize the value of U.S. private-sector cyber talent. In 2016, Congress created the Cyber Excepted Service (CES) to help streamline Cyber Command's process for hiring its civilian workforce.[153] And section 1643(a)(4) of the 2017 National Defense Authorization Act granted the Defense Department authority to set advanced in-hire rates, without justification, when hiring for cyber workforce positions.[154] These hiring reforms coincide with parallel investments in various cybersecurity academic programs, scholarships, and hack-a-thons focused on attracting more junior talent in the private sector.[155] The problem with hiring reforms and new educational initiatives, at least with respect to reinforcing the CMF, is that they are investments in the *future* federal cybersecurity workforce and thus cannot meet the immediate need for talent.

C. Contracting Minimizes Command and Control Risk

Tim Maurer describes a framework in *Cyber Mercenaries* under which private contractors engaged by Cyber Command to conduct cyber operations would

150. Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, NEW YORKER (May 7, 2018), https://perma.cc/6UX3-98S5.

151. *Id.*

152. PERLROTH, *supra* note 27, at 139 (noting the number of former NSA SIGINT officers working for private firms around the beltway in network exploitation positions); Joseph Menn, *Hacked Companies Fight Back with Controversial Steps*, REUTERS (Jun. 17, 2012, 10:41 PM), https://perma.cc/N5WN-2F45 (documenting that private sector firms have been engaging in cyber "self-help" for a decade or more. Some have engaged in actions that almost certainly violate U.S. or foreign domestic law in retaliation for hacks).

153. Press Release, U.S. Cyber Command, Cyber Command Steps Up Recruiting Efforts With Special Hiring Authority (Jun. 7, 2018), https://perma.cc/LKD3-LLPH.

154. National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. .114–328, 13- Stat. 2000 (2016).

155. *Id.*; GRANOVSKIY, supra note 12.

constitute *cyber proxies*.[156] The term refers to "an intermediary that conducts or directly contributes to an offensive cyber operation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect."[157] Maurer argues these proxy relationships generally fall into one of three categories: sanctioning, orchestration, and delegation. These categories exist on a spectrum, distinguished from one another by the level of control the beneficiaries exercise over the proxy's activities.[158] Contracting is a form of delegation and thus, relative to the other three categories of cyber proxy relationships, gives rise to less risk of unwanted behavior by the proxy.

A state sanctions or passively supports its proxy when it "knowingly chooses to tolerate the actor's activities despite having the capacity to do otherwise."[159] At this end of the spectrum, the sanctionor (or beneficiary) exercises the least amount of control over their proxy's actions. Cyber proxies that fall into this category include most patriotic hacking groups that launch independent cyber operations to support nationalist agendas.[160] The thousands of ordinary Russian citizens who launched denial of service attacks against the Estonian government and banking systems are a good example.[161] There could be many potential reasons—i.e. short-term political expediency, or public resource constraints—that create cyber sanctioning relationships.[162] But sanctioners always run the risk that their proxies will engage in cyber conduct that runs contrary to long-term state interests.[163]

Orchestration relationships represent the middle ground in Maurer's proxy continuum. Orchestrators recruit "intermediary actors on a voluntary basis, by providing them ideational and material support, and using them to address target actors in pursuit of political goals."[164] Though the orchestrator may provide armament, intelligence, or logistical support to its proxy, it is shared goals that bind the parties together, not the orchestrator's ability to exercise effective control over the proxy's actions.[165] The 2011-2013 cyber attacks against the U.S.

156. MAURER, *supra* note 83, at 71-80.

157. *Id*. at 17.

158. *Id*. at 42.

159. *Id*. at 46-47.

160. Adam Segal, *The Danger of Patriotic Geeks*, DIPLOMAT (Feb. 29, 2012), https://perma.cc/HZ3E-APQE.

161. Hare, *supra* note 135.

162. MAURER, *supra* note 83, at 47-48.

163. *Id*. at 48. Maurer references a non-cyber example of this risk as described by Tal Becker, former principal deputy legal advisor to the Israeli Ministry of Foreign Affairs, in his 2007 book TERRORISM AND THE STATE. As Becker points out, after the terrorist attacks of September 11, 2001, the U.S. held Afghanistan's Taliban government responsible for the actions of Al-Qaeda because the Taliban allowed Al-Queda "to operate in its territory." TAL BECKER, JOHN CAIRNS JR. & OLIVIA ROBINSON, TERRORISM AND THE STATE: RETHINKING THE RULES OF STATE RESPONSIBILITY 349 (2006).

164. MAURER, *supra* note 83, at 45; *see also* Kenneth W. Abbott, Philipp Genschel, Duncan Snidal & Bernhard Zangl, *Orchestration*, *in* INTERNATIONAL ORGANIZATIONS AS ORCHESTRATORS 3–36 (Kenneth W. Abbott, Philipp Genschel, Duncan Snidal & Bernhard Zangl eds., 2015), https://perma.cc/HX4S-LRSU.

165. MAURER, *supra* note 83, at 45.

financial sector by IRGC-backed computer companies exemplify the orchestration relationship in the cyber context.[166] Importantly, orchestration relationships carry many of the same risks as sanctioning relationships because the principal does not exert specific control over the proxy's cyber operations.

Cyber Command maintains a delegation relationship with its contracted workforce. Delegation relationships allow the principal the tightest control over the actions of its proxy. This is a classic principle-agent paradigm where Cyber Command "delegates authority to [its agents] to act on its behalf."[167] When the relationship operates as intended, Cyber Command maintains effective control of the delegated tasks (and contractor) by: delegating only those tasks that align with its interests; selecting a contractor that will perform the tasks as contracted; and managing contract performance.[168] The risk that Cyber Command's proxies will engage in conduct that runs contrary to long-term U.S. interests is thereby minimized relative to the other forms of proxy relationship.

To be sure, even though government contracts are delegation relationships, the government cannot exercise perfect control over contractor activities.[169] Further, with respect to outsourced gray-zone cyber operations and contracts implicating national security, the negative consequences of contract failure could be severe. For example, Edward Snowden was working on a Booz Allen Hamilton contract with the NSA when he obtained and disclosed a trove of highly classified details about U.S. surveillance activities.[170] Reportedly, Snowden sought the position on Booz Allen's contract specifically because it gave him access to the information that he later transmitted to *The Guardian*.[171] There, the consequences of contract failure did not lead directly to loss of life, but did include massive domestic fallout[172] and increased tension with the United States' international partners.[173]

However, despite the Snowden incident (and others), any concern over increased risks associated with greater contractor participation in U.S. cyber operations may be overblown. Private contractors already participate in the

166. *Id.* at 84-88.

167. *Id.* at 43.

168. *See id.*

169. *See, e.g.*, Matt Apuzzo, *Ex-Blackwater Guards Given Long Terms for Killing Iraqis*, N.Y TIMES (Apr. 13, 2015), https://perma.cc/S999-6CE3 (describing the tragic killing of 14 unarmed Iraqis in 2007 by members of the private security contractor Blackwater).

170. *See* Bryan Burrough, Sarah Ellison & Suzanna Andrews, *The Snowden Saga: A Shadowland of Secrets and Light*, VANITY FAIR (May 2014), https://perma.cc/654C-GKNC.

171. *See* Nate Olivarez-Giles, *Edward Snowden Says He took Booz Allen Job to Collect, Leak NSA Info*, THE VERGE (Jun. 24, 2013), https://perma.cc/97EJ-VAP7. In fact, Snowden claimed to have "take [n] pay cuts in the course of pursuing specific work" and that he had been paid less at Booz Allen Hamilton (the firm that served as his conduit to the information he would later leak) than he had been paid in other positions. *See* Guardian Staff, *Edward Snowden: NSA whistleblower answers reader questions*, THE GUARDIAN (Jun. 17, 2013, 3:31 PM), https://perma.cc/E7WS-8ATA.

172. Heather Kelly, *Protests Against the NSA Spring Up Across U.S.*, CNN (Jul. 5, 2013, 7:24 AM), https://perma.cc/HAK6-KTRH.

173. *Germany Ends Spy Pact with US and UK after Snowden*, BBC (Aug. 2, 2013), https://perma.cc/6WMA-74W5.

pre-launch phase of Cyber Command's operations[174] and therefore possess more than enough critically sensitive information to do great harm to U.S. interests through public disclosures or unsanctioned conduct. For example, any contractor's supporting the 2019 operation against Iran's missile controls[175] with targeting, or weaponization services would likely already possess most of the sensitive operational details. Thus, moving that contractor down the kill-chain—having them launch or support the launch of a cyberweapon into Iranian missile control systems—would not necessary expose any additional sensitive information to the risk of unwanted disclosure.

IV. OTHER RISK CONSIDERATIONS

A. Normalizing the Use of Cyber Proxies

As discussed in this paper, the relationship between Cyber Command and its contractor is that of principal and agent. Of the relationships along the cyber-proxy continuum, this one is the most defensible to rivals and allies whose networks may be penetrated while defending forward. Cyber Command has no true deniability concerning its contractors' actions and expects to assert considerable control over contractor conduct. But this is still a proxy relationship that involves delegating national security and foreign relations tasks to private actors. To be sure, U.S. firms like Booz Allen Hamilton and SAIC do not bear much resemblance to the loose collection of students, freelancers, and hacktivists who conduct operations to benefit Chinese and Russian interests.[176] But the fact remains that outsourced cyber operations are not conducted by uniformed or civil servant personnel. At a time when the U.S. seeks to encourage international consensus towards strong, centralized state control of cyber operations (and against abusive use of proxied cyber assets),[177] contracted cyber operations will force U.S. officials to draw fine distinctions between its own use of proxy forces and those it wishes to proscribe. That might be political capital better spent on pushing international norms in other areas of international disagreement on cyber.[178]

B. Expanding the Market for Highly Sophisticated Cyber Operators

Despite the advantages enumerated in this paper, more aggressively outsourced cyber operations could have the unintended effect of proliferating cyber capability in the U.S. private sector at the expense of the DoD and other civilian

174. *See* MAURER, *supra* note 83, at 77 (discussing Cybercommand's omnibus contract).

175. *US 'Launched Cyberattacks on Iran Weapons Systems'*, AL JAZEERA (Jun. 23, 2019), https://perma.cc/A4FY-KJNV.

176. Segal, *supra* note 160.

177. *See* INT'L INST. FOR STRATEGIC STUD., *supra* note 5, at 16 (emphasizing that in the United States, cyber policy and authority is under unified command and control under the National Security Council and President).

178. *See, e.g.*, Peter Margulies, Ira Rubinstein, *EU Privacy Law and U.S. Surveillance: Solving the Problem of Transatlantic Data Transfers*, LAWFARE BLOG (Mar. 10, 2021), https://perma.cc/7HXA-44V2 (describing the conflict between the E.U. and U.S. concerning privacy and transatlantic data transfers).

agencies. Government-trained cyber operators gain sought-after knowledge and skills directly applicable to their post-military careers, and there is already a "revolving door in and out of cyber-related jobs in government."[179] Private sector cybersecurity salaries are always rising[180] and the federal government is already struggling to compete for talent.[181] Outsourced cyber operations may exacerbate this problem by opening up a new market for cybersecurity professionals with direct experience conducting sophisticated operations in support of Cyber Command.

In *Cyber Mercenaries*, Tim Maurer gives the example of Brendan Conlon, who spent a decade participating in NSA cyber operations before founding the computer security company Vahna.[182] Nicole Perlroth gives the example of the "Maryland Five," a gaggle of the NSA's most elite cyber operators who all left the agency on the same day to found Vulnerability Research Labs.[183] In both examples, and there are countless others, these former civil servants left the government and took their skills with them. Cyber Command may need to develop new tools (e.g. a cooling-off period or similar) to restrict contractor personnel from accepting certain positions directly after participating in cyber operations in support of Cyber Command.

CONCLUSION

After 9/11, the IC identified a particularly urgent need for experienced personnel with high-level language, computer science, and engineering skills.[184] The IC turned to contractors because the demand for these workers was so urgent that the government could not fully meet it through the slower process for hiring civil servants.[185] The skills needed by the Cyber Mission Force are similarly scarce.

The SolarWinds, Microsoft, and Colonial Pipeline penetrations suggest that deeper public-private partnerships may be needed to compete in cyberspace. Indeed, these attacks support the wisdom of a more assertive Cyber Command, one that conducts more frequent out-of-network operations to deter bad behavior. But for defend forward to operate at scale, Cyber Command will need a stable supply of highly-skilled personnel capable of conducting its cyber operations. In a perfect world, that workforce might consist entirely of uniformed cyber operators or experienced civil servants. But in *our* world, at least for now, the necessary skills are too scarce to be sourced solely from public talent pools.

Cyber Command should open up some of its gray-zone operations to full contractor support and orchestration at every phase of the kill chain. This will free up

179. MAURER, *supra* note 83, at 80.
180. ISC2 CYBERSECURITY WORKFORCE STUDY 2021, *supra* note 12.
181. GRANOVSKIY, supra note 12.
182. MAURER, *supra* note 83, at 80.
183. PERLROTH, *supra* note 27, at 139.
184. MAURER, *supra* note 83, at 72-73.
185. Lachow & Grossman, *supra* note 73, at 387.

scarce uniformed cyber operators for the more combat-oriented cyber operations. To be sure, this is not a perfect solution. As Peter Singer said nearly two decades ago, "War is far too important to be left to private industry."[186] Contracted cyber operations raise complicated legal questions that implicate domestic and international law. And indeed, like all privately contracted security services, outsourced cyber operations will always carry some risk of abuse or unwanted conduct. For those reasons and others, this expansion of contractor involvement in U.S. cyber operations should be curtailed as soon as the conventional CMF achieves an adequate force size and capability mix to confront the current threat.

186. SINGER, *supra* note 112, at 242.

***