Seventh Service: Proposal for the United States Cyber Force

Lieutenant Commander Michael G. McLaughlin

ABSTRACT

To fight and win in cyberspace, the United States needs a Cyber Force. During World War II, air power tipped the scale of victory in favor of the allies, as aviation proved to be an indispensable warfighting capability. The creation of the Air Force was predicated on the notion that the effective employment air power is not a matter of choice, but the very condition on which national survival rested. Today, cyber superiority has wider implications for US national security than air superiority had at the close of World War II; however, the federal government is not structured to effectively defend the US national interests. The current division of cyber authorities precludes comprehensive mitigation of cyber-enabled malicious activities. To effectively combat nation-state and non-state actors targeting US and allied interests in cyberspace, the US should establish a Cyber Force modeled on the U.S. Coast Guard with a reserve component modeled on the National Guard. Combining these models would allow for a single force capable of executing military operations, law enforcement activities, and intelligence collection at the direction of the Departments of Defense and Homeland Security, complemented by an expansive reserve component available to both state governors and the federal government.

INTRODUCTION

During World War II, air power tipped the scale of victory in favor of the allies, as aviation proved to be an indispensable warfighting capability.[1] From air-to-air engagements and tactical bombing campaigns to aircraft carrier-centered naval combat and the delivery of nuclear munitions—for the first time in history,

Michael McLaughlin is a cybersecurity attorney in Washington D.C. and research affiliate for the University of Maryland Applied Research Laboratory for Intelligence and Security. He previously served as the Senior Counterintelligence Advisor for United States Cyber Command and Chief of Counterintelligence and Human Intelligence for the Cyber National Mission Force. He holds a Bachelor of Science degree from the US Naval Academy and a Juris Doctorate from the University of Maryland School of Law. Lt. Cmdr. McLaughlin resides in Annapolis, Maryland, with his wife and their two sons.

the air became a significant warfighting domain.[2] Throughout the war, aviation components of the Army and Navy proved the value of complementing land and sea power with air power in every theater of combat.[3] After the war, America's military and political leaders recognized the inefficacy of having all the nation's air power subordinated as components of the Army and Navy.[4] Nearly two years after the end of hostilities, the National Security Act of 1947 officially established the United States Air Force as its own military service within the Department of Defense (DoD).[5]

The creation of the U.S. Air Force was predicated on the notion that a "realistic understanding of the new weapon, of its implications in terms of national security, of its challenge to America, is not a matter of choice," but one of the conditions on which national survival rested.[6] Today, cyber superiority has wider implications for US national security than air superiority had at the close of World War II, as every facet of life in America has become reliant on cyberspace.[7] However, unlike how DoD evolved its structure to meet the new challenges and opportunities of air warfare, no such significant structural change has materialized in the way in which the military resources, trains, and controls its forces for combating threats in the cyber domain. Despite DoD's recognition of cyberspace as a critical warfighting domain, there exists no standalone Cyber Force.[8] This shortcoming places the US at a disadvantage as digital warfare and threats continue to evolve. The US needs a Cyber Force with military, intelligence, and law enforcement authorities sufficient to effectively combat the malicious use of cyberspace.

There exist legal, organizational, and practical impediments to establishing an element with such broad powers. To prevent abuse of government power, the US has developed a system specifically designed to prevent the consolidation of domestic law enforcement, intelligence, and military capabilities.

This is an important division; however, it can also lead to dysfunction. Threats in cyberspace are inherently different from traditional national security threats. Malicious cyber actors recognize neither physical borders nor the distinction between military and non-military targets.[9] Nation-states frequently blend criminal activities, espionage, and military operations to conduct malicious activities and impose costs upon businesses, governments, and individuals.[10] The US considers these types of operations to be traditional military activities, yet the national framework for cyber incident coordination does not include the DoD.[11] To address the novel legal and operational challenges of cyber warfare and cyber-enabled malicious activities, the US needs to move beyond current monolithic military, intelligence, and law enforcement constructs to imagine a new Cyber Force.

Within the United States Code, there are several unique titles that, if combined, would imbue a Cyber Force with authorities commensurate with the evolving threats in cyberspace.[12] While different organizations within the federal government are authorized to conduct various activities under multiple titles, no single organization can leverage all requisite authorities for effectively combating malicious cyber actors and activities.

Within the DoD alone, different organizations and agencies operate in cyberspace under disparate legal frameworks. For example, while Military Department Counterintelligence Organizations (MDCOs)—such as the Naval Criminal Investigative Service (NCIS)—conduct counterintelligence and law enforcement activities, MDCOs are not authorized to conduct military operations.[13] The authority to conduct military operations is derived from orders issued to combatant commanders by the Secretary of Defense through the Chairman of the Joint Chiefs of Staff.[14] Conversely, while the Secretary of Defense (SECDEF) has ordered U.S. Cyber Command (USCYBERCOM) to execute military cyber operations to deter, disrupt, and defeat malicious cyber actors targeting DoD information networks and US critical infrastructure, USCYBERCOM has no authority to conduct counterintelligence or law enforcement activities.[15] However, there are organizations within the federal government whose roles, responsibilities, and authorities enable exceptions under the right circumstances to the separation of military, intelligence, and law enforcement powers—namely, the U.S. Coast Guard and National Guard. The exceptions under which these organizations can operate, and the circumstances under which they are allowable, offer a viable model and framework for designing roles, responsibilities, and authorities for a Cyber Force and corresponding National Guard component.

This article presents shortcomings inherent in both the current construct of DoD's cyber operations forces and the federal government's cyber incident coordination. It contends that the federal government's division of authorities precludes comprehensive mitigation of and response to cyber-enabled malicious activities targeting domestic cyberspace. To combat nation-state and non-state actors targeting US interests in cyberspace effectively, the federal government should establish a Cyber Force modeled on the U.S. Coast Guard with a reserve component modeled on the dual state/federal forces of the National Guard.

Though blending legal authorities in the digital age is a relatively new concept, the Coast Guard serves as a useful model because it has effectively integrated military capabilities and operations with law enforcement and homeland defense authorities for decades, for example in the War on Drugs and the Global War on Terror. Moreover, the National Guard has been extensively leveraged over the past 20 years to respond to natural disasters under state authority and deploy to Iraq and Afghanistan under federal authority. Combining these models would establish a single service capable of executing military operations, law enforcement activities, and intelligence collection at the direction of both DoD and Department of Homeland Security (DHS), complemented by a reserve component available to individual states and to the federal government.

PART I. CURRENT STRUCTURE

Department of Defense Cyber Operations Forces

Within DoD, USCYBERCOM is the unified combatant command whose area of responsibility is the global cyber domain.[16] The Commander of USCYBERCOM is principally charged with defending the DoD Information Network, and, on order, to "defend or secure . . . cyberspace related to critical infrastructure and key resources (CI/KR) of the US."[17] USCYBERCOM comprises 133 teams and over 6,200 cyber operations personnel assigned throughout the headquarters; service cyberspace component commands from the Army, Navy, Air Force, and Marine Corps; Joint Force Headquarters DoD Information Network (JFHQ-DODIN); and the Cyber National Mission Force (CNMF).[18] Each service component of USCYBERCOM executes defensive and offensive cyberspace operations to defend its respective service networks and to engage targets in and through cyberspace.[19] JFHQ-DODIN is the joint component charged with securing, operating, and defending the DoD information technology infrastructure.[20] Furthermore, consisting of over 2,000 personnel from each military service, the CNMF is the joint component responsible for executing the full spectrum of cyberspace operations to deter, disrupt, and defeat malicious cyber actors to defend the United States.[21]

As the DoD's joint force component for national cyber defense, the CNMF conducts cyberspace operations to defeat cyberspace threats to both the DoD Information Network and non-DoD cyberspace.[22] To this end, the CNMF conducts myriad offensive and defensive cyberspace operations external to DoD networks.[23] Since the activation of the CNMF in 2014, the Secretary of Defense has ordered USCYBERCOM to execute numerous cyberspace operations against malicious cyber actors. Frequently, these actors are affiliated with foreign intelligence services or are conducting espionage activities at their behest.[24]

Because the DoD requires the CNMF to execute what would traditionally constitute covert action or counterintelligence activities, Congress authorized the DoD to recharacterize these actors so as permit the CNMF to conduct operations against them.[25] In the 2020 National Defense Authorization Act, Congress reaffirmed that USCYBERCOM may conduct operations in

cyberspace against malicious cyber actors as "traditional military activities."[26] CNMF operations defending against and targeting malicious cyber actors, therefore, do not constitute counterintelligence activities.[27] Despite this limited legal nuance, USCYBERCOM cannot conduct the full range of counterintelligence or law enforcement activities and relies on other government organizations with those authorities to engage with domestic companies and organizations to defend the homeland.[28]

Within DoD, those authorities rest with the cyber elements of the military counterintelligence and law enforcement organizations, which comprise Cyber Crime Investigators from NCIS, the U.S. Army's Counterintelligence Command and Criminal Investigative Division (CID), and the U.S. Air Force Office of Special Investigations (OSI).[29] These organizations are responsible for the collection, production, and dissemination of military-related counterintelligence, as well as conducting military law enforcement and counterintelligence activities both outside of the US and domestically.[30] Because malicious cyber actors target domestic companies and organizations for intellectual property theft, misappropriation of trade secrets, and other acts of espionage affecting DoD information, military counterintelligence and law enforcement organizations have broad authority to conduct activities on the networks of consenting organizations inside the US in coordination with the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ).[31] However, these organizations are not authorized to execute military cyber operations against malicious cyber actors; that authority resides solely with USCYBERCOM.[32]

DEPARTMENT OF HOMELAND SECURITY

DHS is responsible for the security of non-DoD federal information networks[33] and the protection of critical infrastructure,[34] as defined by Presidential Policy Directive (PPD) 21.[35] Within DHS, various agencies have sector-specific cyber responsibilities, such as the Coast Guard—responsible for cybersecurity in the maritime sector;[36] the U.S. Secret Service—responsible for investigating fraud and finance-related crimes;[37] the Transportation Security Administration (TSA)—responsible for the security of all modes of transportation, including, inter alia, aviation, shipping, and pipelines;[38] and the Federal Emergency Management Agency (FEMA)—responsible for the activation and support of emergency support functions under the National Response Framework and the National Cyber Incident Response Plan.[39] For the cyber efforts of the various sector-specific agencies within DHS, the dedicated lead is the Cybersecurity and Infrastructure Security Agency (CISA).[40] For significant cyber incidents, CISA also serves as the lead for asset response activities and coordinating field-level activities among DHS's sector-specific agencies.[41]

FEDERAL GOVERNMENT CYBER INCIDENT RESPONSE

Though DHS serves as the lead agency for protecting and mitigating threats to federal networks and CI/KR, the federal government organizes its response to significant cyber events

affecting the homeland through the coordination of field-level activities, national policy, and national operations across multiple agencies.[42] Field-level activities are those conducted at the affected entity, whether a critical infrastructure element, a federal government agency, or another affected entity.[43] National policy coordination consists of support to the National Security Council in the development and implementation of policy and strategy to address "significant cyber incidents affecting the US or its interests abroad."[44] National operational coordination consists of the establishment of a Cyber Unified Coordination Group (UCG) to coordinate responses to significant cyber incidents among federal government agencies.[45]

Within the UCG, there are designated lead agencies to ensure "maximum effectiveness" across three primary lines of effort: threat response, asset response, and intelligence support.[46] For threat response activities, the DOJ, acting through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), serves as the lead federal agency.[47] Threat response activities include the attribution, pursuit, and disruption of malicious cyber actors and activities.[48] This is done through criminal investigations, federal indictments, and economic sanctions aimed at countering the malicious cyber activity."[49] Asset response, led by the DHS, consists of activities aimed at mitigating network vulnerabilities and protecting assets against malicious cyber actors.[50] DHS does this by providing technical assistance, conducting threat hunting on affected networks, and facilitating information sharing across multiple industries.[51] Intelligence support is led by the Office of the Director of National Intelligence (ODNI), which directs the activities of the US Intelligence Community (IC).[52] Intelligence support activities are intended to identify and build awareness of cyber threats and facilitate information sharing.[53]

While this delineation of roles is intended to "achieve maximum effectiveness in coordinating responses to significant cyber incidents," the DoD and the significant resources and capabilities of the cyber operations forces are notably absent.[54] To compound this ambiguity in the role of the DoD in responding to national cyber incidents, the integration of DoD resources into the federal government's response to cyber events faces other barriers. For example, in 2015, Congress passed the Cybersecurity Information Sharing Act to encourage and facilitate the sharing of threat indicators, defensive measures, and best practices between public and private sector entities.[55] However, in November 2018, the DoD Inspector General (IG) found that the DoD had taken only limited actions to implement the Act's requirements.[56] Federal guidelines direct government agencies to make unclassified cyber threat indicators broadly available to other agencies as well as to non-federal entities as quickly as operationally practicable.[57] The DoD IG found that the DoD did not have the internal controls necessary to meet the Act's requirements for sharing cyber threat indicators and defensive measures.[58]

In addition to the limitations noted above, information silos exist which prevent the integration of different types of intelligence and operational activities that would enable the DoD to assist the federal government in a significant cyber incident and mitigate the risk of compromise by wide-scale cyber aggression. For example, because USCYBERCOM is not a member of

the IC, it primarily relies upon tailored signals intelligence (SIGINT) or law enforcement-derived information to execute its missions.[59] As such, it is dependent on Intelligence Community and law enforcement partners that prize and seek to protect this information for their missions.[60] Where competition for resources exists, these information silos and restrictive information-sharing practices can limit or preclude integration and effective whole-of-government response to cyber events.

The exclusion of DoD from the framework for federal responses to cyber incidents is likely due in part to limitations in the manner in which the armed forces are permitted to operate domestically. For instance, using elements of DoD by civilian law enforcement in such a manner as to subject US citizens to a "regulatory, proscriptive, or compulsory" exercise of military power would violate the Posse Comitatus Act.[61] Intelligence elements of DoD are subject to intelligence oversight provisions of Executive Order 12333, prohibiting the intentional collection of information about US persons.[62] Moreover, non-intelligence elements of DoD are beholden to other legal provisions such as the Wiretap Act, which requires consent for government actors to access private networks.[63]

PART I. SUMMARY

Existing legal frameworks and restrictive departmental constructs like those discussed above keep the federal government from effectively integrating the totality of its capabilities and resources. Instead, it is waging an inefficient campaign, fraught with intra-departmental and interagency redundancies, information silos, and inefficient public-private partnerships.[64] "If the United States is to defeat these cyber threats, traditional notions regarding the division between criminal and national security matters must be reevaluated."[65] While the vast majority of cyber events affecting US cyberspace can be managed by individual network defenders and the current federal response construct, increasingly sophisticated nation-state attacks against the private sector "require a unique approach to response efforts."[66]

PART II. MORE EFFECTIVE MODELS

U.S. Coast Guard

The Coast Guard operates at the intersection of homeland defense, law enforcement, intelligence activities, and military operations.[67] It is the only element within the federal government where individual personnel can conduct activities simultaneously under authorities traditionally reserved for individual governmental agencies. The Coast Guard's unique composition offers a particularly good model for addressing the challenges inherent in the dynamic nature of cyberspace, where lines between domestic security, law enforcement, and warfare are often blurred.

Following 9/11, the Homeland Security Act of 2002 transferred the Coast Guard to the Department of Homeland Security.[68] When operating as a part of DHS, the Coast Guard has five

homeland security missions: (1) Ports, waterways, and coastal security; (2) drug interdiction; (3) migrant interdiction; (4) defense readiness; and (5) other law enforcement activities.[69] As the agency responsible for the maritime sector within DHS, the Coast Guard maintains broad authority over the navigable waters of the US. These authorities include the ability to prescribe how private and commercial vessels operate,[70] control over the anchorage and movement of vessels to ensure the safety and security of US naval vessels,[71] and the ability to prescribe regulations for the inspection and certification of vessels.[72] Additionally, the Coast Guard may use its personnel, equipment, and facilities to assist federal, state, local, tribal, and territorial agencies when its assets are particularly qualified to perform a specific activity.[73]

To fulfill its role in the maritime domain effectively, the Coast Guard is authorized to operate as a law enforcement organization.[74] Coast Guard personnel have federal law enforcement authorities to board any vessel subject to the jurisdiction of the US, whether on the high seas or on waters over which the US has jurisdiction, to "make inquiries, examinations, inspections, searches, seizures, and arrests for the prevention, detection, and suppression of violations of US laws."[75] Additionally, when the President determines that US national security is endangered, the Coast Guard may enforce regulations within US territorial waters, including vessel seizure and forfeiture, and may fine and imprison the master and crew for noncompliance.[76]

In addition to its role as a sector-specific agency within DHS, the Coast Guard is also "a military service and a branch of the armed forces of the United States at all times."[77] As such, the President may direct elements of the Coast Guard be transferred to the Department of the Navy to execute operations consistent with the authorities of the armed forces.[78] For example, in April 2021, two Coast Guard cutters deployed to the Middle East to operate under the U.S. Navy's Fifth Fleet in Bahrain.[79] The Coast Guard has continuously conducted such military deployments to the US Central Command area of responsibility since 2002.[80]

Among its myriad functions, the Coast Guard also operates as a member of the IC.[81] In this role, the Coast Guard has the authority to "collect, analyze, produce, and disseminate foreign intelligence and counterintelligence" and to "conduct counterintelligence activities" at the direction of the Commandant.[82] Because Coast Guard Intelligence does not operate exclusively as an element of DoD, it is not beholden to many of the restrictions imposed upon the Defense Intelligence Enterprise.[83]

A key area where all the Coast Guard's roles and authorities intersect is in cyberspace. Complementing its traditional maritime role, the Coast Guard also operates Coast Guard Cyber Command both as the maritime sector lead for DHS and as a service cyber component of USCYBERCOM.[84] In its DHS role, Coast Guard Cyber Command serves to facilitate the cybersecurity of maritime ports and shipping and to respond to cyber events affecting the maritime sector.[85] For example, in August 2021, the Coast Guard assisted the Port of Houston in defending its network from a cyberattack by a nation-state actor using a zero-day vulnerability.[86] In its DoD role, Coast Guard Cyber Command is responsible for defending and operating the Coast Guard's

portion of the DoD Information Network.[87] Though its current DoD mission is entirely defensive, the Coast Guard's first Combat Mission Team was established in the summer of 2021 to begin growing the service's offensive cyber capabilities.[88] While the Coast Guard's offensive cyber mission remains undefined, it could conceivably execute offensive operations as either a military operation under DoD or as a counterintelligence activity under DHS.

National Guard

Within DoD, there are seven reserve components. Each of the uniformed services, including the Coast Guard, has a reserve.[89] The Army and Air Force also have a National Guard component.[90] While the reserve components of the uniformed services operate exclusively under DoD, elements of the National Guard operate either under the operational control of the governors of individual states and territories or as elements of DoD in federal service when activated by the President.[91] Comprising over half of the total force strength of the reserve elements of the armed forces, the National Guard is a crucial component of both national defense and disaster response and recovery.[92]

There are three ways the National Guard may be activated: state active duty, federal activation, and Title 32 status. State active duty is governed by individual state and territorial laws by which governors can activate members of the National Guard at the governor's discretion.[93] Federal activation occurs in the form of either mobilization[94] or federalization of the National Guard as an organized militia.[95] Title 32 activation is directed by the federal government—and paid for by the federal government—but the command and control of National Guard personnel on Title 32 orders remain with the respective state governors.[96]

During emergencies, a state may use its own National Guard and may leverage the National Guard of other states through the Emergency Management Assistance Compact (EMAC).[97] Depending on the type of emergency, states can also leverage National Guard Civil Support to assist law enforcement.[98] However, the type of activation dictates the types of activities the National Guard can perform. For instance, when National Guard personnel are operating under state active duty or Title 32—either within their home state or in another state under EMAC—they are generally not governed by the Posse Comitatus Act and may perform law enforcement functions.[99] However, when National Guard personnel are activated under Title 10 and perform duties under the control of the President, though they can provide military support to civil authority, they are subject to the Posse Comitatus Act and may not perform law enforcement functions except in specific circumstances enumerated by statute.[100]

Despite the size and broad authorities of the National Guard operating under state authority, it has only been leveraged in limited scope to "prepare for, respond to, and recover from cybersecurity incidents that overwhelm state and local assets."[101] Congress has recognized a lack of standardization and efficient employment of the National Guard for responding to cyber events.[102] In the 2021 National Defense Authorization Act, Congress directed the Secretary of

Defense to evaluate the "statutes, rules, regulations and standards that pertain to the use of the National Guard for the response to and recovery from significant cyber incidents."[103] Congress went on to direct an update to the National Cyber Incident Response Plan to reflect improved employment of the National Guard.[104]

PART II. SUMMARY

Both the Coast Guard and the National Guard have unique characteristics that set each organization apart from traditional government and military entities. The Coast Guard leverages authorities under both DoD and DHS to perform its core functions for national security and homeland defense. Similarly, the National Guard provides both state governments and the federal government with a reserve force capable of executing emergency management and response actions at the state level as well as federal tasking as part of DoD. Because threats in cyberspace span military, law enforcement, homeland defense, and intelligence functional areas, as well as pose substantial risks to CI/KR that could result in significant state-level emergencies, the nation requires a cyber force capable of operating across all of these functional areas and in support of every level of government.

PART III. UNITED STATES CYBER FORCE

The US should establish a Cyber Force with an active component modeled on the Coast Guard and a reserve component modeled on the National Guard. The active component would serve as a sector-specific agency within DHS and "a military service and a branch of the armed forces of the US at all times."[105] The reserve component would be a third National Guard force and would operate alongside each of the 54 current National Guard organizations.

Within DHS, the Cyber Force would be the element responsible for managing DHS contributions in all dimensions of our cybersecurity. This would include defense of federal networks and CI/KR and operational control over the US Computer Emergency Response Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The Cyber Force would work closely with the Cybersecurity and Infrastructure Security Agency (CISA) in supporting private sector engagement, network monitoring, and threat-hunting activities.

The Cyber Force would be imbued with federal law enforcement authorities for the "prevention, detection, and suppression of violations of laws of the United States" in cyberspace similar to those of the Coast Guard in the maritime domain.[106] To limit a broad interpretation of this authority, the Cyber Force's law enforcement functions could be limited to those unlawful activities that target or affect the federal government or CI/KR networks. Among other law enforcement functions, the Cyber Force could use these authorities and the warrant process to mitigate cyber threats proactively.[107] Law enforcement authorities would also permit the Cyber Force to apply for and serve warrants and subpoenas to domestic entities wittingly or unwittingly used by malicious cyber actors to execute operations against the US. Finally,

these authorities would allow the Cyber Force to integrate with and support other federal law enforcement agencies as well as state, local, tribal, and territorial law enforcement elements without violating the Posse Comitatus Act.

Like the Coast Guard, the Cyber Force would also be an individual member of the Intelligence Community. This would enable the training and development of cyber-specific intelligence and counterintelligence collectors, analysts, and operational personnel. The Cyber Force would have the authority to conduct counterintelligence activities, operations, and investigations in direct support of national cyber missions and requirements. As a member of the IC, the Cyber Force would also be able to conduct foreign intelligence liaison relationships and exchange programs with partners to improve the collective cyber defense posture of the US and its allies.

When operating as part of the DoD, the Cyber Force would serve as the force provider for the CNMF. In this role, the Cyber Force would man, train, and equip personnel to conduct full-spectrum cyberspace operations against malicious cyber actors. Under the operational control of USCYBERCOM, Cyber Force personnel would be able to execute offensive and defensive cyber operations targeting malicious cyber actors outside of the US. Rotational assignments would ensure that personnel supporting USCYBERCOM can benefit from the operational experience of performing sector-specific functions for DHS and vice versa. Additionally, mobilization of the Cyber National Guard to support USCYBERCOM and the CNMF would ensure operational experiences are continually shared between state defenders and the active component of DoD. Importantly, the establishment of a Cyber Force would not supplant the cyber components of the other military services. USCYBERCOM's service component commands would maintain their respective offensive and defensive missions in the same way as US Space Command's service component commands carry out appropriate missions despite the existence of the US Space Force.

As the reserve component of the Cyber Force, the Cyber National Guard would serve primarily as a digital militia for individual states and territories, while providing a ready pool of cyber professionals in the event of a national emergency. The establishment of a Cyber National Guard would standardize the training and equipping of a state-level cybersecurity response force. This stand-alone force could be leveraged by governors to respond, using state police powers, to significant cyber incidents affecting state and local governments, CI/KR, and private entities. A Cyber National Guard would also enable the individual states and the federal Cyber Force to tap into the significant talent pool across the private sector by allowing for part-time state and federal service without requiring those individuals to enlist or commission in the regular military.

CONCLUSION

In March 2021, the Government Accountability Office (GAO) found that the federal government "needs to urgently pursue critical actions to address major cybersecurity challenges."[108]

The GAO recommended the federal government establish a comprehensive cybersecurity strategy and perform effective oversight.[109] The segmentation of authorities and capabilities across the federal government makes this difficult if not infeasible. Overcoming this challenge requires establishing a Cyber Force and Cyber National Guard able to leverage the requisite authorities of both the individual states and the federal government and provide a comprehensive array of capabilities to support achievement of the nation's cybersecurity objectives.

DISCLAIMER

The views and opinions expressed in this article are those of the author alone and do not reflect the official policy or position of the Department of Defense (DoD), U.S. Cyber Command, or any agency of the U.S. Government. Any appearance of DoD visual information or reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission, or broadcast.

NOTES

1. Arthur W. Tedder, *Air Power in War,* The University of Alabama Press (2010), 87-124.
2. Ibid., 29.
3. Ibid.
4. Alexander P. de Seversky, *Victory Through Air Power,* Simon & Schuster, Inc. (1942), 254.
5. Pub.L. 80-253, 61 Stat. 495, enacted July 26, 1947.
6. de Seversky, *Victory Through Air Power,* 254.
7. The White House, *National Cyber Strategy of the United States of America* (2018) ("America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace."), 1.
8. Department of Defense Memorandum, "Directing USSTRATCOM's Establishment of a Subordinate Unified Command for Cyber Operations," June 23, 2009, https://nsarchive.gwu.edu/news/cyber-vault/2020-05-11/uscybercom-documents-timeline (accessed October 6, 2021) (Though "the military departments have identified the following organizations to serve as components to USCYBERCOM. . . . (1) ARFORCYBER [Army Cyber Command][,] (2) FLTCYBERCOM [Navy Fleet Cyber Command][;] (3) MARFORCYBER [Marine Forces Cyber Command]; (4) AFCYBER [Air Force Cyber Command]," each military service maintains its own cyber forces.).
9. Daniel, Michael, "Why Is Cybersecurity So Hard?" *Harvard Business Review* (May 22, 2017), https://hbr.org/2017/05/why-is-cybersecurity-so-hard (accessed Oct. 1, 2021) ("[O]ur physical-world mental models simply won't work in cyberspace. For example, in the physical world, we assign the federal government the task of border security. But given the physics of cyberspace, everyone's network is at the border. If everyone lives and works right on the border, how can we assign border security solely to the federal government?").
10. See *United States v. Yuriy Sergeyevich Andrienko, et al.*, No. 20-316 (WDPA) (On October 15, 2020, a grand jury in the Western District of Pennsylvania returned an indictment against six Russian intelligence officers. These officers, members of GRU Military Unit 74455 – more commonly referred to as "Sandworm," were charged with executing a pervasive and continuous destructive malware campaign against nations worldwide since at least 2015.)
11. The White House, "Presidential Policy Directive 41," (July 7, 2016) [hereafter "PPD-41"] (Federal lead agencies for coordinating responses to significant cyber incidents include the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force for threat response activities, the Department of Homeland Security for asset response activities, and the Office of the Director of National Intelligence for intelligence support.).
12. U.S.C. Title 6. DOMESTIC SECURITY governs the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency; U.S.C. Title 10. ARMED FORCES governs the military; U.S.C. Title 14. COAST GUARD governs the activities of the U.S. Coast Guard; U.S.C. Title 18. CRIMES AND CRIMINAL PROCEDURE governs law enforcement; U.S.C. Title 32. NATIONAL GUARD governs the functions of the National Guard Bureau; U.S.C. Title 50 WAR AND NATIONAL DEFENSE governs the activities of the U.S. Intelligence Community.
13. See 10 U.S.C. §§ 5013 (authorizes the Secretary of the Navy to control and supervise intelligence activities of the Department of the Navy); see 10 U.S.C. § 7480 (authorizes the Secretary of the Navy to permit NCIS special agents to execute federal arrest warrants); see also 50 U.S.C. §3038 (authorizes the Department of the Navy to collect and produce intelligence).
14. See 10 U.S.C. § 164(c); see also 10 U.S.C. § 167(b)(d).
15. Pub.L. 116-92—December 20, 2019. § 1631 (c); see 10 U.S.C. § 394 (c); see also 50 U.S.C. 3093 (e)(2).
16. U.S. Cyber Command, "Our History," https://www.cybercom.mil/About/History/ (accessed November 6, 2021).
17. See Department of Defense, Joint Publication 3-12, *Cyberspace Operations,* June 8, 2018 [hereafter JP 3-12], 1-4.
18. U.S. Cyber Command Public Affairs, "Cyber Mission Force achieves Full Operational Capability" (May 17, 2018), https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/ (accessed November 6, 2021).
19. U.S. Army Cyber Command, "About Us" (June 2020), https://www.arcyber.army.mil/Organization/About-Army-Cyber (accessed October 7, 2021).
20. COL Craft, Paul, "JFHQ-DODIN: Fight the DODIN" (May 2019), https://disa.mil/-/media/Files/DISA/News/Events/Symposium-2019/1---COL-Craft_Fight-the-DODIN_approved-Final.ashx (accessed October 7, 2021).
21. Joint Staff Approval of U.S. Cyber Command Concept for Organization (2012).
22. JP 3-12, I-9.

NOTES

23. See JP 3-12, ll-8 to ll-9.
24. See The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," Statements and Releases (July 19, 2021) ("As detailed in public charging documents unsealed in October 2018 and July and September 2020, hackers with a history of working for the [People's Republic of China] Ministry of State Security (MSS) have engaged in ransomware attacks, cyber enabled extortion, crypto-jacking, and rank theft from victims around the world, all for financial gain.").
25. See Executive Order 12333, *United States Intelligence Activities* (as amended by Executive Orders 13284 (2003), 13355 (2004), and 13470 (2008)) § 3.5(a), *Federal Register,* Vol. 40, No. 235 (December 8, 1981), [hereafter EO 12333] ("Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities."
26. Pub. L. 116-92—December 20, 2019. § 1631 (c); see 10 U.S.C. § 394 (c); see also 50 U.S.C. 3093 (e)(2).
27. Sen. Rpt. 102-85, at 46 (1991) ("'[T]raditional military activities' include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding hostilities which are anticipated (meaning approval has been given by the National Command Authorities for the activities and for operational planning for hostilities) involving U.S. military forces, or where such hostilities are ongoing, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.").
28. See DoD Instruction S-5240.17, "(U) Counterintelligence Collection Activities (CCA)," March 14, 2014 (MDCOs conduct consent-based monitoring of select domestic private sector networks under Military Department counterintelligence authorities. Because Commander, U.S. Cyber Command, has not been delegated full-spectrum counterintelligence authorities by the Secretary of Defense, counterintelligence agents assigned to the Cyber Mission Force are not authorized to conduct similar network monitoring.).
29. See Cyber Crime Investigator, *Defense Cyber Workforce Framework*, https://public.cyber.mil/dcwf-work-role/cyber-crime-investigator/ (accessed November 27, 2020); see also EO 12333.
30. EO 12333 § 1.12.
31. See, generally, United States v. Li Xiaoyu (a/k/a "Oro0lxy") and Dong Jiaxhi, No. 4:20-CR-6019-SMJ (E.D. Wash. July 7, 2020); see DoDD 5240.02 (DoD policy outlining the conduct of CI); see 18 U.S.C. § 2511(2)(c) (Exception to the Wiretap Act: "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception. . . ."); see also DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities,* at para. 3.2 Procedure 2: Collection of USPI, August 8, 2016 (DoD policy governing exceptions to the collection of United States Person information, including with valid consent and for the purposes of counterintelligence); see also EO 12333 § 1.11(d) ("CI activities outside the U.S. are conducted in coordination with the Central Intelligence Agency (CIA)[, and] MDCO CI activities inside the U.S. are conducted in coordination with the Federal Bureau of Investigation (FBI).").
32. See 10 U.S.C. §167b; see also 10 U.S.C. §395.
33. Pub. L. 113-283 (Federal Information Security Modernization Act of 2014).
34. Pub. L. 107-296 (Homeland Security Act of 2002); Pub. L. 113-282 (National Cybersecurity Protection Act of 2014); Pub. L. 114-113 (Cybersecurity Act of 2015); Pub. L. 115-278 (Cybersecurity and Infrastructure Security Agency Act of 2018).
35. The White House, Presidential Policy Directive 21 (February 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/ (accessed November 7, 2021) [hereafter "PPD-21"], ("The Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." Critical infrastructure sectors include: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.).
36. 46 U.S.C. §70116.

NOTES

37. 18 U.S.C. §3056.
38. 49 U.S.C. §114; see Transportation Security Administration, "DHS announces new cybersecurity requirements for critical pipeline owners and operators" (July 20, 2021), https://www.tsa.gov/news/press/releases/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline (accessed November 7, 2021).
39. Department of Homeland Security, "National Response Framework" (4th Ed., October 28, 2019).
40. Pub. L. 115-278.
41. PPD-41, supra note 11.
42. Ibid.
43. Ibid.
44. Ibid.
45. Ibid
46. Ibid.
47. Ibid.
48. Department of Homeland Security, "Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government," https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf (accessed November 9, 2021).
49. PPD-41, supra note 11 ("Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response."
50. See PPD-41, supra note 11; see also Department of Homeland Security, "Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government," https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf (accessed November 9, 2021).
51. PPD-41, supra note 11 ("Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.").
52. Ibid.
53. Ibid., "Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.".
54. Ibid.
55. Pub.L. 114-113, "Division N—Cybersecurity Act of 2015, Title I—Cybersecurity Information Sharing," December 18, 2015; 6 U.S.C. § 1502.
56. DODIG-2019-016.
57. Ibid., 11, citing "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015," February 16, 2016.
58. DODIG-2019-016 at 5.
59. Office of the Director of National Intelligence, *Members of the IC* (https://www.dni.gov/index.php/what-we-do/members-of-the-ic) (accessed October 25, 2021).
60. Rpt. to Accompany S. Rpt. 116-4049 (2020), Sec. 1639 at 463, https://www.armed-services.senate.gov/imo/media/doc/FY%202021%20NDAA%20-%20Report.pdf.
61. *United States v. McArthur,* 419 F. Supp. 186 (D.N.D. 1976); see 18 U.S.C. 1385.
62. EO 12333.
63. 18 U.S.C. § 2511(2)(c).

NOTES

64. See U.S. Government Accountability Office, *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-598 (August 18, 2020); see also United States National Security Strategy, 23 (2017); see also The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 18 (2009) (which, in 2009, noted: "government and private-sector personnel, time, and resources are spread across a host of bodies engaged in sometimes duplicative or inconsistent efforts. Partnerships must evolve to clearly define the nature of the relationship [and] the roles and responsibilities of various groups and their participants").
65. LtCol Kurt Sanger and CDR Peter Pascucci, "Revisiting a Framework on Military Takedowns Against Cybercriminals," Lawfare (July 2, 2021) (https://www.lawfareblog.com/revisiting-framework-military-takedowns-against-cybercriminals).
66. PPD-41, supra note 11; see The White House, "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," (April 15, 2021) (The United States has formally named the Russian Foreign Intelligence Service (SVR) "as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures. . . . The scope of this compromise is a national security and public safety concern.").
67. 14 U.S.C. §101.
68. Pub. L. 107-296.
69. 6 U.S.C. §468(a)(1).
70. 33 U.S.C. §1223.
71. 14 U.S.C. §91.
72. 46 U.S.C. §3306.
73. 14 U.S.C. §141.
74. 14 U.S.C. §89.
75. Ibid.
76. 50 U.S.C. §191.
77. 14 U.S.C. §101.
78. 14 U.S.C. §103.
79. United States Coast Guard New Release, "U.S. Coast Guard ships depart Puerto Rico on mission to strengthen Trans-Atlantic ties" (April 2, 2021), https://content.govdelivery.com/accounts/USDHSCG/bulletins/2cb0645 (accessed October 20, 2021).
80. Ibid.
81. Pub.L. 80-253 (amended December 28, 2001).
82. EO 12333.
83. See, for example, Department of Defense Instruction 5240.04, *Counterintelligence Investigations* (Feb. 2, 2009 (*Incorporating Change 1, Effective October 15, 2013*) (Within the Department of Defense, only Military Department Counterintelligence Organizations (Army Military Intelligence, Naval Criminal Investigative Service, and Department of the Air Force Office of Special Investigations) are authorized to conduct counterintelligence investigations. No other DoD counterintelligence elements, including the Defense Intelligence Agency, the Combatant Commands, or other military organizations have this authority. However, because the Coast Guard derives its counterintelligence authorities directly from the President in EO 12333, the Commandant may define the personnel, methods, and means by which it conducts counterintelligence investigations when not operating under the Department of Defense.).
84. U.S. Guard Cyber Command, "Commander's Strategic Direction 2021," (August 2021), https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf (accessed September 21, 2021).
85. 46 U.S.C. §70116.
86. Sean Lyngaas, "Hackers breached computer network at key US port but did not disrupt operations," CNN.com (September 23, 2021), https://www.cnn.com/2021/09/23/politics/suspected-foreign-hack-houston/index.html (accessed October 1, 2021).
87. U.S. Guard Cyber Command, "Commander's Strategic Direction 2021," August 2021, https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf (accessed September 21, 2021), 7.

NOTES

88. Kimberly Underwood, "Coast Guard Embarks on Cyber Offense," *SIGNAL* (October 1, 2021), https://www.afcea.org/content/coast-guard-embarks-cyber-offense (accessed October 5, 2021).
89. 10 U.S.C. §1003.
90. Ibid.
91. 32 U.S.C. §104.
92. Defense Manpower and Data Center, "Selected Reserve Personnel by Reserve Component and Rank/Grade (Updated Monthly): September 2021," DoD Personnel, Workforce Reports & Publications, https://dwp.dmdc.osd.mil/dwp/app/dod-data-reports/workforce-reports (accessed November 5, 2021) (as of September 2021, the combined strength of the Army National Guard and Air National Guard was 446,008 personnel.).
93. See, for example, Md. Public Safety Code Ann. §13 (2020).
94. See 10 U.S.C. §12301(a) (Full mobilization); 10 U.S.C. §12302(a) (Partial mobilization); see also 10 U.S.C. §12304 (Active Duty other than War or National Emergency).
95. See 10 U.S.C. §12406 (Federal activation to repel an invasion, suppress a rebellion, or execute laws of the United States); (10 U.S.C. §251 (Federal activation of the militia of one state to quell insurrection in another); see also 10 U.S.C. §252 (Federal activation to enforce federal law in the event of an insurrection).
96. 32 U.S.C. §502(f).
97. Pub. L. 104-321.
98. Chief National Guard Bureau Instruction 3000.04, *National Guard Bureau Domestic Operations*, January 24, 2018 ("National Guard Civil Support -- Support provided by the National Guard while in a State Active Duty status or Title 32 status to civil authorities for domestic emergencies, designated law enforcement, and other activities.").
99. See, e.g., Md. Public Safety Code Ann. §13-402 (2020).
100. See 18 U.S.C. 1385; but see 10 U.S.C. §12406.
101. Cyberspace Solarium Commission ("Examples of states relying on National Guard units to deal with cybersecurity incidents include Colorado, Louisiana, and Texas, where the governors declared state of emergencies to activate their National Guard."), 65.
102. Pub. L. 116-283 § 1729.
103. Ibid.
104. Ibid.
105. 14 U.S.C. §101.
106. See 14 U.S.C. §89.
107. Fed. Rules of Crim. Pro. 41(6)(b)(6); see April Falcon Doss, "We're From the Government, We're Here to Help: The FBI and the Microsoft Exchange Hack," JustSecurity.org (April 16, 2021), https://www.justsecurity.org/75782/were-from-the-government-were-here-to-help-the-fbi-and-the-microsoft-exchange-hack/ (accessed April 16, 2021). (The FBI used this authority to remove malware from networks affected by the Microsoft Exchange Server vulnerability exploited by the Hafnium – malicious cyber actors associated with the Chinese government.).
108. U.S. Gov't Accountability Off., GAO-21-288, *HIGH-RISK SERIES: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (March 2021), https://www.gao.gov/assets/gao-21-288.pdf ("To address this challenge, federal agencies need to take the following four actions: (1) develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace, (2) mitigate global supply chain risks, (3) address cybersecurity workforce management challenges, and (4) ensure the security of emerging technologies.").
109. Ibid.