Atlantic Council

Operationalizing a Cybersecurity Strategy for the United States

Part I—Operations

Franklin D. Kramer, Robert J. Butler, and Melanie J. Teplinsky

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

January 2026

Contents

I. Introduction and summary

A fundamental approach of the Trump administration is ensuring and enhancing the defense of the United States homeland. Border security has accordingly been prioritized, and a "Golden Dome" missile defense has been proposed. But equivalent to the challenges of the border and of missile defense is the defense of the information and operational technology systems upon which the national security, economy, and public safety of the United States depend. This report focuses on operations and its companion report focuses on technology and architectures; together they identify the challenges facing the United States and describe a proposed national cybersecurity strategy that encompasses key roles for government and for the private sector.

The proposed two-pronged strategy establishes an operational road map for defensive and offensive campaigning with appropriate roles for government and the private sector (as described in this report); and scales resilience by accelerating the development and adoption of safe coding and zero trust architectures for key critical infrastructure systems and enterprises (as described in the companion report, Part II: Safe Coding and Trusted Architectures). By accomplishing these two sets of activities, the United States will establish a homeland defense cyber posture that provides the president and the national leadership with the necessary capabilities to deter and counter nation-state and criminal adversaries in cyberspace.

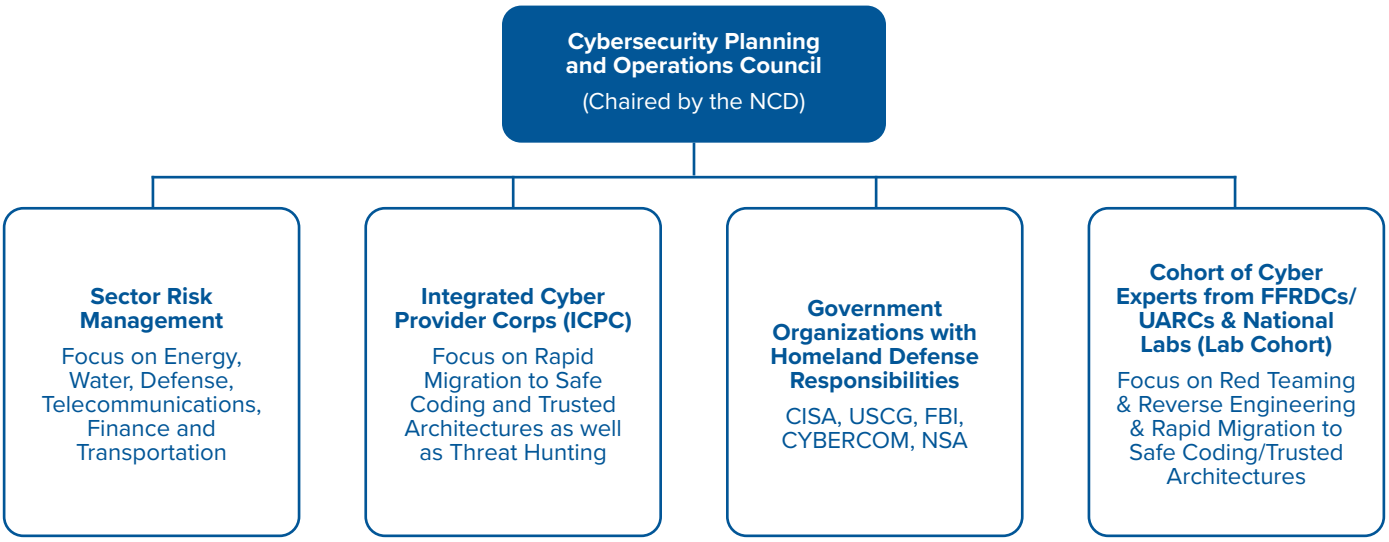
Specifically, as described in this report, an operational road map for defensive and offensive campaigning requires:

- **CPOC.** Establish a Cybersecurity Planning and Operations Council, a high-level group headed by the national cyber director to coordinate both governmental and public-private campaigning activities.
- **ICPC.** Create an Integrated Cybersecurity Providers Corps of high-end, private-sector cybersecurity providers and secure cloud service providers to undertake continuous defensive campaign development and execution assistance, particularly focused on "Section 9" critical infrastructure companies.[1]
- **National cyber lab cohort.** Create a consortium of experts from federally funded research and development centers, university affiliated research centers, and the National Laboratories to provide technical direction and support to the national cyber director and other government leaders in cyber defense and offensive planning to counter and deter nation-state adversaries. As discussed in more detail in Part II, the unique expertise of the national cyber lab cohort would complement the ICPC's high-end, private-sector expertise and would be leveraged to support various activities designed to bolster critical infrastructure resilience (e.g., expertise in formal methods application could be leveraged to accelerate Section 9 entities' migration to safe coding technologies).
- **National reserve force.** Scale this force—by expanding the National Guard's cyber mission and civilian cyber reserve forces—to bolster support for defensive and offensive cyber missions.
- **Regional resilience districts.** Organize regional resilience districts for key geographic areas to develop resilience among interlocking capabilities to limit cascading effects and establish reconstitution mechanisms that would be required after a cyberattack. As initial efforts, establish pilot programs for selected port cities (ideally with important military facilities such as Charleston) focused on key critical infrastructures including local governance and establishing mechanisms for prompt recovery from cyberattacks.
- **Wartime threat hunting on key operational technology (OT) networks.** Establish a wartime active defense threat-hunting capability for key critical infrastructures by expanding Cyber Command's mission to include wartime threat hunting strictly limited to key critical infrastructures' operational technology/industrial control system (OT/ICS) networks (starting with National Guard units with OT hunting experience) and coordinating those activities with ongoing Cybersecurity and Infrastructure Security Agency (CISA) and Coast Guard domestic threat-hunting activities.
- **Cyber-enabled offensive action.** Develop cyber-enabled offensive actions and campaigns by the US government to state-supported intrusions into US critical infrastructures.
- **Private-sector disruption.** Foster private-sector action to disrupt criminal activities including dark web sites through coordination with the government and to support the government including serving as a cyber reserve in wartime.

The requirements for scaling resilience through safe coding and zero trust architectures (ZTAs) are described in Part II of the report, but a summary is included in the Part I Appendix.

To effectuate the proposed national strategy, this report argues for a new national cyber governance construct that brings together the most capable cybersecurity actors from both the public and private sectors. This governance construct, described in figure 1, would be led by the national cyber director as chairman of a National Cyber Planning and Operations Council. As noted in figure 2, different private-sector entities would function in different capability areas to accomplish the thrusts of a new, fortified cybersecurity strategy. Figure 2 delineates the roles of each of these private-sector entities.

Figure 1. National Cybersecurity Governance for Homeland Defense



Thrusts

- Strenghtening most critical enterprise resilience through rapid migration to safe coding and trusted architectures
- Establishment and enabling of regional resilience districts for critically important economic and defense geographies
- Continuous threat hunting around most critical enterprises and regional resilience districts
- Offensive planning support and red teaming of plans against nation-state adversaries
- Offensive planning support and red teaming against large scale criminal cartels and groups

Figure 2. Private Sector Support to National Cybersecurity Governance for Homeland Defense

Roles Private Sector Entities	National Campaign Planning Support	"Threat Hunting" in the Homeland	Augmented and Certified Defensive Operations	Safe Coding Support to Section 9 Companies	Trusted Architecture Support to Section 9 Companies
Cybersecurity Companies (ICPC)	Yes	Yes	Yes	No	Yes
Cloud Providers (ICPC)	Yes	Yes	Yes	Yes	Yes
Federally Funded R&D Centers (Lab Cohort)	Yes	No	Yes*	Yes	Yes
University Affiliated Research Centers (Lab Cohort)	Yes	No	Yes*	Yes	Yes
National Labs (Lab Cohort)	Yes	No	Yes*	Yes	Yes

Note: *Red Teaming and Reverse Engineering Support Only

II. The cybersecurity challenge: Adversaries

A fundamental cybersecurity challenge facing the United States is that US information and operational technology systems are at high risk from state-sponsored attacks by the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea (i.e., North Korea) and from financial and other attacks by criminal organizations.

China

Perhaps most significantly, China has penetrated critical operational infrastructures throughout the country, as noted by Jen Easterly, then-director of CISA, in describing efforts to evict Chinese cyber actors, and as described by then-Rep. Mark E. Green (R-Tenn.), who stated:

> Volt Typhoon, a malicious state-sponsored cyber actor connected to the People's Republic of China (PRC), repeatedly targeted critical U.S. infrastructure. By prepositioning cyber threats within critical infrastructure networks, Volt Typhoon was poised to launch destructive cyberattacks of immense proportions against the U.S. . . . the malign group compromised critical infrastructure organizations in communications, energy, transportation systems, and water and wastewater systems.[2]

Likewise of high concern, Salt Typhoon, a PRC state-sponsored cyber threat actor that reportedly targeted networks in more than eighty countries,[3] "breached at least nine U.S.-based telecommunications companies with the intent to target high profile government and political figures."[4]

More recently, China state-aligned hacking groups—including Linen Typhoon and Violet Typhoon[5]—have exploited vulnerabilities in Microsoft's SharePoint Server software to engage in a major cyber-espionage campaign affecting hundreds of agencies, businesses, and organizations. While the full extent of the SharePoint breach is not yet known (as of this writing, the investigation has only just begun), victims reportedly include the National Reconnaissance Office's Acquisition Research Center website,[6] the Department of Energy's National Nuclear Security Agency,[7] the Department of Homeland Security, and the Department of Health and Human Services including the National Institutes of Health.[8] Moreover, what started as a cyberespionage campaign now appears to have evolved, with Storm-2603—a China-based threat actor—having been observed exploiting the SharePoint vulnerabilities to deploy ransomware.[9]

Other high-profile Chinese attacks—including Operation Aurora,[10] the 2014 Office of Personnel Management hack,[11] the Equifax hack,[12] and the Microsoft Exchange/Hafnium hack[13]—have targeted valuable individual, business, and government information including industrial trade secrets.

Russia

Russia has similarly undertaken highly significant cyberattacks such as the Solar Winds supply chain attack with "nearly 18,000 . . . customers receiv[ing] compromised software,"[14] the NotPetya attack resulting in "more than $10 billion in total damages,"[15] and the Viasat attack affecting multiple commercial companies and communications throughout Europe.[16]

Iran

Iranian cyberattacks have long targeted US financial institutions and other critical infrastructure. The infamous distributed denial of service [DDoS] attacks against dozens of US financial-sector victims beginning in 2011 were perpetrated by a group of Iranian hackers working for an Iranian Revolutionary Guard Corps affiliate,[17] and one of those hackers later infiltrated the supervisory and control systems of the Bowman Dam in New York.[18] CISA cited recent Iranian attacks against OT "devices,"[19] with the Treasury Department last year citing "ransomware attacks against critical infrastructure."[20] It is notable that Iranian targeting of industrial control system devices also can enable espionage or disruptive/destructive attacks against critical infrastructures.[21]

North Korea

North Korea has a long history of engaging in cyberattacks including the well-known Sony[22] and Wanna Cry attacks.[23] Much of the North Korean cyber effort is undertaken to support its overall economic resilience, including through attacks on cryptocurrency,[24] and its nuclear program, including cyberespionage to obtain nuclear secrets and leveraging ransomware operations to finance its nuclear weapons program.[25] Notably, North Korea has attacked key critical infrastructures through, for example, ransomware campaigns targeting healthcare and public health organizations and other sectors.[26]

Criminal organizations

Multiple criminal organizations have undertaken frequent ransomware attacks[27] against vulnerable targets such as state and local governments and hospitals and other health providers.[28] Likewise, individual, business, and governmental information has regularly been stolen by criminal organizations—as exemplified by the attacks on national public data—resulting in the disclosure of millions of records containing personally identifiable information and the theft of valuable trade secrets.[29]

Threat actors exploiting advanced AI capabilities

Advanced artificial intelligence capabilities are expected to rapidly supercharge the existing spectrum of cyber threats from espionage to ransomware[30] and other cybercriminal operations. One harbinger of such change is the "AI-orchestrated cy-

ber espionage campaign,"[31] first detected in September 2025, in which alleged Chinese state-sponsored actors reportedly used agentic AI, largely without human intervention,[32] to attack thirty global targets and achieve a "handful of successful intrusions."[33] While the attack garnered significant attention as "the first documented case of a large-scale cyberattack executed without substantial human intervention," it reflects the more general trend toward greater incorporation of AI into the cyberthreat landscape with criminals increasingly using AI models to automate various stages of criminal operations (e.g., reconnaissance, credential harvesting, and network penetration)[34] in furtherance of sophisticated attacks,[35] and artificial intelligence lowering barriers to entry, allowing criminals with minimal technical skill to carry out complex cybercrime operations,[36] including against industrial control systems.[37]

The risks and losses from ongoing, and increasingly AI-enabled, cyber invasions are of enormous consequence to the United States. From a national security perspective, attacks against key infrastructures—such as the electric grid, railroads, or ports—during a conflict would significantly degrade the United States' capacity to achieve the country's war aims. As a recent report concluded, "The cybersecurity of the critical air, rail, and maritime infrastructure that underpins U.S. military mobility is insufficient."[38] There is, however, little doubt that an adversary—for example, China in the context of a Taiwan scenario or Russia in a European contingency—would undertake precisely such actions. As the March 2025 *Annual Threat Assessment of the U.S. Intelligence Community* states:

> If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.[39]

Regarding Russia, the assessment states:

> Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat. Moscow's unique strength is the practical experience it has gained integrating cyber attacks and operations with wartime military action, almost certainly amplifying its potential to focus combined impact on U.S. targets in time of conflict.[40]

The potential for significant impact on key critical infrastructures has been demonstrated in the context of the Russia-Ukraine war. According to *The Kyiv Independent*, Ukraine's military intelligence agency (known as HUR) inflicted damage in "a large-scale cyberattack against the network infrastructure of Russian energy giant Gazprom." Disruptions from the July 18 attack included:

> Hundreds of terabytes of data were downloaded by the Ukrainian hackers prior to their deletion from the Russian systems [and] . . . the attackers managed to destroy clusters of "extremely powerful" servers running 1C, a software widely used for managing documents and contracts, analytics data for pipelines, valves, pumps, and SCADA [supervisory control and data acquisition] systems—key elements in operating Gazprom's technical infrastructure. [Additionally], multiple servers reportedly had operating systems removed or disabled, and the BIOS (i.e., basic firmware) of many devices was damaged, making them inoperable without physical repairs.[41]

The harms from cyberattacks are not, however, confined to the national security sphere. Economic losses from cyberattacks are estimated to be in the hundreds of billions of dollars (some estimates are in the trillions[42]), with one estimate placing US economic losses at $320 billion for 2023.[43] A World Bank cybersecurity literature survey, while emphasizing the difficulty of determining the reliability of available data,[44] nonetheless concluded:

> Our analytical survey reveals that the economic losses of cyber incidents go beyond the immediate quantifiable costs since cyber incidents often incur indirect costs that have often remained unmeasured. For example, our survey reveals that cyber incidents can translate into systemic risk in financial markets, contagion effects to other firms in the same industry, and volatility in both domestic and global stock markets.[45]

In sum, for both national security and economic reasons, it is time—indeed, past time—for a far more effective approach to ensure the cybersecurity of the United States.

III. Cybersecurity strategic road map: Operational campaigning

A strategic road map to enhance cybersecurity in the United States should recognize, leverage, and coordinate the roles of both government and the private sector and focus on two distinct, but complementary efforts: operational campaigning and the adoption of safe coding and zero trust architectures for key critical infrastructures. The discussion below describes an operational road map based on defensive and offensive campaigning. (The Part II companion report focuses on safe coding and zero trust architectures.)

As a preliminary point, the role of the private sector cannot be overemphasized. First, the private sector, which is the backbone of the US economy, is a significant target of adversarial attacks. Key critical infrastructures—ranging from the electric grid to pipelines and transportation to finance and water (and more)—are largely private-sector entities and, as the discussion of the cyber threat above makes clear, are high value targets for adversarial states like China and Russia. Likewise, communications and information technology companies—such as telecommunications, internet service providers, and cloud companies—are privately owned and operated, and have also been subject to attack. Finally, cybersecurity capabilities are in substantial part provided by private-sector cybersecurity companies that often excel in innovation, speed, and agility. Accordingly, improving cybersecurity will require significant engagement with the private sector. To be sure, the government quite obviously will need to be substantially involved and often in the lead: in providing capabilities, establishing effective organizational structures, and furnishing resources. But a fundamental premise of the strategy described herein is the necessity of coordinated private-public efforts.[46]

A key driver of this report's recommendations for more fully engaging with the private sector is the inexorable and accelerating pace of technological change and its impact on our nation's cybersecurity posture. While the organizational constructs in Part II of this report are focused on bringing today's most effective cybersecurity approaches—namely formal methods and ZTAs—to Section 9 companies, once established, those same mechanisms may be used in the future as a pipeline for dissemination of new cybersecurity capabilities. Similarly, the framework set forth in Part I of this report, notably including creation of an ICPC and CPOC, is designed to leverage—now and over the long term—the private sector's innovative work at the forefront of cybersecurity for the benefit of US national cybersecurity through sustained campaign efforts.

*** *** ***

As part of an overall response to adversary cyber intrusions, the United States will need to undertake concerted campaign efforts including both defensive and offensive activities. The required campaigning should include actions in the US homeland prior to and during conflicts to eliminate adversary cyber intrusions; by the US government outside the homeland against adversarial nations to respond to and deter adversary intrusions into US critical infrastructures; and by the private sector to disrupt criminal activities including dark web sites working both in coordination with the US government and in support of it, including to act as a cyber reserve in wartime.

A. Actions in the United States

1. Establishing a coordinating group to integrate campaigning activities headed by the national cyber director

Effective campaigning will be a key requirement of a national cybersecurity strategy. As discussed below, there will be multiple organizations—both governmental and from the private sector—engaged in such campaigning. Policy coordination to ensure an integrated approach to campaigning will be a key element of a national cybersecurity strategy. Such coordination should be undertaken by a coordinating group headed by the national cyber director.

A properly staffed and resourced Office of the National Cyber Director (ONCD) would be well-situated to coordinate governmental cybersecurity activities, akin to the way in which the Office of the Director of National Intelligence's National Counterterrorism Center leads counterterrorism efforts and conducts strategic operational planning, "driving whole-of-government action to secure our national [counterterrorism] objectives."[47] Such coordination falls well within the NCD's formal remit:

> The National Cyber Director leads the coordination and implementation of national cyber policy and strategy, including the National Cyber Strategy—in coordination with the heads of relevant Federal departments or agencies, monitoring and assessing the effectiveness, including cost-effectiveness, of the implementation of such national cyber policy and strategy by Federal departments and agencies.[48]

However, the government cannot, by itself, undertake the entirety of cybersecurity activities required by an effective cybersecurity strategy. The private sector will have key roles, as described below. If the private sector is to work successfully, the relevant private-sector parties will need to integrate their activities with those the government is undertaking. For example, with effective coordination, private-sector activity with

disruptive effects could be strategically timed to further governmental objectives. To facilitate the necessary private-sector interactions with government, it will be important to establish an effective coordinating group.

The US government has been authorized to work with the private sector on cybersecurity matters for nearly three decades, going back to Presidential Policy Directive (PPD) 63 during the Clinton administration. In 2016, the US government codified a public-private sector approach specifically focused on national cybersecurity incident response under a new PPD-41.[49] Yet, despite such efforts, adversaries have had significant successes in intruding into key critical infrastructures as described in Section II above.

To create the nature and degree of coordination necessary to be significantly more effective, a Cybersecurity Planning and Operations Council should be established.[50] Such a council would be headed by the ONCD, which is best positioned and empowered to accomplish such whole-of-nation work. Its governmental membership would include those departments operating as sector risk management agencies with cybersecurity mandates[51] and key federal agencies with cybersecurity responsibilities including the Federal Bureau of Investigation and relevant representation from the intelligence community. Its private-sector membership would include the high-end cybersecurity and cloud providers who would be members of a proposed Integrated Cybersecurity Providers Corps (described below), along with the federally funded research and development centers (FFRDCs), university affiliated research centers (UARCs), and the National Labs that are members of a proposed lab cohort (also described below). In the discretion of the NCD, coordination on specific matters could be limited as appropriate to entities focused on specific arenas or capabilities. The CPOC would develop both defensive and offensive campaigns (as described below) including appropriate oversight of private-sector members.

The recommended actions are consistent with the thinking set forth in the Trump administration's March 19, 2025, executive order, which directed publication of a National Resilience Strategy addressing critical infrastructure protection from a "risk-informed approach," prioritizing resilience and action over routine information sharing. [52]

2. Creating an ICPC of high-end cybersecurity and cloud providers to undertake continuous defensive campaigning

Most private-sector companies do not have the capability to defend against highly capable cyber adversaries such as China or Russia. Accordingly, for Section 9 critical infrastructures essential to national defense or the economy, it would be highly valuable to have the most capable expertise defending their activities.[53] To do so, as the authors have previously recommended, the government should establish an Integrated Cybersecurity Providers Corps. ICPC members would be: "focused on providing effective cybersecurity for those critical infrastructures most relevant to military activities, continuity of government, and maintaining the performance of the economy."[54]

To qualify for ICPC membership, cybersecurity firms and major cloud providers would have a capability bar to clear:

> Broadly speaking, an integrated cybersecurity provider should be able to provide high-end cybersecurity services including authentication, authorization, segmentation, encryption, continuous monitoring, and protection against DDoS attacks. Cloud providers should have the ability to protect the cloud itself and to offer other expert security providers the opportunity to provide cybersecurity as a service on the cloud.[55]

As previously recommended, the ICPC was intended to support key critical infrastructures in wartime.[56] It is certainly true that wartime support is necessary, but given the very extensive intrusions by China (and others) into US critical infrastructures, it would be extremely important for the ICPC members to work with Section 9 key critical infrastructures on a regular basis even absent an actual kinetic conflict. Accordingly, Congress should direct Section 9 companies to establish support arrangements with ICPC members. As this would be done for national security purposes, Congress should further establish line-item budgetary support for such activities, most likely as part of the Department of Defense (DOD) budget.

To be most effective, ICPC companies should receive government intelligence support to enhance their ability to provide effective cybersecurity. Both CISA and the National Security Agency (NSA) currently have undertaken useful engagements with the private sector through the Joint Cyber Defense Collaborative and the NSA Cybersecurity Collaboration Center,[57] respectively. Similarly, the Department of Defense (through Cyber Command) has established Under Advisement, an "unclassified program that allows partners across all sectors of industry to collaborate and share technical information on foreign threats, which has been pivotal in countering foreign cyber threats to the Nation."[58]

The government should expand those existing interactions to include providing operationally useful intelligence information[59] to the ICPC companies and the key critical infrastructures. Such information, for the most part, should be provided in unclassified fashion. Historically, that has not been the case, but the reality is that adversaries know the information (obviously, since it is their malware); not only is it much easier to undertake defensive measures working with unclassified information, but there are significant long-term costs for the failure to share actionable intelligence information with those parties most capable of contributing to our collective cyber defense.[60] There are narrow circumstances in which classification will be appropriate (e.g., to protect intelligence sources and methods), but that should be the exception, not the rule.

Sharing key information should also move from the ICPC companies to the government. ICPC companies will have very

broad access to information, and such information can be used defensively but also for cyber-enabled offensive operations.[61] As further described below, ICPC companies would be key players working with the government in supporting and/or undertaking operational campaigning.

3. Establishing a national lab cohort to provide technical direction to the NCD

A consortium of FFRDC, UARCs, and national laboratory experts (the lab cohort) should be created to provide technical direction and support to the NCD and other government leaders in cyber defense and offensive planning to counter and deter nation-state adversaries. As demonstrated in the wake of World War II, FFRDCs, UARCs, and the National Laboratories are uniquely qualified to help guide the nation in developing and using new technologies and concepts for national security. The United States has a rich tapestry of government-supported and affiliated academic research and development institutions with deep knowledge and experience across the cyberspace domain, including critical infrastructures. As the NCD's technical direction agents, this cohort **would provide technical advisement, perform risk assessments, and conduct experiments to demonstrate new concepts, acting as a crucial bridge between government, industry, and the National Laboratories' deep technical capabilities.** Most, if not all, of these institutions already have cyber programs underway. Leveraging these existing structures takes advantage of this expertise by creating a path for that knowledge to inform broader cybersecurity design, planning, and implementation.

4. Scaling a national reserve force

The national reserve force should include both a federal reserve corps as well as the National Guard, which can support both federal and state needs. Congress has recognized the National Guard's contributions to cybersecurity and has directed DOD to evaluate expanding Guard cyber missions.[62] Many National Guard members bring cutting-edge industry expertise to their roles due to their work in the technology and cybersecurity sector as civilians. As citizen-soldiers, National Guard members provide critical cyber expertise and synchronization of effort at the federal, state, and regional levels.

As part of this effort and to meet needs across state lines, the NCD would work with National Guard leaders and state government leadership to develop cross-state agreements and enable greater unity of effort in cyber defense across the homeland. Generating regional capabilities that could be tapped in support of the regional resilience districts would help ensure that a critical mass of highly capable cybersecurity professionals would have had the opportunity to train and exercise together prior to a contingency in which their talents are needed.

Lessons learned from National Guard involvement in the State Partnership Program can usefully be applied to the National Guard's defensive role and shared from one unit to another.[63]

In addition to these defensive mission activities, the National Guard could play a critical role in augmenting the cadre and expertise of US military offensive cyber operators.

Another significant element to scaling an overall national reserve force and bolstering private-sector expertise for national cybersecurity campaign planning can be found in the recent US Army initiative to create an Executive Innovation Corps by bringing senior executives from firms such as Meta, Palantir, and OpenAI into the Reserves.[64] This initiative should be expanded to all services, with executives functioning as a group of senior advisers to the NCD and other national cybersecurity leaders.

Finally, the nation would benefit greatly—in both scaling capacity and capability—from the expansion of civilian cyber reserve forces. Multiple states including Michigan, California, Maryland, Ohio, and Texas have established volunteer programs (and others are reviewing the option). Meanwhile, the National Defense Authorization Act for 2024 (NDAA) set in motion a pilot program for a civilian cybersecurity reserve to bolster US Cyber Command.[65]

Such a reserve force can usefully support state and local critical infrastructures, providing needed resources to improve cybersecurity to water and wastewater utilities, for example, and to state and local governments themselves. While each state will have to determine its own structure, the national cyber director could provide organizational support, coordinate across state lines including for regional resilience districts, and establish automated intelligence-sharing pipelines to support the states including through the volunteer cyber civilian reserve organizations.[66] Cyber civilian reserves could be further expanded through volunteer commitments of cybersecurity experts from corporate America. Under this construct, companies would provide paid time off to employees who volunteered and committed time to a civilian cyber reserve force,[67] and companies with highly capable employees could be incentivized to do so.[68] Individual participation in the proposed cyber reserve force could be further incentivized through a combination of the same benefits used to attract and retain volunteer firefighters, namely, compensation (including paid time off as proposed above), tax benefits,[69] and retirement programs.[70]

5. Establishing regional resilience districts

In addition to the actions above, Congress should fund the establishment of "regional resilience districts" with a focus on mitigating regional cybersecurity risks across sectors in key areas.[71] A regional resilience pilot program could focus on how to engage different entities in a collaborative fashion within and across state boundaries.[72] Regional resilience districts could be established for key geographic areas throughout the United States to enhance cross-sectoral cybersecurity with focus on limiting cascading effects and establishing mechanisms for recovery after a cyberattack. Initial pilots might focus on the Houston ship channel,[73] and involve East and West Coast port cities with important military facilities, such as Charleston, Norfolk, and San Diego.

The activities of such a regional resilience district should be built around a regional risk registry. The risk registry would identify and prioritize cyber risks and would be developed in conjunction with private, state and local, and federal entities. Such a regional resilience district could then undertake cyber risk mitigation and responses by combining the capabilities of high-end cybersecurity providers with both the engaged critical infrastructures and with state and local governments. Such an arrangement could be particularly useful in dealing with cascading risks generated by cybersecurity attacks.

The establishment of regional resilience districts should be under the auspices of the ONCD. Regional resilience districts would develop and implement cyber risk controls consistent with ONCD guidance/direction. However, the operational leadership of different regional resilience districts should be undertaken by an organization with consequential cybersecurity capabilities. In this regard, the Coast Guard would be well-positioned to undertake a series of pilot programs: It has promulgated cybersecurity regulations governing "vessels, harbors, and waterfront facilities," and uses "captain of the port" authorities.[74]

Moreover, significant attention also needs to be paid to ensuring and enhancing the US capability to bring key critical infrastructures back online as quickly as possible after any cyberattack. These capabilities need to be in place before any conflict. This cyber resilience capability would be extremely important to US national security in the context of a conflict in which an adversary—say, China—attacked US critical infrastructures. The need extends to state and local governmental functions such as police, fire, and water.

Section 1517 of the Fiscal Year 2024 NDAA established a "pilot program for assuring critical infrastructure support for military contingencies."[75] The statute includes requirements for testing "cyber resiliency," including coordination with the private entities responsible for the critical infrastructures of power, water and telecommunications. In meeting the statutory tasking, the DOD will need to focus on techniques for accelerated recovery.

Section 1517 is written in terms of base security. While base security is of obvious importance, the resilience effort has far broader implications. Accordingly, Congress should take a second step and establish comparable programs focused on enhancing resilience and recovery for key areas that would be covered by resilience districts. For example, pilot programs for one or several port cities would be of high consequence because the stable functioning of this infrastructure is essential for both the military and the public. If successful, the program could be expanded to other areas as additional steps toward more effective national resilience.

BOX 1: Regional resilience districts: membership/precedents

A regional resilience district could include federal entities; state and local governments; and both for-profit and nonprofit entities. Precedents and authorities include multistate compacts such as the Port of New York and New Jersey, and state-authorized political subdivisions such as the Houston Ship Channel Security District. The latter, for example, includes multiple public partners including federal (Coast Guard), state (the Port of Houston Authority), city (City of Houston), and private entities (ranging from chemical manufacturers to shipyards).

Sources: Steve P. Mulligan, "Interstate Compacts: An Overview," Congressional Research Service, June 15, 2023, https://www.congress.gov/crs-product/LSB10807; "Houston Ship Channel Security District: The Basics," FAQ, Houston Ship Channel Security District, updated October 6, 2015, https://hscsd.org/about-the-district/faq/; and "Ship Channel Security Districts," Chapter 68 Section 68.051(b) Definition of Qualifying Facility, Assessments, Houston Ship Channel Security District, https://hscsd.org/wp-content/uploads/2019/03/Chapter-68-Section-68.051b-Facilities.pdf.

6. Expanding USG risk mitigation capabilities to support critical domestic infrastructures

Beyond these organizational and workforce actions, it is also important to expand US active cyber defenses by resourcing threat-hunting teams in the homeland that are designed to find, neutralize, and expel adversary cyber capabilities and attacks with a focus on key critical infrastructures. Today, the United States undertakes such actions on a limited basis. CISA "hunt[s] cyberthreats against U.S. infrastructure to mitigate national risk,"[76] and employs red-teaming capabilities primarily focused on federal civilian networks and some critical infrastructures in coordination with sector risk management agencies and the relevant companies.[77] The Coast Guard likewise does so,[78] exercising its Captain of the Port authorities[79] (within the Department of Homeland Security),[80] and focusing on critical port infrastructure.[81] Cyber Command does, of course, undertake to protect the DOD's Information Network (DODIN),[82] and there are existing DOD programs which, with consent, will review defense industrial base company networks.[83] These are all quite worthwhile activities but would be insufficient in wartime to protect the breadth of critical infrastructures.

As part of its worldwide activities today, Cyber Command's Hunt Forward program works directly with allied and partner nations to ensure the cybersecurity of allied military networks. When asked by hosts, the program also will provide cyber support to host nations' critical infrastructures: "Personnel have deployed more than 85 times to over 30 countries in partner-enabled missions to hunt on host networks. They conducted more than two dozen 'hunt forward' missions in 2024."[84] Those operations not only observe and detect malicious cyber activity on host nation networks but also generate insights that bolster US homeland cybersecurity.

As discussed above, assuring the resilience of the full spectrum of key critical infrastructures in the United States is of ut-

BOX 2: DOD offers "cybersecurity-as-a-service" programs

DOD Cyber Crime Center (DC3) programs

DC3 offers several "cybersecurity-as-a-service" programs. For example, DC3:

> Executes programs to analyze an organization's vulnerability to threat actors based on network architecture, software, and processes. . . . DC3 also conducts penetration testing, which includes network mapping, vulnerability scanning, phishing assessments, and web application testing.

DC3 also offers DCISE, an intelligence-driven automated threat detection and blocking system designed to meet the needs of under-resourced small and medium-sized businesses.

NSA Cybersecurity Collaboration Center (CCC) programs

NSA's CCC offers defense industrial base (DIB) companies numerous DOD-funded cybersecurity services. For example, NSA offers an attack surface management service that:

> Helps DIB customers find and fix issues before they become compromised by identifying DIB Internet-facing assets, then leveraging commercial scanning services to find vulnerabilities or misconfigurations on these networks. Each customer receives a tailored report with issues to remediate that is prioritized based on both severity of the vulnerability and whether it is being exploited.

CCC enables DIB suppliers to conduct "self-service" penetration testing (aka pentests), through a service known as continuous autonomous penetration testing (CAPT). NSA offers the service in partnership with a private company, "leveraging an AI-powered platform to give small businesses a way to conduct their own pentests for internal networks at no cost and with no prior expertise."

NSA also offers protective domain name services (PDNS), provided by commercial providers. PDNS is a filter that blocks users from connecting to malicious domains, protecting against malware, botnets, and ransomware. PDNS is "powered with a continuously evolving combination of proprietary and governmental domain blocklists."

Sources: DOD, *Defense Industrial Base Cybersecurity Strategy*, 2024, 19–20, https://media.defense.gov/2024/Mar/28/2003424523/-1/-1/1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF. *Note: Other sources*: "DoD-Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE)," DOD Cyber Crime Center (DC3), https://www.dc3.mil/Missions/DIB-Cybersecurity/DCISE-Resources/; "National Security Agency Cybersecurity Services," NSA Cybersecurity Collaboration Center, https://www.nsa.gov/Portals/75/documents/Cybersecurity/CCC/DIB_Services_NOV2024.pdf?ver=J3m46AgqPV4%3d; "DIB Cybersecurity Services," NSA/Central Security Service, https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/; "Fortifying the Defense Industrial Base (DIB): NodeZero® for Supply Chain Security," Horizon3.ai, https://horizon3.ai/nsa-capt-program-for-dib-suppliers/; and NSA/CCC, "DIB Cybersecurity Services."

most importance. This will require support both prior to, and during, wartime for those critical infrastructures most relevant to national defense, particularly the electric grid, pipelines, air, rail, and water/wastewater systems (and, as necessary, with additional focus on ports). While the Defense Department has not generally undertaken cyber operations in the United States apart from defense of the DODIN, there are overwhelming and obvious policy reasons for DOD to strengthen and make effective cybersecurity for key critical infrastructures during a war. Accordingly, in wartime, US Cyber Command and its components, starting with the National Guard units that have OT hunting experience, should be authorized to undertake domestic threat-hunting activities strictly limited to the operational technology systems of Section 9 entities. Prior to wartime, US Cyber Command would not operate domestically beyond the DODIN outside of a support capacity, such as may be authorized by the Defense Support to Civil Authorities (DCSA) framework,[85] or an appropriate consent framework.

Leveraging US Cyber Command's capabilities in these focused ways recognizes that the Command need not—and in fact does not have the resources to—cover all critical infrastructure organizations throughout the United States. Rather, Cyber Command (including the National Guard),[86] CISA, and the Coast Guard should coordinate their activities, focusing in the first instance on the operational technology systems of the most important companies—those already federally designated as critical Section 9 companies for which a "cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[87] Such coordination should be done under the auspices of the NCD and would involve establishing plans for wartime action. Moreover, the government's combined threat-hunting capabilities should be coordinated with the relevant critical infrastructures and the proposed Integrated Cybersecurity Providers Corps (described above), each of whom should be engaged in prewartime planning.

BOX 3: Cyber Command threat hunting in the United States

While the Department of Defense has engaged in operations in the United States including through the Northern Command, Transportation Command, Space Command, and Strategic Command activities, Cyber Command operations in the homeland are mainly directed to protection of the DODIN and to support the defense industrial base. Expanding Cyber Command's threat-hunting activities to the broader private sector would likely raise privacy and civil liberties concerns (and could require changes to privacy law), but such concerns could be ameliorated with no impact on mission success by permitting domestic threat hunting by Cyber Command only during wartime—and only on Section 9 entities' operational technology systems (which are primarily designed for industrial control and do not typically store personally identifiable information), and by implementing appropriate procedural limitations. Some illustrative examples follow:

- **Search authority limitations:** Cyber Command (as well as CISA and the Coast Guard), under the auspices of the ONCD, should work with Section 9 companies and the ICPC prior to conflict to establish supporting arrangements. If necessary, and absent any such agreements, wartime threat hunting on Section 9 entities' OT networks could be undertaken pursuant to Fourth Amendment reasonable search criteria and/or warrants.
- **Purpose limitation:** Information gained through government access should be used only for cybersecurity purposes, as that term is defined in the Cybersecurity Information Sharing Act of 2015 [see CISA §102(4)]. Information gained should not be used by any federal, state, tribal, or local government to regulate (including via an enforcement action) the lawful activity of any nonfederal entity
- **Data retention limitations**: There should be zero data retention; sensitive data (e.g., personal data, corporate intellectual property) should not be stored beyond its immediate use.

Sources and notes:
The Northern Command, which has a homeland defense and civil support mission, is operating domestically to secure the southern border, according to *Breaking Defense*, but is serving in a support capacity to civilian law enforcement as its operations on domestic soil are limited by the Posse Comitatus Act. Specifically, Defense Secretary Hegseth "has authorized troops from US Northern Command to conduct mobile ground-based monitoring to track suspected illegal activity." See Carley Welch, "Pentagon Deploys Offensive Cyber Ops to Target Criminal Orgs, Bolster Southern Border Security," *Breaking Defense*, May 7, 2025, https://breakingdefense.com/2025/05/pentagon-deploys-offensive-cyber-ops-to-target-criminal-orgs-bolster-southern-border-security/. DOD is, moreover, "using offensive cyber capabilities to bolster security at the southern border and disrupt the 'illicit' behavior of transnational criminal organizations," reported *Breaking Defense*, and, as the defense secretary's chief cyber adviser, Ashley Manning, is quoted as saying in the above piece: "We are actively working to disrupt these networks, intercept their communications and dismantle their digital infrastructure. By denying them to take haven in the digital realm, we can significantly degrade their ability to operate."

Separately, regarding privacy and civil liberties concerns, James A. Lewis wrote: "Any discussion of an expanded government role in defending networks runs into powerful antibodies that grow out of civil liberties and privacy concerns. Even if existing legal authorities allow for an expanded government role, the 'perception problem' remains significant. . . . Frankly, these privacy and civil liberties concerns are reasonable." See James A. Lewis, "Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border," Center for Strategic and International Studies (blog), June 4, 2015, https://www.csis.org/blogs/strategic-technologies-blog/hunting-hackers-nsa-secretly-expands-internet-spying-us-border.

B. Actions outside the United States: Respond with offensive actions to state-supported intrusions into US critical infrastructures

As described above, China's Volt Typhoon malware infiltrated critical infrastructures throughout the United States and its Salt Typhoon malware intruded into communications; moreover, other adversarial nations have undertaken comparable intrusions. Those actions have understandably led to calls for the United States to take aggressive action in response.[88] Responsive actions are warranted—and specific approaches are described below. However, it is important to take any such responses as part of a strategically thoughtful approach, recognizing the following considerations, so that there is a net benefit to the United States.

As a starting point, it seems reasonable to assume that the United States has intelligence access into the activities of cyber adversaries. While the revelations from the Snowden disclosures of a decade ago can only be illustrative, they do indicate a rather substantial capability.[89] More recently, prior to Russia's invasion of Ukraine, the US government undertook to disclose significant information gleaned from sensitive (undescribed) capabilities about intended Russian actions.[90] Without trying to parse the precise US capability against the PRC, Rus-

sia, and others, it seems important not to act in such a way as to impede those capabilities.

Additionally, in undertaking action against an adversary, it is always important to recognize the adversary's capability to respond. As the Pentagon saying goes, "The enemy gets a vote."[91] Disrupting critical infrastructure operations in the PRC or elsewhere would be of important consequence in the context of a conflict: Doing so prior to conflict might not only be escalatory, but could also disclose vulnerabilities that the PRC or others could take steps to ameliorate.

These considerations should not, however, preclude taking actions, given the degrees of intrusion described above—and, in fact, failure to act would be an unfortunate demonstration of weakness. Focusing on the PRC as a key challenge, the issue is how best to take actions that demonstrate the PRC's vulnerability—thereby enhancing deterrence—without unduly affecting US capabilities needed for intelligence purposes and/or for operations during a conflict. Two approaches seem warranted.

First, the United States could engage in hybrid actions against the PRC, utilizing cyber methods to support other activities, such as information operations. For example, and somewhat analogous to what was done vis-à-vis the Soviet Union in the Cold War, the United States could use the multiple internet networks in the PRC as places to provide information that citizens normally could not easily access. WeChat is one example—and though the PRC internet censors would undertake as quickly as possible to keep such material off the networks, a 100 percent success rate is not assured.

Second, when it comes to offensive cyber operations, the United States has historically "operated quite cautiously with respect to the possible negative impacts of campaigns and without a strong expectation among political leaders that cyber operations can deliver strategically significant outcomes."[92] However, the growing threat posed by PRC-affiliated threat actors, most recently evidenced by the Typhoon cases,[93] has jump-started discussions among military and political leaders about the need to impose consequences on US adversaries in response to such activity.[94] In keeping with this shift, Admiral (Ret.) Mike Rogers, former commander of US Cyber Command and director of the National Security Agency, recently talked about US offensive cyber operations in a podcast, saying: "I believe that what we ought to authorize is not just going after infrastructure but directly going after capability within those nations that are generating these effects against us."[95] Rob Joyce, former director of the NSA Cybersecurity Directorate, has similarly stated:

> Adversary schemes to penetrate digital infrastructure . . . must be met with a multilayered response. Introducing "friction" into the equation for threat actors by doggedly countering and frustrating their efforts becomes a baseline strategy.
>
> Fending off attacks is followed in short order by "disruption," which [requires] … taking out "their infrastructure . . . their tools." This covers a wide range of actions, from "getting them ejected from their botnets all the way to . . . turn[ing] over their tools so that the commercial world can find them in other places."
>
> Then comes the "offensive cyber destructive level," [including] . . . confronting nation state actors directly, including operations extending "all the way into critical infrastructure" with the intent "to deter them because they're afraid I'm going to cyber them mightily. Right at that point."[96]

One way that the United States can accomplish the foregoing is to make certain penetrations obvious, using techniques that are well-known, and to attack targets with demonstrative but not necessarily escalatory potential. Doing so could demonstrate capabilities that could be used in wartime, illustrating that in the cyber arena US adversaries are as vulnerable to attack as is the United States. Additionally, at least some of the identified advanced, persistent threat groups in China and elsewhere appear to be nongovernmental,[97] and responsive actions against the infrastructures being utilized by those groups would be appropriate. Taking down an advanced persistent threat actor's infrastructure would not be a permanent solution, but it would be disruptive and have deterrent value. Such actions have some precedent including Cyber Command's 2019 takedown of the Russian Internet Research Agency.[98]

C. Private-sector actions to disrupt criminal activities including dark web sites and to support the government including as a cyber reserve in wartime

Offensive action has the potential to be significantly more effective when the US government works in partnership with highly capable private-sector actors. In recognition of this reality and as one example, the US Department of Treasury's Project Fortress "aims to enhance cybersecurity in the financial sector by moving . . . to a more proactive defense model that includes offensive capabilities."[99] In support of these aims, Project Fortress is creating automated intelligence-sharing pipelines between the US government and the financial sector and seeking to exploit the unique capabilities and perspectives that each partner has to offer.[100] This model goes beyond collaboration to integration, seeking real-time situational awareness between the government and the private sector. Offensive actions can "make clear to US adversaries that they will face consequences for their attacks," wrote then-Deputy Treasury Secretary Wally Adeyemo.[101] Currently, the publicly stated offensive actions associated with Project Fortress involve the use of Department of the Treasury authorities to sanction "threat actors targeting the financial system."[102]

As one key step to enhancing public-private coordination, the national cyber director should build on the Project Fortress approach including the use of automated intelligence pipelines. The NCD could help ensure the broad reach of informa-

tion-sharing efforts such as the NSA's CCC and Cyber Command's Under Advisement. Furthermore, there are numerous other information-sharing activities that could be supported through automated intelligence pipelines. These include sector-specific information sharing and analysis centers and private-sector activities such as those undertaken by the Center for Internet Security.[103]

A good starting place for expanded involvement by the private sector in active defense would be in response to the multitude of ongoing ransomware attacks. In recent years, the Department of Justice—increasingly working with the private sector—has had some notable successes in its fight against ransomware,[104] including arrests of major illicit actors,[105] disruptions and takedowns of key ransomware digital infrastructure,[106] and, in a small number of cases, even seizure of ransomware payments, depriving illicit actors of their benefit.[107] However, despite these actions, the number of ransomware attacks has continued to increase.[108]

Given the issues ransomware and other criminal intrusions present, a useful set of initial private-sector offensive actions would be to work in coordination with the government to prioritize the targeting and blocking of so-called bulletproof hosting (BPH) providers.[109]

BPH providers are illicit cloud infrastructure providers that host malicious domains and provide various services for cybercriminals.[110] BPH providers use complex technical arrangements to evade law enforcement takedown and abuse complaints, thereby allowing cybercriminals to operate with near impunity. BPH providers have been known to "help their clients evade detection by law enforcement and continue their crimes uninterrupted by monitoring sites used to blocklist technical infrastructure used for crime, moving 'flagged' content to new infrastructure, and registering all such infrastructure under false or stolen identities."[111] Earlier this year, Dutch police took down a BPH provider (that reportedly facilitated Lockbit ransomware attacks) and advertised that customers could commit crimes from its servers and that "the owners of these servers would remain anonymous when law enforcement agencies would make inquiries with them, and payments for the services purchased could also be made anonymously via crypto currency," according to reports and the police statement.[112] BPH providers offer a range of services that make takedown requests difficult, including, as CISA recently warned, so-called fast flux services, which help malicious actors evade detection by hiding the location of malicious servers.[113]

Successfully targeting BPH providers would be effective because it would "halt malicious activity early in the kill chain," according to a cyber threat intelligence firm.[114] Such activities against BPH sites would also provide the knowledge and operational skills that would allow the authorized companies to effectively support wartime US government offensive cyber campaigns, as described below.

The private sector could undertake not only counter-BPH actions but broader activities against cyber criminals as well as nation-state adversaries at three levels: supplying information for the government to use in its own actions; undertaking and expanding actions taken on a private-sector entity's own networks; and, in coordination with the government during wartime or specified circumstances, taking offensive actions against approved targets beyond owned networks.

First, supplying information to the government would not be a new activity since there are already information flows from the private sector to the government (e.g., programs like DOD's Under Advisement). The additional part would be for the private sector to increase its intelligence, surveillance, and reconnaissance activities, searching and analyzing beyond what is being done in order to act as an operational intelligence arm for governmental actions.

Second, undertaking action on an entity's own networks is generally authorized according to the terms and conditions of use. Section 104 of the Cybersecurity Information Sharing Act of 2015 specifically authorizes private entities to monitor their own networks and "operate a defensive measure that is applied to an information system of such private entity in order to protect the rights or property of the private entity."[115] Network owners thus have the authority to bar users acting in violation of the network owners' terms and conditions—and have done so for multiple reasons including an entity's use of the network to install malware or otherwise undertake cyberattacks. By way of example, Google recently shut down a spyware operation hosted on one of Google's developer platforms,[116] pursuant to Google's terms of use, which prohibit its customers from hosting malicious software or spyware operations on its platforms.[117] In particular, hyperscale cloud companies who are network owners could usefully work with one another and the government to combine their intelligence capabilities and establish a campaign approach—consistent with their terms and conditions of network use—to keep off the network any entity using BPH capabilities or otherwise undertaking inappropriate malicious actions.[118] For the private sector to undertake such offensive measures on a concerted basis, it would be important that the terms of service include the ability of the cybersecurity provider to work with the government to protect against malicious intrusions.

Third, the private sector—and particularly the ICPC companies—could under certain circumstances and most importantly during wartime, undertake direct action against an entity, doing so under the direction and control of the government. The importance of doing so could well arise in wartime as the government almost certainly would benefit from added capabilities. The private-sector companies comprising the ICPC could essentially act as a cyber reserve. To make such actions most effective, the ICPC companies and the government should plan and train for such contingencies. Such an arrangement would be somewhat analogous to the Civil Reserve Air Fleet,[119] and, as with CRAF, the private-sector actors should be appropriately compensated through line-item funding in the DOD budget. Short of war and in specifically authorized circumstances—somewhat akin to covert action under Title 50,

BOX 4: Private-sector offensive operations: Key factors

To make private-sector offensive operations both effective and conforming to national policy, the government would need to address:

- **Targeting.** The government should designate the targets against which the private ICPC actor would take offensive action.
- **Liability.** The government would need to amend existing statutes—specifically the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act—to protect private-sector actors from criminal liability when acting with the US government's knowledge and consent. Under a revised statute, the government could authorize private-sector wartime actions and at times short of wartime and in specified circumstances actions against designated adversaries that would not trigger criminal liability and prosecution.
- **Indemnification.** In return for the participation of a private-sector actor, the government should also provide for indemnification in the event that the private-sector actor, acting in an authorized manner, were to cause unintended damage, for example, through mistaken attribution, inadvertently hitting the wrong target, causing collateral damage, or otherwise causing harm.
- **Cost allocation.** Finally, the government should consider how the costs of any offensive efforts taken by the private sector would be allocated. While private-sector actors likely would be willing to make reasonable investments in joint offensive campaigns, the government should be willing to shoulder the costs of offensive campaigns taken in the interest of national security.

Sources and notes: Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2523, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285. Regarding liability, the Active Cyber Defense Certainty Act (ACDC) is noteworthy (see H.R. 3270, https://www.congress.gov/116/bills/hr3270/BILLS-116hr3270ih.pdf.) Introduced in 2019 but not passed, ACDC sought to revise the Computer Fraud and Abuse Act to enable authorized companies to take defensive measures (e.g., attributing an attack or disrupting a cyberattack without damaging others' computers) outside the boundaries of their own networks without being subject to criminal prosecution.

including appropriate congressional notification—private-sector ICPC companies might be authorized to act against designated targets.[120]

To reiterate, in undertaking offensive operations against designated targets, private-sector ICPC companies should only act in coordination with the government.[121] However, the Cybersecurity Planning and Operations Council described above, along with wartime planning with Cyber Command, would provide the necessary venues for such coordination, particularly if, as suggested, authorized private-sector actions were limited to the select group of highly-capable companies comprising the Integrated Cybersecurity Providers Corps.[122] In effect, such companies should be looked upon as an important asset able to act as a cyber reserve force.[123]

IV. Conclusion

A national cybersecurity strategy will require an operational road map for offensive and defensive campaigning and significantly enhanced resilience for key critical infrastructures built upon the development and adoption of safe coding and the implementation of zero trust architectures. Establishment of such capabilities will provide the president and the national leadership with the necessary capabilities to deter and defeat nation-state and criminal activities in cyberspace.

About the authors

Franklin D. Kramer is a distinguished fellow at the Atlantic Council and serves on its board. He is a former US assistant secretary of defense for international security affairs.

Robert J. Butler is a co-founder and the managing director of Cyber Strategies LLC. He served as the first deputy assistant secretary of defense for space and cyber policy and has also served as a chief security officer for a global data center company, among various other corporate roles.

Melanie J. Teplinsky is an adjunct professor at American University, Washington College of Law, where she is a senior fellow in the Technology, Law and Security Program. She served (pre-IPO) on the advisory board for CrowdStrike Inc. and previously practiced technology law at Steptoe & Johnson LLP.

Appendix: Requirements for scaling resilience through safe coding and zero trust architectures

Accelerating the development and adoption of safe coding and of zero trust architectures for key critical infrastructures requires several steps.

- **Enhance the security of software code for key critical infrastructures.**
  - Utilize formal methods for code in key critical infrastructures that are identified as Section 9 companies.
  - Engage private-sector companies currently utilizing formal methods to support utilization for Section 9 companies.
  - Support the development and adoption of key cybersecurity technology projects focused on safe coding being undertaken by the Defense Advanced Research Projects Agency.
- **Establish trusted architectures.**
  - Establish regulatory requirements for Section 9 companies in key sectors mandating zero trust requirements, with the national cyber director providing overall coordination/harmonization and the sector risk management agencies generating the specific regulatory requirements.
  - For each sector that includes Section 9 companies, organize a task force consisting of government and private-sector experts that can both generate the technical requirements for and support the establishment of zero trust controls with the actual implementation activities provided through a combined effort of the Section 9 company and outside private-sector expert assistance.
  - Develop and/or utilize advanced capabilities including artificial intelligence (including agentic AI), ephemeral authentication, and quantum-resistant encryption.
- **Organize "regional resilience districts" for key areas.** The purpose is to develop resilience among interlocking capabilities, including limiting cascading effects and establishing a reconstitution mechanism that would be required after a cyberattack.
- **Establish pilot programs for key port cities.** As initial efforts, these pilot programs should focus on zero trust architectures for key capabilities including local governance and establishing mechanisms for prompt recovery from cyberattacks.
- **Provide financial assistance.** Recipients should include each Section 9 company and regional resilience district undertaking the establishment of zero trust architectures. This assistance should include direct funding and/or tax credits to support the initial effort and upgrades and maintenance.

Endnotes

1 The Department of Homeland Security annually identifies and maintains a list of critical infrastructure entities that meet the criteria specified in Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, Section 9(a)("Section 9 entities"). Section 9 entities are defined as «critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.» See "Support to Critical Infrastructure at Greatest Risk ("Section 9 Report") Summary," Cybersecurity and Infrastructure Security Agency (CISA), February 8, 2021, https://www.cisa.gov/resources-tools/resources/support-critical-infrastructure-greatest-risk-section-9-report-summary.

2 Representative Mark E. Green of Tennessee, then-chairman of the House Homeland Security Committee, is quoted in Jen Easterly's blog, "Strengthening America's Resilience Against the PRC Cyber Threats," CISA, January 15, 2025, https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats.

3 Adam Goldman, "'Unrestrained' Chinese Cyberattackers May Have Stolen Data from Almost Every American," *New York Times*, September 4, 2025, https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html.

4 Scott Caveza, "Salt Typhoon: An Analysis of Vulnerabilities Exploited by this State-Sponsored Actor," *Tenable Blog*, January 23, 2025, https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor; see also Joint Cybersecurity Advisory, "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," September 2025; and Davina Tham, "Singapore Actively Dealing with Ongoing Cyberattack on Critical Infrastructure: Shanmugam," Mediacorp's CNA, updated July 21, 2025, https://www.channelnewsasia.com/singapore/unc3886-cyber-security-threat-actor-attack-singapore-5245791.

5 Microsoft Threat Intelligence, "Disrupting Active Exploitation of On-premises SharePoint Vulnerabilities," July 22, 2025, https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/#attribution.

6 Bill Gertz, "Hackers Breach Intelligence Website Used by CIA," *Washington Times*, July 24, 2025, https://www.washingtontimes.com/news/2025/jul/24/major-intelligence-website-hacked-search-cia-spying-secrets/.

7 Kristina Beek, "US Nuclear Agency Hacked in Microsoft SharePoint Frenzy," *DarkReading,* July 23, 2025, https://www.darkreading.com/cyberattacks-data-breaches/us-nuclear-agency-hacked-microsoft-sharepoint.

8 "US Nuclear and Health Agencies Hit in Microsoft SharePoint Breach," *Washington Post*, July 23, 2025, https://www.washingtonpost.com/technology/2025/07/23/sharepoint-microsoft-hack-nih-nnsa/; and David DiMolfetta and Frank Konkel, "DHS Impacted in Hack of Microsoft SharePoint Products, People Familiar Say," Nextgov/FCW, July 23, 2025, https://www.nextgov.com/cybersecurity/2025/07/dhs-impacted-hack-microsoft-sharepoint-products-people-familiar-say/406941/.

9 Microsoft assesses with "moderate confidence" that Storm 2603 is a China-based threat actor. See "Disrupting Active Exploitation of On-premises SharePoint Vulnerabilities," Microsoft Threat Intelligence, updated July 23, 2025, https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/.

10 "Operation Aurora: The Largest Cyber Heist in History," *Medium*, January 26, 2023, https://medium.com/kopfkino/operation-aurora-the-largest-cyber-heist-in-history-6da33219b121.

11 US House of Representatives Committee on Oversight and Government Reform, "The OPM Data Breach: How the Government Jeopardized Our National Security for More Than a Generation," September 7, 2016, https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

12 "Inside the Equifax Breach: A Case Study on What Went Wrong,» *Medium*, June 21, 2025, https://medium.com/@shajalapsdel/inside-the-equifax-breach-a-case-study-on-what-went-wrong-84c4edf50536

13 National Counterintelligence Security Center, "HAFNIUM Compromises MS Exchange Servers," August 19, 2021, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/HAFNIUM%20Compromises%20MS%20Exchange%20Servers.pdf.

14 US Government Accountability Office, "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response," GAO blog, April 22, 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

15 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

16 National Cyber Security Centre, "Russia Behind Cyber Attack with Europe-wide Impact an Hour Before Ukraine Invasion," May 10, 2022, https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion.

17 Department of Justice, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," Press Release, March 24, 2016, https://www.justice.gov/archives/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

18 DoJ, "Seven Iranians."

19 CISA, "Iran Threat Overview and Advisories," n.d., https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran.

20 US Department of the Treasury, "Treasury Designates Iranian Cyber Actors Targeting U.S. Companies and Government Agencies," Press Release, April 23, 2024, "Treasury https://home.treasury.gov/news/press-releases/jy2292.

21 Andy Greenberg, "A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems," *Wired*, November 20, 2019, https://www.wired.com/story/iran-apt33-industrial-control-systems/.

22 FBI, "Update on Sony Investigation," Press Release, December 19, 2014, https://www.fbi.gov/news/press-releases/update-on-sony-investigation.

23 Thomas P. Bossert, "It's Official: North Korea Is Behind WannaCry," *Wall Street Journal*, December 18, 2017, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537.

24 Joe Tidy, "North Korean Hackers Cash Out Hundreds of Millions from $1.5bn ByBit Hack," BBC, March 9, 2025, https://www.bbc.com/news/articles/c2kgndwwd7lo; and Fortune Samuel, "From Upbit's $49M to Bybit's $1.46B: How Lazarus Group is Terrorizing Crypto," *Cointab*, March 13, 2025, https://cointab.com/how-lazarus-group-is-terrorizing-crypto/.

25 Doreen Horschig, "How Are Cyberattacks Fueling North Korea's Nuclear Ambitions?," Center for Strategic and International Studies, July 31, 2024, https://www.csis.org/analysis/how-are-cyberattacks-fueling-north-koreas-nuclear-ambitions.

26 CISA, "North Korea Threat Overview and Advisories," https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea; DoJ, "North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers," Press Release, July 25, 2024, https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

27 Kurt Baker, "Ransomware Examples: 16 Recent Ransomware Attacks," CrowdStrike, March 28, 2024, https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-examples/.

28 FBI, "Ransomware," n.d., https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware; and Josh Nadeau, "Research Finds 56% Increase in Active Ransomware Groups," IBM, https://securityintelligence.com/news/research-finds-56-percent-increase-active-ransomware-groups/

29 See, e.g., Microsoft, "National Public Data Breach: What You Need to Know," https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535 (describing 2024 National Public Data breach exposing "up to 2.9 billion records with highly sensitive personal data of up to $170 million people in the US, UK and Canada").

30 The world's first "generative AI-powered ransomware implant" already is under development, Kevin Poireault, "Researchers Discover First Reported AI-Powered Ransomware," *Infosecurity Magazine*, updated September 5, 2025, https://www.infosecurity-magazine.com/news/first-ai-powered-ransomware/.

31 Anthropic, "Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign," November 13, 2025, https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf.

32 The article states that "80-90% of the operations involved in the attack were performed without a human in the loop." See Aisha Down, "AI Firm Claims It Stopped Chinese State-Sponsored Cyber-Attack Campaign," *Guardian*, November 14, 2025, https://www.theguardian.com/technology/2025/nov/14/ai-anthropic-chinese-state-sponsored-cyber-attack.

33 Anthropic, "Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign," November 13, 2025, https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf.

34 See, e.g., "Detecting and Countering Misuse of AI," Anthropic blog, August 2025; the blog described how a sophisticated cybercriminal "used Claude Code to commit large-scale theft and extortion of personal data."

35 For example, one cybercriminal "used Claude to develop, market, and distribute several variants of ransomware, each with advanced evasion capabilities, encryption, and anti-recovery mechanisms. The ransomware packages were sold on internet forums to other cybercriminals for $400 to $1,200 USD."

36 "Criminals with few technical skills are using AI to conduct complex operations, such as developing ransomware, that would previously have required years of training," according to the Anthropic blog, "Detecting and Countering Misuse of AI."

37 "Low-barrier tools like large language models (LLMs) and agentic AI platforms are transforming the cyber threat landscape by enabling 'script kiddies' and non-state actors to automate, scale, and iterate attacks against industrial control systems. The convergence of unsophisticated actors with powerful AI tools widens the attack surface for critical infrastructure while complicating attribution and defense." Daniel Pereira, "A New Wave of Cyberattackers Enabled by Adversarial Use of LLMs and Agentic AI," *OODA Loop,* May 9, 2025.

38 Annie Fixler, RADM (Ret.) Mark Montgomery, and Rory Lane, *Military Mobility Depends on Secure Critical Infrastructure,* Monograph, Foundation for Defense of Democracies, March 27, 2025, 4, https://www.fdd.org/analysis/2025/03/27/military-mobility-depends-on-secure-critical-infrastructure/.

39 Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the U.S. Intelligence Community*, March 2025, 11, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

40 ODNI, *Annual Threat Assessment of the U.S. Intelligence Community*, 19.

41 Anna Fratsyvir and Andrea Januta, "Ukrainian Hackers Wipe Databases at Russia's Gazprom in Major Cyberattack, Intelligence Source Says," *Kyiv Independent*, July 18, 2025, https://kyivindependent.com/ukrainian-intel-hackers-hit-gazproms-network-infrastructure-sources-say-07-2025/.

42 Blake Hall, "How AI-driven Fraud Challenges the Global Economy—and Ways to Combat It," *World Economic Forum*, January 16, 2025, https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/.

43 "The Cost of Cyber Theft to the U.S. Economy in 2024: Projected to Exceed $350 Billion," CipherTex Data Security, May 24, 2024, https://ciphertex.com/2024/05/24/the-cost-of-cyber-theft-to-the-u-s-economy-in-2024/#:~:text=The%20Financial%20Impact&text=This%20figure%20includes%20expenses%20related,%E2%80%8B%20(Astra%20Security)%E2%80%8B.

44 The breadth of estimates, ranging from the billions to the trillions, is reflected in a story from *The Economist*: "Nevertheless, it is clear that the scale is staggering, with billions, possibly trillions, of dollars in economic costs each year. The low end of the range comes from tallies of reported crimes by law-enforcement agencies. The FBI said it received reports of direct losses of $16.6bn in 2024, a 33% increase over 2023. Adding in unreported losses and wider economic costs leads to bigger numbers. Britain puts its current annual losses at more than £27bn (based on old data). The European Commission reckons that the worldwide costs of cybercrime were €5.5trn ($6.5trn) in 2021." See "The Uber of the Underworld," *Economist*, May 29, 2025, https://www.economist.com/international/2025/05/29/the-uber-of-the-underworld. A top US national security official warned in 2023 that the global cost of cybercrime is projected to reach $23 trillion by 2027. See US Department of State, "Digital Press Briefing with Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technologies," October 18, 2023, https://2021-2025.state.gov/digital-press-briefing-with-anne-neuberger-deputy-national-security-advisor-for-cyber-and-emerging-technologies/.

45 Estefania Vergara Cobos and Selcen Cakir, "A Review of the Economic Costs of Cyber Incidents," World Bank, 2024, 13, https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf.

46 For a description of the role of the private sector in warfare see Franklin D. Kramer, "The Sixth Domain: The Role of the Private Sector in Warfare," Atlantic Council, October 4, 2023, https://www.atlanticcouncil.org/wp-content/uploads/2023/10/The-sixth-domain-The-role-of-the-private-sector-in-warfare-Oct16.pdf.

47 "The National Counterterrorism Center," home page, ODNI, https://www.dni.gov/index.php/nctc-home.

48 "Office of the National Cyber Director," home page, https://www.whitehouse.gov/oncd/.

49 White House, "Presidential Policy Directive—United States Cyber Incident Coordination," July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

50 There have been previous recommendations for the establishment of a center along these lines. See Kramer, "The Sixth Domain," 8–10; and Franklin D. Kramer and Robert J. Butler, "Cybersecurity: Changing the Model," Atlantic Council, April 24, 2019, https://www.atlanticcouncil.org/in-depth-research-reports/report/cybersecurity-changing-the-model/

51 CISA, "Sector Risk Management Agencies," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies.

52 Exec. Order No. 14239, 90 Fed. Reg. 13267, "Achieving Efficiency through State and Local Preparedness," March 19, 2025, https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/.

53 This model could be scaled beyond the Section 9 critical infrastructures, possibly through development of a dynamic Section 9 list that accounts for evolving cyber risks, as identified and prioritized in the risk registry proposed herein.

54 Kramer, "The Sixth Domain," 12.

55 Kramer, "The Sixth Domain," 12. Such an approach to the requirements for the ICPC would be somewhat analogous to how the government is establishing requirements for its use of cloud technology, particularly when relying on private-sector cloud companies.

56 Kramer, "The Sixth Domain," 12.

57 CISA, "Joint Cyber Defense Collaborative," https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative; and NSA Cybersecurity Collaboration Center, https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/.

58 Cyber National Mission Force Public Affairs, "Cybercom's 'Under Advisement' to Increase Private Sector Partnerships, Industry Data-Sharing in 2023," June 29, 2023, https://www.cybercom.mil/Media/News/Article/3444464/cybercoms-under-advisement-to-increase-private-sector-partnerships-industry-dat/; see also Department of Treasury, "Project Fortress–2025 Offerings," https://home.treasury.gov/system/files/216/Project-Fortress-Brochure.pdf.

59 Actionable intelligence information includes operational intelligence, such as indicators of compromise (IOCs), and tactical intelligence such as threat actor tactics, techniques, and procedures.

60 Veronica A. Chinn, Lee T. Furchas, and Barian A. Woodward, "Information Sharing with the Private Sector," National Defense University, *Joint Force Quarterly* 73, April 1, 2014, 37–38, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/577502/information-sharing-with-the-private-sector/#:~:text=A%20key%20element%20of%20extending,%2Dshare%E2%80%9D%20culture%20of%20integration.

61 CISA 2015 reauthorization (whether "clean" reauthorization, as some urge to avoid delay, or passage of an updated and expanded version of the law designed to address current cyber threats), will be important inasmuch as the legal protections set forth in CISA 2015 have been essential to private-sector participation in information sharing with the government.

62 Franklin D. Kramer and Robert J. Butler, "Expanding the Role of the National Guard for Effective Cybersecurity," *Hill*, April 28, 2021, https://thehill.com/opinion/cybersecurity/550740-expanding-the-role-of-the-national-guard-for-effective-cybersecurity/.

63 See "State Partnership Program," National Guard, https://www.nationalguard.mil/Leadership/Joint-Staff/J-5/International-Affairs-Division/State-Partnership-Program/.

64 See Jon Harper, "Army Recruits Officers from Meta, OpenAI and Palantir to Serve in New Detachment," *DefenseScoop*, June 13, 2025, https://defensescoop.com/2025/06/13/army-detachment-201-executive-innovation-corps-meta-openai-palantir/.

65 Cynthia Brumfield, "Civilian Cyber Reserves Gaining Steam at the US Federal and State Levels," *CSO Online*, January 24, 2024, https://www.csoonline.com/article/1297690/civilian-cyber-reserves-gaining-steam-at-the-us-federal-and-state-levels.html.

66 See intelligence sharing under the Department of the Treasury, "Project Fortress–2025 Offerings."

67 Several high-tech companies offer this type of construct already; see Top Volunteer Time Off Companies | 35 Programs to Know. Further, the American Bar Association's Pro Bono Initiative Challenge offers some useful lessons for setting up such a program.

68 For example, akin to the Law Firm Pro Bono Challenge Initiative, which spurred large law firms to provide the institutional support for their attorneys to provide pro bono legal services, a challenge could be initiated to encourage companies to support their employees' "pro bono" cybersecurity work. See *Report on the Law Firm Pro Bono Challenge Initiative*, Pro Bono Institute, 2024, https://www.probonoinst.org/wp-content/uploads/2024_PBI_Challenge-ReportFinal.pdf..

69 Pursuant to the Volunteer Responder Incentive Protection Act (VRIPA), the first $600 of volunteer firefighter stipends (and other incentives) are exempt from federal tax; see "Benefits," https://www.volunteerfirefighter.org/benefits. See also the Taxpayer Certainty and Disaster Relief Act of 2020, Section 103 (making the federal tax exemption permanent); and David Finger, "Federal Tax Exemption for Volunteer Responders Made Permanent," January 26, 2021, https://www.nvfc.org/federal-tax-exemption-for-volunteer-responders-made-permanent/. Some states also offer tax credits for volunteer firefighters: see, e.g., https://marylandvolunteer.org/benefits/.

70 "Do Volunteer Firefighters Get Paid?," https://volunteerguide.org/2024/09/06/do-volunteer-firefighters-get-paid/; and "Volunteer Firefighter Pension Fund," Colorado Department of Local Affairs, https://dlg.colorado.gov/volunteer-firefighter-pension-fund..

71 Some states may likewise undertake to support regional approaches.

72 In designing such a pilot, lessons could be drawn from programs such as the Jack Voltaic critical infrastructure cybersecurity exercise, a regionally focused exercise addressing cities' abilities to respond to a cyberattack. The Voltaic exercise "explored the interdependencies, roles and responsibilities among military installations and cities, which often share critical infrastructure." See George I. Seffers, "What Does the Future Hold for Jack Voltaic Cyber Exercise?," *AFCEA's Cyberedge*, August 1, 2024, https://www.afcea.org/signal-media/cyber-edge/what-does-future-hold-jack-voltaic-cyber-exercise. Also notable in connection with regional research development collaboration networks is recent congressional interest in regional approaches to mitigating cybersecurity risk in key sectors. *See*, *e.g.*, "The Cybersecurity in Agriculture Act," which proposes establishment of a national network of five Regional Agricultural Cybersecurity Centers; and "US senators introduce bipartisan bill to combat foreign cyberattacks targeting American agriculture sector," Industrial Cyber, September 24, 2025, https://industrialcyber.co/regulation-standards-and-compliance/us-senators-introduce-bipartisan-bill-to-combat-foreign-cyberattacks-targeting-american-agriculture-sector/.

73 "Port Houston," https://porthouston.com/; and Houston Ship Channel Security District, https://hscsd.org/.

74 33 C.F.R. Part 6, as amended November 30, 2025, https://www.ecfr.gov/current/title-33/chapter-I/subchapter-A/part-6.

75 National Defense Authorization Act for Fiscal Year 2024, Section 1517, Pub. L. No. 118-31, https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf.

76 Department of Homeland Security, CISA, "Threat Hunting: Fiscal Year 2023 Report to Congress," July 13, 2023.

77 "Statement on CISA's Red Team," CISA, March 12, 2025, https://www.cisa.gov/news-events/news/statement-cisas-red-team The administration has raised issues regarding CISA activities in the context of elections, and its proposed budget provides for plans to reduce CISA's workforce by approximately 1,000 people. But with the administration fully recognizing the threat China poses, it should avoid reducing the important CISA capabilities that are designed to contest China's (and others') cyberattacks. The administration has directly recognized these concerns, stating, by way of example: "CISA's Red Team is among the best in the world and remains laser focused on helping our federal and critical infrastructure partners identify and mitigate their most significant vulnerabilities and weaknesses. This has not changed. Contrary to inaccurate reporting, CISA has not "laid off" our Red Team. . . . CISA's Red Teams continue their work without interruption. The team works directly with network defenders, system administrators, and other technical staff to address strengths and weaknesses across critical infrastructure networks and systems. They continue to assist organizations in refining their detection, response, and hunt capabilities to protect the nation's critical infrastructure from a range of threats."

78 US Coast Guard Cyber Command, "US Coast Guard Cyber Protection Team (CPT)."

79 Captain of the Port authorities are quite broad, with key authorities set forth in 33 C.F.R. Parts 6 and 160. A recent GAO report explains: "The Coast Guard relies on both cyber and non-cyber personnel to help mitigate maritime cyber risks. In particular, the Coast Guard relies on cyber specialists at the Captain of the Port level to advise MTS owners and operators on cybersecurity best practices and cyber protection teams from Coast Guard Cyber Command to provide direct technical assistance through assessment, threat hunting, and incident response." GAO, "Coast Guard: Additional Efforts Needed to Address Cybersecurity Risks to the Maritime Transportation System," February 2025, footnote 89.

80 The Coast Guard operates under DHS authorities except during wartime, when it operates as part of the Navy. See Alexander Hernandex and Liz Hutton, "The Status of the U.S. Coast Guard's People, Bases and Equipment, and Vessels Under LOAC," *Articles of* War, West Point's Lieber Institute for Law & Warfare, January 28, 2025, https://lieber.westpoint.edu/status-us-coast-guards-people-bases-equipment-vessels-loac/ .

81 "U.S. Coast Guard Cyber Protection Team (CPT)," https://www.uscg.mil/Portals/0/CPT%20One%20Pager.pdf.

82 Mark Pomerleau, "Cybercom's Defensive Arm Elevated to Sub-unified Command," *DefenseScoop*, May 30, 2025, https://defensescoop.com/2025/05/30/cybercom-jfhq-dodin-dcdc-designated-sub-unified-command/.

83 DOD, *Defense Industrial Base Cybersecurity Strategy 2024*, March 21, 2024, https://media.defense.gov/2024/Mar/28/2003424523/-1/-1/1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF.

84 Hearings Before Senate Comm. on Armed Services' Subcomm. on Cybersecurity, 119th Cong. (2025) (posture statement of William J. Hartman, US Cyber Command), https://www.armed-services.senate.gov/imo/media/doc/united_states_cyber_command_posture_statement_ltg_william_jhartman.pdf.

85 "Defense Primer: Defense Support of Civil Authorities," Congressional Research Service, January 3, 2023, https://www.congress.gov/crs_external_products/IF/PDF/IF11324/IF11324.13.pdf. For a useful discussion of DSCA authorities, see Jason Healey and Erik B. Korn, "Defense Support to the Private Sector: New Concepts for the DoD's National Cyber Defense Mission," *Cyber Defense Review*, Special Edition 2019, https://cyberdefensereview.army.mil/Portals/6/Session%205%20Number%201%20CDR-Special%20Edition-2019.pdf.

86 Cf., Jon Harper, "Air Force Cyber Leader Warns Threats Like Volt Typhoon Could Enable China to Wage 'Total War' Against US," *CyberScoop*, September 23, 2025 (describing various Air Force cooperative research and development agreements (CRADAs) with public utility companies, including as follows: "There are some CRADAs where, you know, we can get an agreement where we can put our sensors on their system, and we can do the persistent monitoring. That [last] one gets a little bit trickier, because you have Department of Homeland Security responsibilities and authorities—but the great thing is, if we got some [National] Guard folks that are out there, the Guard has authorities to be able to do that kind of work, and so they are key in that nexus point there.")

87 The Department of Homeland Security annually identifies and maintains a list of critical infrastructure entities that meet the criteria specified in Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, Section 9(a)('Section 9 entities'). Section 9 entities are defined as «critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.» https://www.cisa.gov/resources-tools/resources/support-critical-infrastructure-greatest-risk-section-9-report-summary.

88 A broad spectrum of activity may qualify as an offensive cyber operation. For useful discussions of this topic, see Kim Zetter, "What It Means That the U.S. Is Conducting Offensive Cyber Operations against Russia," *Zero Day Newsletter*, June 17, 2022, https://www.zetter-zeroday.com/what-it-means-that-the-us-is-conducting/; and Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," *National Academy of Science, Proceedings of a Workshop on Deterring Cyberattacks*, 82–83, https://nap.nationalacademies.org/download/12997. Formal definitions of offensive cyberspace operations vary (*cf.* https://csrc.nist.gov/glossary/term/offensive_cyberspace_operations and https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/), but generally speaking, the term offensive cyber operations is used broadly to encompass operations to manipulate, deny access to, disrupt, degrade or destroy targeted computers, information systems, or networks. See e.g., Stacy H. O'Mara, "To Hack Back, Or Not Hack Back? That Is the Question . . . Or Is It?," Center for Cybersecurity Policy and Law, May 2025; ("Offensive cyber operations are generally understood to involve actions that sabotage, deny access, or otherwise degrade or disrupt adversary systems"). And see "Defining Offensive Cyber Capabilities," Australian Strategic Policy Institute, July 4, 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities/; (defining state-sponsored offensive cyber operations as "operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks").

89 US House of Representatives, "Executive Summary of Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden," September 15, 2016, https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_-_unclass_summary_-_final.pdf. See also https://intelligence.house.gov/uploadedfiles/hpsci_snowden_review_declassified.pdf.

90 Julian E. Barnes and Adam Entous, "How the US Adopted a New Intelligence Playbook to Expose Russia's War Plans," *New York Times*, February 23, 2023, https://www.nytimes.com/2023/02/23/us/politics/intelligence-russia-us-ukraine-china.html?smid=nytcore-ios-share&referringSource=articleShare.

91 Jim Mattis Quotes, Brainy Quote, https://www.brainyquote.com/quotes/jim_mattis_788513.

92 *Great-Power Offensive Cyber Campaigns: Experiments in Strategy*, International Institute for Strategic Studies, https://www.iiss.org/research-paper/2022/02/great-power-offensive-cyber-campaigns/.

93 In addition to Volt and Salt Typhoon, described earlier, other PRC activities include Silk Typhoon (supply chain), (Microsoft Threat Intelligence, "Silk Typhoon Targeting IT Supply Chain," March 5, 2025, https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/), Nylon Typhoon (remote access services and appliances) (Microsoft Security, "Nation State Actor Nylon Typhoon," January 25, 2024, https://www.microsoft.com/en-us/security/security-insider/nylon-typhoon), and Violet and Linen Typhoon (cyberespionage campaign exploiting Microsoft SharePoint server software vulnerability) (Microsoft Threat Intelligence, "Disrupting Active Exploitation of On-Premises SharePoint Vulnerabilities," *Microsoft* Security, July 22, 2025, https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/).

94 For an overview of these discussions, see O'Mara, "To Hack Back, Or Not Hack Back?," 3–4.

95 Frank Cilluffo, host, *Cyber Focus*, podcast, season 2, episode 14, "Rethinking Offensive Cyber: Strategy, Deterrence, and Real-World Impact with Adm. Mike Rogers (Ret.)," April 15, 2025, https://podcasts.apple.com/us/podcast/rethinking-offensive-cyber-strategy-deterrence-and/id1727584821?i=1000703637952&l=pt-BR.

96 The Cyber Initiatives Group Newsletter, July 20, 2025 (on file with one of the authors).

97 Piotr Malachinski and Marine Pichon, "The Hidden Network," *Orange Cyberdefense Blog*, November 24, 2024, https://www.orangecyberdefense.com/global/blog/cert-news/the-hidden-network-how-china-unites-state-corporate-and-academic-assets-for-cyber-offensive-campaigns.

98 "Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections," *New York Times*, February 26, 2019, https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html.

99 US House Subcomm. on Cybersecurity and Infrastructure Protection, 118th Cong. (2024) (statement of Frank J. Cilluffo, McCrary Institute for Cyber and Critical Infrastructure Security, University of Auburn), https://homeland.house.gov/hearing/sector-down-ensuring-critical-infrastructure-resilience/; and Cilluffo, host, *Cyber Focus*, season 1, episode 24, "Treasury's Cyber Defenses and AI Future with Todd Conklin," June 12, 2024 , https://mccraryinstitute.com/podcast/cyber-focus/33/treasuryx27s-cyber-defenses-and-ai-/.

100 Department of the Treasury, "Project Fortress–2025 Offerings," https://home.treasury.gov/system/files/216/Project-Fortress-Brochure.pdf.

101 Matt Egan, "Treasury Launches 'Project Fortress,' An Alliance with Banks Against Hackers," *CNN*, May 9, 2024, https://www.cnn.com/2024/05/09/business/treasury-launches-project-fortress?cid=ios_app. (According to then-Deputy Treasury Secretary Wally Adeyemo, Project Fortress includes "offensive actions" that employ Treasury's national security tools as well as US law enforcement to "make clear to our adversaries that they will face consequences for their attacks.")

102 U.S. Treasury Office of Cybersecurity and Critical Infrastructure Protection, "Project Fortress," https://home.treasury.gov/system/files/311/Project%20Fortress%20-%20Cloud%20FACI%20Presentation%20-%20Sept%202024.pdf

103 Center for Internet Security, "Why Warning and Analysis Matter in an Evolving and Complex Threat Landscape," *ThreatWA*, https://www.cisecurity.org/threatwa

104 ODNI Cyber Threat Intelligence Integration Center, "Worldwide Ransomware, 2024: Increasing Rate of Attacks Tempered by Law Enforcement Disruptions," https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf.

105 See e.g., U.S. Attorney's Office, District of New Jersey Press Release, "Dual Russian and Israeli National Extradited to The United States for His Role in the LockBit Ransomware Conspiracy," March 13, 2025,https://www.justice.gov/usao-nj/pr/dual-russian-and-israeli-national-extradited-united-states-his-role-lockbit-ransomware (announcing the March 2025 extradition of Rostislav Panev, the alleged developer of the LockBit ransomware group); and https://www.justice.gov/opa/pr/phobos-ransomware-affiliates-arrested-coordinated-international-disruption (announcing criminal charges against Roman Berezhnoy and Egor Nikolaevich Glebov, two Russian nationals alleged to have operated a cybercrime group using the "Phobos" ransomware).

106 E.g., Gyana Swain, "Feds and Microsoft Crush Lumma Stealer That Stole Millions of Passwords," *CSOonline*, May 22, 2025, https://www.csoonline.com/article/3993289/feds-and-microsoft-crush-lumma-stealer-that-stole-millions-of-passwords.html (describing how Microsoft and DoJ dismantled Lumma, one of the world's largest cybercrime operations that provided malware-as-a-service for cybercriminals including ransomware operators); see also https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/ and https://www.justice.gov/usao-nj/pr/us-and-uk-disrupt-lockbit-ransomware-variant (announcing the February 2024 disruption of the LockBit ransomware-as-a-service operation, which was responsible for somewhere between 25% and 33% of all ransomware attacks in 2023).

107 For example, in 2023, DOJ "obtained the final forfeiture of millions of dollars' worth of ransom payments obtained through two . . . civil forfeiture cases, which included 39.89138522 Bitcoin and $6.1 million in US dollar funds traceable to alleged ransom payments received by . . . members of the [REvil ransomware group]." DoJ Press Release, "Sodinokibi/REvil Affiliate Sentenced for Role in $700M Ransomware Scheme," May 1, 2024, https://www.justice.gov/archives/opa/pr/sodinokibirevil-affiliate-sentenced-role-700m-ransomware-scheme.

108 Steve Alder, "Cybersecurity Firms Report Record-Breaking Quarter for Ransomware Attacks," *The HIPAA Journal*, April 10, 2025, https://www.hipaajournal.com/q1-2025-ransomware-report/; "The Uber of the Underworld," *The Economist*, May 29, 2025, https://www.economist.com/international/2025/05/29/the-uber-of-the-underworld.

109 "Bulletproof Hosting: A Critical Cybercriminal Service," *Intel 471 Blog*, January 22, 2024, https://intel471.com/blog/bulletproof-hosting-a-critical-cybercriminal-service ("Targeting and blocking BPH providers can be one of the most effective defense mechanisms from a cost-benefit perspective that can often halt malicious activity early in the kill chain.")

110 DoJ, "Two Individuals Sentenced for Providing 'Bulletproof Hosting' for Cybercriminals," Press Release, October 20, 2021, https://www.justice.gov/archives/opa/pr/two-individuals-sentenced-providing-bulletproof-hosting-cybercriminals (describing bulletproof hosting organization that "rented IP addresses, servers and domains to cybercriminal clients who employed this technical infrastructure to disseminate malware use to gain access to victims' computers, form botnets, and steal banking credentials for use in frauds.")

111 DoJ, "Two Individuals Sentenced for Providing 'Bulletproof Hosting' for Cybercriminals," Press Release, October 20, 2021, https://www.justice.gov/archives/opa/pr/two-individuals-sentenced-providing-bulletproof-hosting-cybercriminals.

112 Joe Warminsky, "Dutch Police Say They Took Down 127 Servers Used by Sanctioned Hosting Services," *Record*, February 13, 2025, https://therecord.media/dutch-police-take-down-127-servers-sanctioned-host (describing Dutch police takedown of 127 servers used by Zservers, a Russia-based BPH company); and a Netherlands Police statement, https://www.politie.nl/nieuws/2025/februari/13/politie-amsterdam-ontmantelt-digitaal-crimineel-netwerk-127-servers-offline-gehaald.html.

113 CISA Cybersecurity Advisory, "Fast Flux: A National Security Threat," April 3, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-093a ("Fast flux" rapidly changes Domain Name Server records to hide the location of malicious servers).

114 Kevin Poireault, "Why Bulletproof Hosting Is Key to Cybercrime-as-a-Service," *InfoSecurity Magazine*, n.d., https://www.infosecurity-magazine.com/news/why-bulletproof-hosting-key-caas/.

115 Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015), https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf. Notably, the status of CISA 2015 is in flux as of the writing of this report, with the statute having expired on September 30, 2025.

116 Zack Whittaker, "Google Took a Month to Shut Down Catwatchful, A Phone Spyware Operation Hosted on Its Servers," *TechCrunch*, July 25, 2025, https://techcrunch.com/2025/07/25/google-took-a-month-to-shut-down-catwatchful-a-phone-spyware-operation-hosted-on-its-servers/

117 Google Cloud Acceptable Use Policy, *Google Cloud*, https://cloud.google.com/terms/aup?hl=en

118 Blocking BulletProof hosting services by IP Address
- Identifying malicious IPs:
  - Threat intel services: Defenders often use threat intelligence services and databases to identify IP addresses associated with malicious activities, including those used by BulletProof Hosting providers.
  - IP reputation lists: Many organizations maintain and share lists of IP addresses owned by a BulletProof Hosting service, hosting malicious content, or other nefarious activities. These lists can be used to update firewall and network security rules.
- Implementing blocks: Once identified, these IP addresses or entire blocks can be blocked at the network perimeter, preventing connections to and from these known bad actors.

119 Air Force, "Civil Reserve Air Fleet," July 2014, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104583/civil-reserve-air-fleet/.

120 Steve P. Mulligan, "Letters of Marque and Reprisal (Part 1): Introduction and Historical Context," Congressional Research Service, February 26, 2025, https://www.congress.gov/crs-product/LSB11272.

121 Principle #8 of the Paris 2018 Paris Call for Trust and Security in Cyberspace reads: "No private hack back: take steps to prevent non-state actors, including the private sector, from hacking back, for their own purposes or those of other non-state actors"). While the United States did not initially sign onto the Paris Call, it has since expressed its support for the Paris Call, and leading US companies—including Microsoft, Google, Facebook and Intel—have signed on. See https://pariscall.international/en/; https://blogs.microsoft.com/on-the-issues/2019/11/12/paris-call-consensus-cyberspace/.

122 The proposed National Cyber Cohort—FFRDCs and UARCs—might also provide capabilities.

123 Private cybersecurity firm Resecurity recently exploited a flaw to collect intelligence on BlackLock ransomware operators; see https://www.resecurity.com/blog/article/blacklock-ransomware-a-late-holiday-gift-with-intrusion-into-the-threat-actors-infrastructure.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org