SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 5: Evaluating U.S. Cyber Strategy

Emily Harding Aosheng Pusztaszeri Julia Dickson

A Report of the CSIS Intelligence, National Security, and Technology Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 5: Evaluating U.S. Cyber Strategy

AUTHORS
Emily Harding
Aosheng Pusztaszeri
Julia Dickson

A Report of the Intelligence, National Security, and Technology Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

The authors would like to extend their gratitude to those who graciously agreed to be interviewed. The authors would also like to thank Rex Booth and George Corbari for providing valuable feedback, Susan Hines for helping with the project contract, and the CSIS iDeas Lab for offering their design expertise.

This report is made possible by project support from the Smith Richardson Foundation.

Contents

Authors' Note About the Series

Photo: Zack Frank/Adobe Stock

This report is part of a series on the future of cyber warfare. This part of the series examines how the United States fights in the cyber domain, including the core elements of Washington's strategy for conducting cyber operations, how that strategy fits in a larger foreign policy context, and who the frontline fighters are in this new mode of conflict.

Part 1 of this series offers a broad introduction to the report, covers key takeaways from the comparative studies and wargames, and summarizes the authors' recommendations. Parts 2, 3, and 4 examine how Russia, China, and Iran, respectively, fight in the cyber domain, and this part (Part 5) examines U.S. cyber practices. Part 6 tests how U.S. policymakers view cyber operations as part of the spectrum of war, peace, and irregular warfare, illuminated by a set of wargames. Finally, Part 7 fully explains the new playbook that will close the gap between how the United States and its adversaries fight and succeed in the cyber domain.

Overview of the United States' Cyber Playbook

The United States is generally accepted as among the most effective offensive cyber actors on the planet, but it is also self-restrained.[1] This reputation for effectiveness is built upon its extensive cyber infrastructure, strategic approach to cyber operations, and use of advanced technologies.[2] Intelligence services and U.S. Cyber Command (USCYBERCOM) have considerable capabilities and a growing authority to conduct operations against adversaries abroad. Further, U.S. tools and precision are unmatched, and strong alliances and partnerships serve as force multipliers.

This offensive skill, however, is counterbalanced by a huge attack surface and weak domestic defense. The United States has a scattered patchwork of protections, attempting to cover a broad attack surface in a hyperconnected society. It has largely left cyber defense up to private entities, asking businesses—from multinational corporations to corner stores—to navigate a dizzying array of software packages, cyber vendors, and guidelines for effective defense. When something goes wrong, the Federal Bureau of Investigation (FBI) can investigate limited cases, but very little can be done to punish bad actors overseas. This defensive picture is a Maginot line for cyber: perhaps it feels secure in places, but adversaries can easily work around existing defenses to find weak spots and take advantage of gaping holes in the cyber defenses of domestic critical infrastructure.

The sum of these characteristics—a strong offense, a strong legal and moral constraint on the offense, and a weak defense—results in hesitation to use the tools available and a reluctance to retaliate against attackers. U.S. policymakers have unconsciously created a default policy of categorizing cyberattacks on the U.S. homeland as crimes or natural disasters. The response is

to recover, rebuild, and call for better resilience, but rarely does anyone in authority call such an attack hostile or retaliate aggressively enough to deter future attacks.

The dichotomy between a strong offense and a weak defense stems from the clear, bright line between foreign-facing services, such as the Central Intelligence Agency (CIA), the National Security Agency (NSA), and USCYBERCOM, and domestic-facing services, such as the Department of Homeland Security (DHS), Department of Energy (DOE), and myriad state and local entities. A core tenet of the U.S. government has been to project strength abroad but defer to free enterprise and personal freedoms at home. As a result, the Department of Defense (DOD) may be equipped for cyber combat, while a local water treatment plant may not.

In the domestic space, the U.S. government largely defers to the private sector to manage its own affairs. Just as a private organization is responsible for hiring security guards for deterrence and day-to-day security, so too is it responsible for managing security in the cyber domain. A robust set of private sector entities, such as Palo Alto Networks, CrowdStrike, and Mandiant, have sprung up to provide this service for those who can afford it. But many cannot—particularly small utility companies responsible for critical infrastructure.

In the cyber domain, there is no equivalent to the defensive and deterrent function of DOD in conventional armed conflict. FBI functions as a cyber police force of sorts: it will investigate select crimes after they take place. That is hardly a deterrent, however, to cyber actors who are overseas and are highly unlikely to be prosecuted. Private entities that bought insurance can lean on that funding stream, but those that did not must pick up the pieces, find help with remediation where they can, and carry on. For individual victims whose data is stolen and lives are disrupted, there is no recovery. Like private entities, government entities face the same challenges. The Cybersecurity and Infrastructure Security Agency (CISA) can help, often collaborating with the U.S. Federal Emergency Management Agency (FEMA) to distribute cybersecurity grant programs.[3] But throughout this response, the missing piece is an acknowledgement that cyber actors are not criminals or natural disasters but hostile foreign powers and that the attacks are a conscious part of an adversary's foreign policy strategy.

Adversaries continue to exploit weak spots. In 2023, for instance, a state-sponsored actor based in China, Volt Typhoon—also known as Vanguard Panda—penetrated telecommunications, energy, water, and other sectors, once again proving the vulnerability of U.S. domestic infrastructure.[4] Meanwhile, China, Iran, and Russia have worked to isolate their domestic internet from the world's influence—not an option for a liberal democracy that believes in open societies and free speech. The United States could stand to learn quite a bit from Ukraine, which has proved that investing in resilience is worthwhile. Russia has repeatedly targeted Ukraine's power grid, banking sector, and communications infrastructure but has had limited success thanks in large part to Ukraine's effective and active defense built over the last decade.[5]

Improving defense and offense are key components of a larger overall goal: creating a coherent strategy that seamlessly integrates cyber into foreign policy so that policymakers are not scared to use it. To transform today's hesitant stance into a robust policy tool kit, the United States must

establish a framework for thinking about cyber's role. It must decide how cyber activity fits in with larger foreign policy actions, including deterrence, proportional response, and international norms. U.S. government responses have been slow and limited and have not challenged the adversary's risk calculus. For example, in response to an attack on U.S. Department of State networks that led to the extraction of terabytes of information, CSIS's James Andrew Lewis wrote in 2009, "If Chinese or Russian spies had backed a truck up to the State Department, smashed the glass doors, tied up the guards and spent the night carting off file cabinets, it would constitute an act of war. But when it happens in cyberspace, we barely notice."[6] In 2023—14 years later—actors affiliated with Iran's Islamic Revolutionary Guard Corps (IRGC) attacked U.S. water treatment facilities. The U.S. Department of the Treasury later announced sanctions on the already heavily sanctioned IRGC—an important gesture, but one that lacked practical impact.[7] Decades of this type of approach have led to the total absence of deterrence in the cyber domain. Given this pattern of behavior, an outside actor would have to assume that the United States has few real red lines in cyberspace.

Improving defense and offense are key components of a larger overall goal: creating a coherent strategy that seamlessly integrates cyber into foreign policy so that policymakers are not scared to use it.

Recent administrations have made clear that they reserve the right to use all elements of state power to respond to operations in the cyber domain. But it remains unclear how that power should be meted out and in response to what.[8] For example, there is mixed or inadequate guidance on interpreting attacks on economic systems or systems tangential to national defense. It is also a constantly shifting domain. The International Institute for Strategic Studies (IISS) stated in a 2021 U.S. cyber power report, "The speed at which the cyber threat has continued to evolve has proven highly disruptive even to a policy process as advanced as that of the US."[9] At the same time, U.S. government leaders have publicly stated self-imposed restrictions on responses, indicating that these responses will be proportional. For example, U.S. policy is not to use force to respond to a cyber operation that is not an act of force. Instead, the United States can respond with measures such as "a diplomatic protest, an economic embargo, or other acts of retorsion."[10] This stated policy implies a narrow path to walk: policymakers could respond to a cyberattack with diplomatic, cyber, economic, military, or informational tools, but they also seek to maintain proportionality and deescalate most situations.

Crafting a policy through this wilderness of uncertainty, rules, and morals is challenging. For this project, researchers conducted a set of wargames to test how U.S. policymakers would react to severe cyberattacks at varying levels of catastrophe. The findings of the wargames are spelled out in Part 6: Testing U.S. Policy Responses to Destructive Cyberattacks with Wargames, but there were two clear findings. First, policymakers had no intellectual framework to draw upon in responding

to a cyberattack. They did not know whether to view cyberattacks as an act of war or as another natural disaster. Second, they could not decide how much evidence was enough to respond, and they debated vociferously about what constituted a proportional response. In the final accounting, the combination of a strong offense and a weak defense means that the U.S. government is easily self-deterred from decisive action in the cyber domain. That confusion and self-deterrence must end if the United States has any hope of competing effectively in modern warfare.

Recent administrations have made clear that they reserve the right to use all elements of state power to respond to operations in the cyber domain. But it remains unclear how that power should be meted out and in response to what.

Core Elements of U.S. Cyber Strategy

The goal of U.S. cyber strategy is twofold. First, government policy must allow industry to be simultaneously unhampered by requirements and also, somehow, secure. Second, on the offensive side, cyber tools should support espionage and warfighting efforts. The United States' de facto strategy is unlikely to achieve the first goal and is overqualified to execute the second. After-the-fact patchwork defense, crafted largely by market forces and cajoling, is not strong enough to create resilience. The United States has a strong offense sitting on the bench, but policymakers need to figure out how to use it.

The current state of U.S. activities in the cyber domain, which make up this strategy, may be roughly divided into three main functions: espionage, offense, and defense.

- **Espionage:** The United States has long used computer network operations to collect information on other governments.[11] Most examples are classified. This report treats espionage as a separate category from offense or defense, as do many scholarly studies. Espionage often bridges offense and defense, as the tools and intent of espionage may be directed at either. Further, the goal of espionage is never to disrupt or destroy but rather to sit quietly and collect.[12]
- **Offense:** Washington has had notable successes in cyber offense, such as the 2018 disruption of the Russian troll farm responsible for election interference. A complex web of legal and policy restrictions governs those operations.
- **Defense:** The United States lags its near-peer competitors in cyber defense, largely because it has a free and open society and a mindset that individual entities are responsible for

protecting themselves. This approach leads to a decentralized system with significant gaps. For example, the U.S. defense industrial base is a point of intersection between the private sector and government, but cyber defense has been lacking here as well.[13]

This section addresses each of these categories, describing how the interaction of these activities creates a de facto U.S. cyber strategy. The section on espionage is intentionally limited, given the generally classified nature of such activities and the fact that leveraging cyber capabilities to support espionage is, by and large, uncontroversial and falls neatly into long-established norms regarding espionage writ large. The focus here is instead on cyber offense and defense.

Espionage

In the international space, the national security apparatus is largely free to use the cyber domain to conduct espionage, although it is somewhat hampered by questions over what elements of cyberspace are truly foreign and which are too likely to touch U.S. persons, mandating different rules. Espionage is self-limited by U.S. rules about government action vis-à-vis private entities and a prohibition on spying for economic gain. A web of laws and orders governs U.S. government actions, including the Foreign Intelligence Surveillance Act, executive orders, presidential policy directives, national security directives, and laws under Titles 10 and 50.

The cyber domain is well suited to the United States' preferred style of espionage activity. Discreet, illuminating, and persistent surveillance is possible if a service is committed, diligent, patient, and careful. Cyber espionage has also proved remarkably nonescalatory, even by intelligence standards: When a victim detects penetration, attributing that penetration is difficult. Further, physical damage is usually limited, making espionage in the cyber domain among the least escalatory forms of intelligence work.

The cyber domain is well suited to the United States' preferred style of espionage activity. Discreet, illuminating, and persistent surveillance is possible if a service is committed, diligent, patient, and careful.

Cyber operations are far more potent when combined with other strong intelligence disciplines. The collaboration between human intelligence, other forms of signals intelligence, and computer network operations makes U.S. operations stronger than the sum of their parts. Cyber espionage can be designed to gather information against a specific intelligence target, such as leadership decisionmaking, or on a tactical level to support the planning and execution of later cyberspace operations. Cyber espionage tends to yield extensive fruit: the scale and efficiency of acquisitions are so great that they can outpace the U.S. government's ability to consume them. Examples of successful cyber espionage are largely classified.[14]

Offense: Power and Restraint

"We will impose costs on you until you get the point."

—John Bolton, referring to nations targeted by U.S. digital operations[15]

In 2019, U.S. National Security Advisor John Bolton described a new, more aggressive approach to cyber offense, partly in response to Russian attempts to interfere in the 2016 and 2018 elections. In this watershed moment, the defense establishment adopted General Paul M. Nakasone's persistent engagement strategy. Theory and practice in offensive cyber are squarely settled within DOD, both in USCYBERCOM and the services' cyber units, with coordination and guidance from the National Security Council (NSC). It was a change in authorities and bureaucracy that acknowledged increasing comfort with pushing the boundaries of the cyber domain. It also allowed a more offensive mindset at USCYBERCOM. Even with these relatively revolutionary changes in its approach to offensive cyber, however, USCYBERCOM has remained a talented but rule-bound bureaucracy plagued by policymaker uncertainty and hamstrung with self-deterrence.

HOW THE UNITED STATES USES OFFENSIVE CYBER OPERATIONS

The United States has used cyber tools for hypertargeted strikes to accomplish specific, narrow goals:

- In Operation Glowing Symphony, policymakers used cyber activities as part of a larger kinetic campaign. The United States employed both conventional means to target fighters of the Islamic State of Iraq and Syria (ISIS) and cyber tools to disrupt ISIS's ability to recruit and communicate.[16] (For more, see Case Study: Operation Glowing Symphony on page 35.)
- Washington has used cyber to disrupt information operations, as with the Russian Internet Research Agency (IRA). In that case, USCYBERCOM used degrading actions to remove tools that the IRA might have tried to use to disrupt the U.S. elections in 2018.[17]
- The *New York Times* reported in 2017 about alleged use of cyber tools to disrupt the North Korean nuclear program, causing missiles to spin off course.[18]
- The *Washington Post* reported in 2019 about a U.S. cyber strike against IRGC computer systems used to plot attacks on tankers in the Persian Gulf. Tom Bossert, a former official, said, "This operation imposes costs on the growing Iranian cyberthreat, but also serves to defend the United States Navy and shipping operations in the Strait of Hormuz."[19]

In each case, there were no human casualties and little to no property damage, limiting the risk of escalation.

Each of these operational effects was deemed worth losing any associated intelligence collection. Deciding to exploit a vulnerability to cause a noticeable disruption, rather than preserve access for persistent spying, is a policy judgment call. Given the overlap between creating access for intelligence purposes and doing so for offensive action, one consideration is always whether securing the operational gain is worth burning the access. For example, following Russia's interference in the 2016 election, one factor that restrained the administration of U.S. President

Barack Obama from retaliating against Russia in the cyber domain was a concern that, as the *New York Times* put it, the Pentagon might "expose some of its best weaponry."[20]

A TURNING POINT IN STRATEGY: THE 2018 DEVOLUTION

In the early days of operating in the cyber domain, decisions about cyber operations were made only at the very top of the U.S. policymaking establishment. Often the president was the one making decisions regarding the trade-off between intelligence collection and burning access for an operation. But as cyber capabilities have matured and policymakers have achieved a greater degree of familiarity and comfort with the cyber domain, the U.S. policymaking establishment has devolved the authority to conduct cyber operations.

Policymakers see activity in the domain as generally low risk and unlikely to escalate. Thus, in recent years, presidents have agreed to delegate the authority for conducting an operation to the commander of USCYBERCOM. In 2018, President Donald Trump signed National Security Presidential Memorandum-13 (NSPM-13), a directive that devolved considerable authority to the secretary of defense, who then delegated some authority to USCYBERCOM. It further provided blanket authorization to a set of objectives that the secretary of defense and commander of USCYBERCOM could pursue without further approvals from the president or any other cabinet secretary. This marked a departure from the 2012 Obama-era policy requiring offensive cyber operations (OCOs) to have presidential and relevant agency approval.[21] Also in 2018, Congress passed legislation in the fiscal year (FY) 2019 National Defense Authorization Act (NDAA), approving routine conduct of "clandestine military activity" in cyberspace to "deter, safeguard or defend against attacks or malicious cyberactivities against the United States."[22] The new law equated cyber activities to routine, traditional military activity in other domains that does not require high-level approval.[23] (For more, see the subsection on USCYBERCOM.)

This devolution has allowed for a far more agile stance, better integrating proactive operations with reactive retaliation and cleanup. In 2019, General Nakasone, then commander of USCYBERCOM, said that USCYBERCOM has evolved its cyber strategy, transitioning from a primarily reactive "response force" to a more proactive "persistence force."[24] This proactive approach aims to actively disrupt adversary cyber activities by targeting enemy cyber infrastructure and resources. General Nakasone also stated that the cornerstone of this approach is to establish a cyber force that maintains persistence, defends forward, and takes action against U.S. adversaries "on their virtual territory."[25]

Implementation: Campaigns or Opportunism?

In each part of this series, researchers attempted to answer the question of whether an actor is largely opportunistic or whether it pursues campaigns—a set of actions designed to achieve a certain end. The United States' cautious approach means that it is far more of a deliberate, intentional campaigner than an opportunist, but there is a certain element of opportunism in every cyber campaign. Retired U.S. Army Colonel George Corbari described the U.S. approach as "taking advantage of the opportunistic elements of cyberspace."[26]

The United States might undertake a campaign in which the goal is to preempt cyberattacks by rapidly pulling down a hostile power's network infrastructure based in a third party. That campaign would involve patiently constructing a concept, mapping those networks, and likely getting approval from that third party, but no further progress is possible until an opportunity presents itself. Such an opportunity might be a new hire with lax security practices, a newly discovered zero-day exploit, or an incorrectly performed reconfiguration of the network. An actor must be pre-positioned to exploit those opportunities and may do so as part of a campaign. For example, the Stuxnet attack was rumored to require four zero-day exploits—in cyber terms, a windfall of opportunities that cost dearly to burn. Devolution of cyber authorities to the commander of USCYBERCOM greatly increased the flexibility of those forces and made capitalizing on quick opportunities far more possible.

Box 1: The Strength in Alliances

A large factor contributing to U.S. strength in the cyber domain—both in espionage and in offense—is the power of alliances. Information and communications technology (ICT) infrastructure is global, as is talent. The ability to draw on the capabilities of NATO, allies in the Pacific, or Five Eyes partners is a force multiplier for USCYBERCOM and the U.S. intelligence community (IC).[27]

- Israel has repeatedly proved itself a cyber power that punches well above its weight, both in its government capability and in its robust private sector, whose talent has been trained and honed serving in the Israel Defense Forces.
- The United Kingdom and Australia participated in Operation Glowing Symphony to combat ISIS's use of the cyber domain.[28]
- In 2022, NATO served a defensive cyber role for Albania and Montenegro, helping them respond to cyberattacks by Iran and Russia, respectively.

Some scholarly work has been done on whether a country could invoke Article 5 of the North Atlantic Treaty for collective self-defense in the face of a cyberattack. In 2014, the Wales Summit Declaration stated that the North Atlantic Council would take decisions to invoke Article 5 on a case-by-case basis and report them to the UN Security Council.[29]

Defense: A Threadbare Patchwork

"Cyber governance in the US is highly pluralistic."[30]

—IISS, Cyber Capabilities and National Power

Characterizing cyber governance as "pluralistic" is a diplomatic way of saying it is decentralized or even chaotic. Defense in the United States is multilayered, but rather than overlap and create redundancies, the layers leave significant gaps. The United States has very little by way of an

overall defensive umbrella. DOD is responsible for securing its own networks (the Department of Defense Information Networks, or DODIN), and by necessity, that defense is fairly strong. By contrast, civilian non-Title 10, non-Title 50 agencies—from the Department of Commerce to the National Archives—are responsible for funding and executing their own cyber defense, and that defense is chronically underfunded. CISA provides select assistance as requested, but the capacity and capabilities of the civilian cybersecurity agency is not enough to cover defense for the entire U.S. government, let alone all of its stakeholders. The Office of the National Cyber Director (ONCD) manages cyber policy and works to coordinate efforts across the U.S. government, but it is not operational and, at the time of this writing, is still finding its footing among the cyber centers of gravity within the federal government—specifically NSC, CISA, NSA, and FBI.

At the state, local, tribal, and territorial (SLTT) level, the picture is far bleaker. States only recently began to realize that they are a target, thanks to the Russian attempts to interfere in the 2016 election and an ongoing epidemic of ransomware attacks. Only a handful of federal programs exist to assist SLTT governments, such as the State and Local Cybersecurity Grant Program and the Tribal Cybersecurity Grant Program, which CISA and FEMA jointly implement.[31] Still, tight budgets and disagreement about the nature and severity of the threat have prevented many states from investing properly in cyber defense, much less localities.

Critical infrastructure is where this gap is most stark. In much of the United States, local authorities or private entities run water, power, and some transportation. For example, in the water sector, there are approximately 50,000 water utilities, or an estimated 153,000 systems, 94 percent of which are run by local or private entities.[32] After Iran attacked several water facilities in 2023, the Associated Press reported that one oft-heard excuse was "it's difficult to invest in cybersecurity when upkeep of pipes and other water infrastructure is already underfunded."[33] The net effect is a deeply vulnerable set of critical infrastructure facilities.[34]

In late 2023, actors affiliated with the IRGC-Quds Force attacked a municipal water authority in Pennsylvania, along with others from across the country, because the water authority used software from Unitronics, an Israeli software firm. The attack compromised systems, displaying the image on the next page on the water authority's screens. The hackers disabled a water pressure monitor in at least one system, prompting the authority to switch to manual operation.[35] It was not a sophisticated attack; default passwords and lax security were enough.

Tools made available to critical infrastructure providers at the federal level are weak at best, and local authorities frequently oppose those that exist. For example, months before the Iranian attack, the U.S. Environmental Protection Agency (EPA), as the water regulatory authority, proposed a rule requiring states to audit the cybersecurity of water systems. Arkansas, Iowa, and Missouri sued, and the EPA withdrew the rule weeks before the Iranian attack. Anne Neuberger, former deputy national security advisor for cyber and emerging technology, told the Associated Press in late 2023 that the proposed required audits could have "identified vulnerabilities that were targeted in recent weeks."[36]

Screen of a Unitronics device in Pennsylvania hacked by Iranian actors.

Source: Associated Press, "Congressmen ask DOJ to Investigate Water Utility Hack, Warning It Could Happen Anywhere," SecurityWeek, December 1, 2023, https://www.securityweek.com/congressmen-ask-doj-to-investigate-water-utility-hack-warning-it-could-happen-anywhere/.

A handful of states have passed legislation requiring stronger oversight of utilities' cybersecurity, including New Jersey and Tennessee. California, Indiana, and Missouri also already have laws on the books. The Associated Press reported that several states have proposed but never enacted legislation, including Pennsylvania and Maryland, where "public water authorities fought bills backed by private water companies to force them to upgrade various aspects of their infrastructure," including cybersecurity.[37] Pennsylvania was one of the localities that publicly acknowledged Iranian hacking in 2023.

The U.S. system has largely viewed the prevention of, and recovery from, malevolence in the cyber domain akin to crime or a natural disaster. As when a natural disaster strikes the United States, the first response to a cyberattack, even an attack by a state-sponsored group on the U.S. homeland, tends to be mitigation and shoring up defense. When the Iran-affiliated hacking group attacked U.S. critical infrastructure, for instance, the immediate response focused on recovery, with the United States imposing sanctions days later. While it is expected—and essential—that everyone see security as their responsibility and engage in basic cyber hygiene, the limitations of this decentralized approach become apparent when the actor is a hostile foreign power or protected by one. In comparison to a well-resourced, motivated state actor, victims generally work with limited understanding of the problem set and even more limited resources; they have little clear guidance on what kind of security is "good enough." Further, as explained by Rex Booth,

chief information security officer (CISO) of Sailpoint and a former official at CISA and ONCD, entities with a disproportionate impact on societal functioning, such as water and energy, face a cultural gulf between their core business and cyber. Whereas their core business tends to be slow, methodical, and focused on operational technology, cyber is fast, reactionary, and on the forefront of information technology (IT).[38]

While it is expected—and essential—that everyone see security as their responsibility and engage in basic cyber hygiene, the limitations of this decentralized approach become apparent when the actor is a hostile foreign power or protected by one.

Many ransomware syndicates operate beyond the reach of U.S. law enforcement. According to the World Cybercrime Index, China, Russia, Ukraine, Romania, and Nigeria consistently appear in the top 10 countries for ransomware crime, along with the United States.[39] In 2021, 74 percent of all ransomware revenue went to Russia-affiliated hackers.[40] A state-backed attack, such as the one on Sony Pictures in 2014, is highly unlikely to result in arrests because the actors are typically smart enough to avoid extradition. Deterrence is nonexistent if the actors know that the United States will default to law enforcement entities who do not have jurisdiction to punish entities unbound by U.S. law.

How Cyber Strategy Fits into Foreign Policy

Given that espionage is strong, offense is capable but restrained, and defense is relatively weak, the sum total of the parts is a cautious approach. In the most acute cases, a fear of retaliation against weakly defended domestic critical infrastructure has stayed the hand of the U.S. president when in the cyber domain.

In other domains—air, sea, land, and space—the United States has escalation dominance, a largely predictable default to proportionality, and well-established deterrence theory, but none of these has been established in the cyber domain. U.S. policymakers tend to eschew escalation and prefer proportionality, but there is no established strategy to match noncyber responses to actions in the cyber domain. Questions remain: Are sanctions a proportional response to a cyberattack on critical infrastructure? Does an information campaign such as naming and shaming meet the same threshold of severity as putting a domestic population at physical risk? As yet, none of these steps has effectively established deterrence. (For more on proportional response, ethical considerations, and policy options generally, see Part 6: Testing U.S. Policy Responses to Destructive Cyberattacks with Wargames.)

Part of the proportionality challenge is the U.S. policy preference to protect the health and safety of civilian populations—a taboo that adversaries have frequently broken. For example, the United

States generally avoids harming infrastructure that will indiscriminately affect noncombatants, such as water pumping stations and hospitals. By contrast, Iran has hacked water facilities inside the United States several times, although so far producing no physical damage. Likewise, Russia has hacked Ukraine's power grid, throwing millions into darkness, and it has deliberately targeted civilian infrastructure across Ukraine with kinetic strikes as well.

In other domains—air, sea, land, and space—the United States has escalation dominance, a largely predictable default to proportionality, and well-established deterrence theory, but none of these has been established in the cyber domain.

However, the United States' restraint is a preference, not a prohibition. Media sources reported in 2018 that the United States had penetrated Russia's power grid in retaliation for Russian cyberattacks on the U.S. grid. White House officials and General Nakasone, then commander of USCYBERCOM, declined to comment but said that they had "no national security concerns" about a *New York Times* report on the targeting of the Russian grid, which the newspaper assessed was "perhaps an indication that some of the intrusions were intended to be noticed by the Russians."[41] As of this writing, the United States had not turned any of that access into action against the Russian grid.

Deterrence and Escalation in the Cyber Domain

The signals sent to adversaries about how the United States will—or more often will not—retaliate for cyberattacks have yet to establish a modicum of deterrence. U.S. foreign policy has rested in part on a theory of deterrence and a subtext of escalation dominance. Thanks to a robust defense establishment and political will to act, the U.S. government can create deterrence by punishment; it can bring to bear overwhelming force in retaliation for a hostile act, making that act far too costly. The United States has also established some deterrence by denial: air defenses, for example, can limit the damage caused by air strikes, whereas defensive measures at airports are meant to make would-be terrorists think twice about reattempting a 9/11-style attack.

But the cyber domain does not follow rules that lend themselves to deterrence. First, action in the cyber domain is far more deniable than a missile attack. The implant can take time to discover, and it may be carefully camouflaged, bearing no markers of the actor. That deniability prevents direct and fast retaliation.

Second, cyberattacks generally cause disruption or annoyance but, thankfully, have not resulted in a significant loss of life. As a result, an outcry for retaliation or retribution after a traditional cyberattack has yet to emerge. According to Erica D. Lonergan and Shawn W. Lonergan, cyber escalations rarely devolve into severe kinetic conflict, and they typically feature restrained, reciprocal responses below the threshold of armed conflict.[42] A 2019 study by Sarah Kreps and

Jacquelyn Schneider showed that most Americans are reluctant to support kinetic retaliation in response to a cyberattack, even when the cyberattack's impact mirrors that of traditional kinetic attacks (i.e., severe damage to critical infrastructure).[43] Nearly all theorized pathways to lethality through cyber activity are still indirect. For example, shutting down a power grid could lead to a lack of heat or air conditioning, which might cause death, or a cyberattack could cause an industrial system to malfunction, leading to exploding components, which might cause collateral damage. "Smart" medical devices might be the most direct route from cyber to death—for example, if a person's Bluetooth-enabled insulin delivery device or pacemaker were to be attacked.[44]

The 2017 NotPetya case further strengthens this assessment. Although NotPetya stands as one of the most destructive cyberattacks in history, affecting more than 60 countries and causing over $10 billion in damage globally, it notably did not lead to significant escalation.[45] Instead, the targeted nations, some of the most powerful in the cyber domain, collectively issued a joint statement officially condemning Russia for the attack.[46] As devastating as NotPetya was, it did not result in loss of life or a kinetic escalation.

It is tempting to settle into the assumption that cyber is a relatively safe domain and that deterrence against annoyance is unnecessary. In other words, the consequences are low, so why spend resources on deterring action? This project questions whether those assumptions and assessments are still valid. Cyberattacks have been escalating in sophistication and seriousness in recent years; further, adversaries such as Iran have shown a willingness to conduct brazen attacks. Some of those attacks—such as the bolder attacks on power grids or water plants—could risk human life in the U.S. homeland. Yet, retaliation for those attacks has not escalated as quickly. As discussed, no country has yet created deterrence in this unique domain. Further, there is a certain inertia in foreign policy: humans are slow to recognize sudden or significant change and adapt to it. In other words, slowly escalating aggression gradually expands tolerance to the aggression; it takes a shock to the system to shift out of a comfortable, albeit false, paradigm. The combination of these factors could mean an adversary, by intent or accident, will cause a high-casualty event, likely through an attack on critical infrastructure. U.S. policymakers must reckon with this potential before such an event occurs.

A 2020 Cyberspace Solarium Commission (CSC) report advocated for implementing a *layered cyber deterrence strategy*. The ultimate goal of this strategy was to diminish the likelihood and severity of cyberattacks by following three key pathways:

- The United States must *shape behavior* "to promote responsible behavior in cyberspace."
- The United States must *deny benefits* to adversaries who exploit U.S. and allied cyberspace.
- The United States must *impose costs* on adversaries by maintaining advanced cyber capabilities and capacity to retaliate against malicious actors.[47]

The CSC discussed applying deterrence-by-denial theory to cyberspace, largely by improving vulnerabilities at home and, in essence, denying adversaries easy targeting of U.S. systems.[48] Some professionals who operate in this domain emphasize that these are aspirational goals at best. Shaping the behavior of adversaries is exceedingly difficult in any domain, particularly one where deterrence is unproven. The benefits of action in the cyber domain are extensive, and

denying benefits would require far better cybersecurity than the United States has created thus far, necessitating perhaps a generational change.

The CSC also adopted the language from the 2018 DOD Cyber Strategy on "defending forward," which lays out an approach to "proactively observe, pursue, and counter adversaries' operations and impose costs short of armed conflict."[49] This approach was also intended to signal to adversaries the U.S. government's willingness to respond to cyberattacks.[50] Unfortunately, according to one interviewee, while the United States has extensive capabilities, "we just continue to not use them, nor do we take any meaningful actions to retaliate. When we do take action, it is late to need, short of need, and ineffective to the point that we actually continue to embolden adversaries."[51]

The 2018 attack on the IRA was effective at temporarily removing Russian mercenary leader Yevgeny Prigozhin's cyber soldiers from their keyboards, but no real consequences accrued to the Kremlin, which most likely, at least tacitly, approved the operations of the IRA. China has suffered few consequences for its repeated thefts of data and even for far more aggressive activity such as Volt Typhoon. The picture for U.S. allies is far worse: Albania, Montenegro, and Australia all suffered large-scale disruptive attacks by Iran, Russia, and China, respectively—but all were largely powerless to respond, and nearly all have been highly reluctant to "name and shame" the perpetrator. Albania alone stands out as willing to loudly and repeatedly blame Iran for their hack. Overall, however, the deterrence gap seems set to expand.

Is Critical Infrastructure a Real Red Line?

In a June 2021 speech aimed at Moscow, then-President Biden explicitly listed the 16 critical U.S. infrastructure sectors, declaring them "off limits to attack—period."[52] He said the two countries agreed to task their experts to "work on specific understandings about what's off limits." He called for "responsible countries" to "take action against criminals who conduct ransomware activities on their territory." He warned, should Russia "violate these basic norms," the United States would "respond with cyber." He did not specify what he would consider an appropriate target for that cyber activity.[53] Biden's team later clarified that he was referring to destructive attacks rather than espionage, but no one has said whether the attacker's intent matters, rather than just outcomes, or where financial loss fits in the severity spectrum.[54]

Biden laid out this apparent red line on the heels of the SolarWinds attack, in which Russian attackers used a sophisticated supply chain hack to compromise a host of entities across government and industry, and the Colonial Pipeline attack, in which ostensibly private Russian hackers disrupted gas delivery to the U.S. East Coast, likely unintentionally. While meant to be a strong, if toothless, warning to a committed adversary, clearly this policy construction leaves considerable room for ambiguity. Since then, Microsoft and NSA have announced that China compromised several elements of U.S. critical infrastructure in an operation called Volt Typhoon, and Iranian actors have targeted water facilities in Pennsylvania.[55] Still, U.S. responses have remained muted. One interviewee described this approach as "draw a red line, erase it and redefine it boldly, then do nothing when it is crossed."[56]

Constructing Strategy

Given the increasing interconnectedness of the United States, plus increasingly aggressive action by Russia, China, and Iran, more thinking needs to be done on how to address gaps in strategy. The United States has defensive gaps that must be closed, and with respect to offense, it must work out how to integrate cyber activity into the broader foreign policy tool kit. Much progress has been made in the last four years shoring up defenses, supporting the creation of tools, closing coordination gaps between U.S. agencies, and attempting to recruit cyber talent. But these efforts will need to carry forward into the current Trump administration and beyond—what one interviewee called a "generation of consistent approaches."[57] For recommendations on how to get from here to there, see Part 7: How the United States Can Win.

Organization of Capabilities

Derived from a legacy and national ethos of overthrowing an overbearing national government, the U.S. system is careful to create checks, balances, and limited power at the federal level. There is a clear line between foreign- and domestic-facing organizations, with the former quite strong but deeply constrained in how they operate inside the boundaries of the United States and having little to no law enforcement authority. Domestic-facing agencies are weak by design and deeply constrained in how they operate. For example, cooperation with DHS is largely voluntary, although the Biden administration made a clear strategic shift toward demanding a greater focus on security by private organizations. FBI straddles both worlds. It engages in domestic-facing law enforcement activity, such as investigating ransomware attacks, but it also plays a role in combating hostile foreign actors' attacks in the United States. Under its domestic law enforcement authorities, it must follow a strict set of rules on evidence, probable cause, and other procedures. Under its intelligence and counterintelligence authorities, it has a broader set of functions but is still greatly constrained.

DOD houses a wide breadth of cyber capabilities, including intelligence authorities and military authorities, while the IC, including NSA and CIA, contains narrower but exquisite capabilities.

Military Cyber Structure

In line with its 2023 cyber strategy, DOD engages in various cyber operations, encompassing OCOs, defensive cyber operations (DCOs), and operations that protect the DODIN.[58] DOD's national defense missions and cyber operations take primacy over the standing missions of other

departments or agencies when authorized by the commander of USCYBERCOM, the secretary of defense, or the president.[59]

U.S. CYBER COMMAND (USCYBERCOM)

The bulk of U.S. offensive capabilities lie with DOD's USCYBERCOM, a unified cyber command supported by the individual military services. USCYBERCOM's core mission areas are to secure and defend the DODIN, protect the nation against cyberattacks, and provide cyber support to combatant commanders.[60] USCYBERCOM's mission space has grown considerably. A turning point came in 2018 when it was elevated to a unified combatant command and President Trump implemented NSPM-13.[61]

USCYBERCOM's authority to conduct operations stems from multiple sources, including through NSPM-13 and provisions within the U.S. Code (Titles 10, 32, and 50) and the various NDAAs[62]:

- **Section 954** of the FY 2012 NDAA affirms that DOD "has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies, and interests, subject to the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and the War Powers Resolution."[63]
- **Section 1632** of the FY 2019 NDAA permits DOD to conduct cyberspace operations, including clandestine activities outside of hostile contexts, and categorizes these operations as traditional military activities.[64]
- **Section 1642** of the FY 2019 NDAA allows DOD "to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter" attacks on the U.S. government or its citizens.[65]

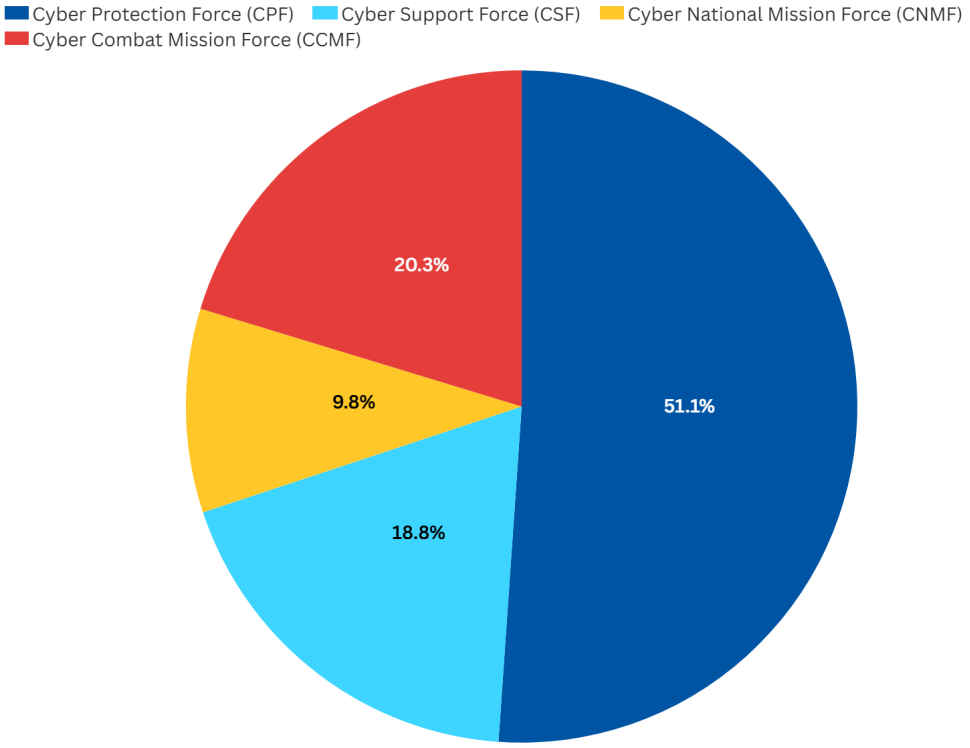
Furthermore, specific authorities for various military cyber operations are delineated within the secretary of defense's policies, which include "DOD instructions, directives, and memoranda," as well as execution orders and operations orders authorized by the president or secretary of defense and subordinate orders from approved commanders.[66] This includes the directive authority for cyberspace operations, established by the chairman of the Joint Chiefs of Staff, which plays a key role in facilitating DOD coordination for safeguarding the DODIN.[67]

The Cyber Mission Force (CMF) executes DOD's cyber operations.[68] As of 2023, CMF comprised 133 teams, consisting of 6,000 service members and 200 nonmilitary personnel, including National Guard and Reserve personnel on active duty.[69] The number of CMF teams is expected to increase to 147 by 2027.[70] The 133 CMF teams are organized into four specialized forces, each with its own area of focus (Figure 1).[71] In the event of a cyberattack on the United States, all four of these forces would be responsible for coordinating a cyber response.[72] Furthermore, these four groups answer to their respective subordinate command elements headquarters and combatant commands.[73]

1. **The Cyber National Mission Force (CNMF)** contributes 13 of the 133 teams within CMF. Its primary mission is to conduct cyber operations that protect the DODIN and the nation from malicious cyber threats.[74]

2. **The Cyber Combat Mission Force (CCMF)** contributes 27 of the 133 teams within CMF. Its primary mission is to conduct military cyber operations and to support the missions, plans, and priorities set by the various combatant commands, such as U.S. Africa Command, U.S. Indo-Pacific Command, and U.S. Strategic Command.[75]
3. **The Cyber Protection Force (CPF)** contributes 68 of the 133 teams within CMF. Its primary mission is to protect the DODIN and prepare cyber forces for combat, which it does through internal cyber operations that defend the DODIN or other blue cyberspace.[76] CPF includes national resources that report to the Joint Force Headquarters, teams that answer to combatant commands, and service teams that answer to each service's cyber command.[77]
4. **The Cyber Support Force (CSF)** contributes 25 of the 133 teams within the CMF. Its primary aim is to provide analytic and planning support to the CNMF and CCMF.[78]

Figure 1: Distribution of Teams in the Cyber Mission Force



Source: CSIS research.

SERVICE CYBER EFFORTS

Each service has its own cyber element whose mission is both offensive and defensive. These commands play a vital role in supporting their assigned combatant commands during cyber missions and can carry out OCOs as directed.[79] On the defensive side, they safeguard their respective segments of the DODIN through Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDMs) and DODIN operations.[80]

It is worth noting that each military service has a different approach and a different perspective for activities in the cyber domain, leading to an additional lack of coherence across DOD's cyber mission. USCYBERCOM is meant, in part, to address that.

Organization

These teams have a complex set of responsibilities. Operational control comes from their service command, but the commander of each unit functions both as the service representative to USCYBERCOM and as the commander for Joint Force Headquarters-Cyber (JFHQ-C).[81]

Further, these cyber elements support other combatant commands. The Army element, ARCYBER, supports U.S. Central Command, U.S. Africa Command, and U.S. Northern Command; the Navy's Tenth Fleet cyber element supports the U.S. Indo-Pacific Command, U.S. Southern Command, and U.S. Space Command; the Sixteenth Air Force supports U.S. European Command, U.S. Transportation Command, and U.S. Strategic Command; and the Marines' MARFORCYBER supports U.S. Special Operations Command. These service cyber commands provide personnel, training, and equipment to USCYBERCOM through the CMF.[82] While this arrangement allows a relatively small specialty to support a variety of missions, it is another example of the complex structures surrounding cyber that can lead to confusion.

The U.S. Coast Guard stands as an exception to this structure. Under the memorandum of agreement between DOD and DHS, the Coast Guard's commandant retains full control over its cyberspace forces and resources. However, USCYBERCOM and the U.S. Coast Guard Cyber Command frequently collaborate and conduct joint operations.[83]

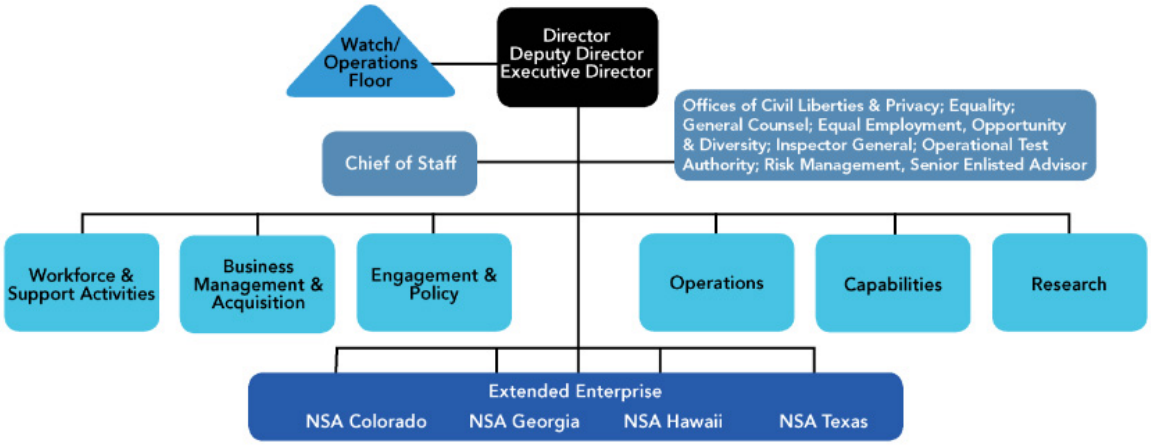
NATIONAL SECURITY AGENCY (NSA)

NSA is renowned as one of the world's preeminent computer network operations groups. Furthermore, the NSA Director (DIRNSA) also holds a dual-hatted role as the commander of USCYBERCOM. It is necessarily secretive about its approach, but operations revealed in the press have shown sophisticated capabilities and highly targeted operations.

In a rare revelation, NSA announced in 2019 that it was creating a new Cybersecurity Directorate "to better provide information gleaned from signals intelligence to agencies and the private sector in order to protect national critical infrastructure."[84] Further, according to an NSA spokesperson, this new Cybersecurity Directorate plans to combine NSA's "foreign intelligence and cyberdefense mission" and eradicate "threats to national security systems and the defense industrial base."[85] According to a CBS report, the new directorate also includes a Cybersecurity Collaboration Center, which is intended to "serve as a gathering point for government and private sector cybersecurity experts to exchange information about hacking threats from adversaries in real time."[86] The Cybersecurity Directorate's website will also serve as a publicly accessible repository on cybersecurity vulnerabilities. For instance, the directorate published open-source NSA research on the malware engineering tool Ghidra and has issued public alerts about the Windows vulnerability known as BlueKeep.[87]

Other details of NSA's organizational structure are closely guarded. The agency underwent a significant restructuring from 2016 to 2017, after contractor Edward Snowden released massive amounts of information about NSA operations. The reorganization, known as NSA 21, merged the Information Assurance Directorate with the SIGINT Collection Directorate to create a new Directorate of Operations (Figure 3). According to FedScoop, the rationale behind this merger was to improve coordination between NSA's hacking and patching capabilities and to "reduce costs [and] staffing levels."[88] Little else is public about the reorganization and its results.

Figure 2: Reorganization of NSA, 2016–2017



Source: "The New Design: Simple. Functional. Effective," NSA, n.d., https://www.nsa.gov/portals/75/documents/news-features/initiatives/nsa21/nsa21-org-chart.pdf.

DEFENSE INFORMATION SYSTEMS AGENCY (DISA)

As a combat support agency, the Defense Information Systems Agency (DISA) has the primary objectives of protecting DOD networks and furnishing command, control, and information-sharing capacities to DOD, national leaders, and allies during military operations.[89] DISA is tasked with addressing and neutralizing critical threats to its portions of the DODIN (mainly through the use of DCO-IDMs) and managing other network infrastructure challenges.[90] DISA has created a zero-trust architecture called Thunderdome for DOD networks, for example, and is encouraging strong cyber hygiene among DOD employees.[91] DISA leadership reports to DOD's chief information officer (CIO). Its budget is nearly $12 billion—about an eighth of the entire IC budget—derived from $3.4 billion in congressional appropriations and $8.5 billion in a defense working capital fund. This budget supports the entire DOD, including the Joint Chiefs, the Joint Staff, combatant commands, and support to the White House.[92] Due to this vast mission and large budget, DISA's 7,000 employees are highly influential in the protection of DOD resources.

The DISA commander functions as both the JFHQ-C DODIN commander and is responsible for defending the DODIN. This creates tension for the commander, who works for the DOD CIO and the commander of USCYBERCOM simultaneously.[93]

Civilian Agencies

While the lines are somewhat blurred between military and intelligence cyber agencies, as with NSA and USCYBERCOM, there is a clearer separation between domestic civilian and foreign-facing civilian agencies. This section reviews the broad swath of civilian agencies with a role in the cyber realm, from the IC to FBI to CISA, with a general progression from those with a foreign mission to those with a mission of securing the homeland.

NATIONAL SECURITY COUNCIL (NSC)

The NSC sits atop a vast national security apparatus with a dual mandate to staff the president and to manage the policymaking process. Each president shapes the NSC differently. Some presidents want a huge staff deeply enmeshed in policy; others want a lean staff that directs and shapes without getting into the weeds.

The deputy national security adviser for cyber and emerging technology serves this dual role, advising the president, shaping cyber policy, and crafting a strategic course on emerging tech. Under the Biden administration, this role had "deputy assistant to the president" status—a high rank for the NSC, just below the national security adviser's role as assistant to the president. That rank signifies the deputy national security adviser's ability to bring the weight of the White House to interagency policy debates as well as their access to the president and the national security adviser. With an issue such as cyber, where the bureaucracy and mechanisms are still relatively young, that power is significant. The deputy national security adviser for cyber and emerging technology runs an interagency process that includes CISA, ONCD, and all cyber actors across DOD, the IC, and the Department of State, as well as other players such as the Department of the Treasury. CISA, ONCD, and even the deputy national security adviser are new by government standards, leading to expected churn related to establishing roles and responsibilities.

OFFICE OF THE NATIONAL CYBER DIRECTOR (ONCD)

ONCD takes its mandate from Congress and is guided by the White House's Strategic Intent Statement and National Cybersecurity Strategy. A national cyber director oversees each of seven key efforts:[94]

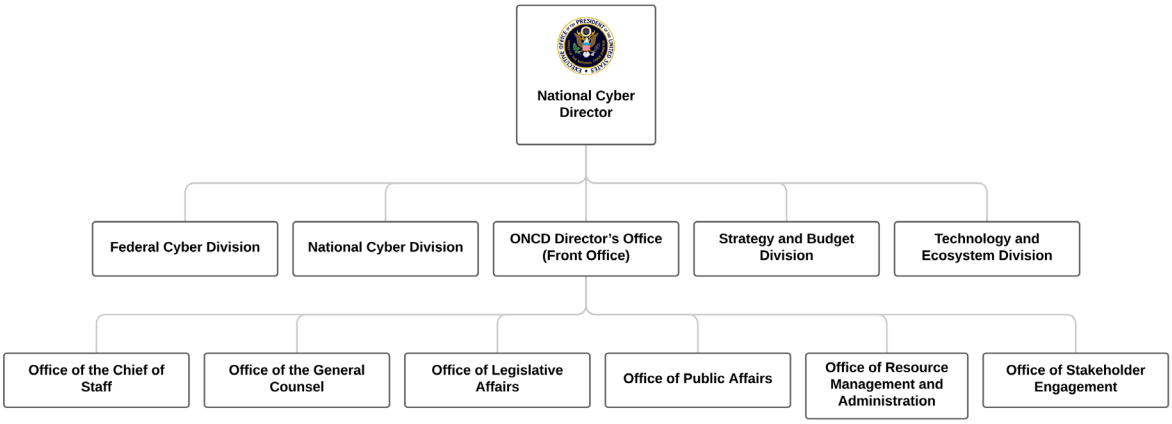
1. **National cybersecurity:** ONCD coordinates programs and missions aimed at protecting and defending local government and private sector networks. Additionally, it serves as a liaison between these programs and relevant international partners.
2. **Federal cybersecurity:** ONCD oversees and ensures that U.S. departments and agencies have access to "world-class cybersecurity."
3. **Budget review and assessment:** ONCD collaborates with the Office of Management and Budget to assist federal departments and agencies in planning and accounting for current

and future cybersecurity resources. This also involves assisting agencies in assessing the effectiveness of ongoing programs and supporting effective initiatives.

4. **Technology and ecosystem security:** ONCD collaborates with the private sector to cultivate a more secure digital supply chain and works to create a trusted digital ecosystem of products, devices, and services essential to the digital economy.
5. **Planning and incident response:** ONCD works closely with federal agencies, such as CISA, in "preventing and responding to cyber incidents to ensure they are . . . prepared . . . in protecting against, detecting, and responding to malicious cyber activity across government networks and critical infrastructure."
6. **Workforce development:** ONCD aims to ensure that both the public and private sectors have reliable access to new cyber talent, as well as to enhance broader cyber literacy and digital fluency among the public through capacity-building initiatives.
7. **Stakeholder engagement:** ONCD collaborates with Congress and stakeholders to keep all parties informed about recent cyber developments and promote new cyber initiatives.[95]

Situated within the Executive Office of the President, ONCD is a relatively small office, with a budget of $22 million (as of FY 2023) and approximately 100 staffers.[96] Additionally, the ONCD structure may be further delineated into its constituent deputy and assistant directors, each responsible for overseeing specific branches of the office.[97]

Figure 3: ONCD Organizational Chart



Source: CSIS research based on "Freedom of Information Act," White House, n.d., https://www.whitehouse.gov/oncd/freedom-of-information-act/#offices.

The CSC created ONCD to organize the federal government's response to pervasive and growing cyber threats. The CSC intended for ONCD to be within the White House for access to the president and added credibility for the mission. However, they decided to create a Senate-confirmed head of the program for accountability to Congress—a highly unusual arrangement. The president's staff is generally accepted as just that—responsible to the president but not to Congress. Inside the cone of the NSC and other White House offices, the job of the staff is to give candid advice to the president, and part of what protects that relationship is a buffer between the staff and Capitol Hill.

So far, the national cyber directors have assumed responsibility for executing the president's vision but also for wrangling the various parts of the U.S. government to a stronger cyber posture. With the power of attachment to the White House, the officers have pushed for better funding, closer coordination, and more attention to the cyber threat. Chris Inglis, the first national cyber director, said that he hoped to work himself out of a job—that in five years ONCD would be irrelevant because the government's defensive structures would be comprehensive, self-sustaining, and sound. After four years, ONCD has created the National Cybersecurity Strategy and an implementation plan designed to achieve the office's vision.

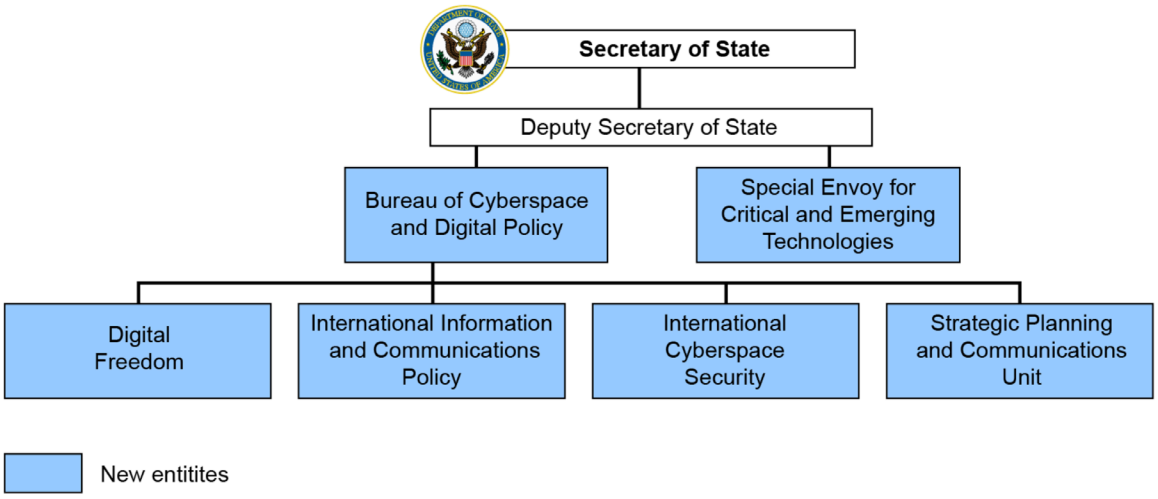
U.S. DEPARTMENT OF STATE

The State Department carries out diplomatic and foreign assistance activities that advance the objectives outlined in the 2023 National Cybersecurity Strategy, primarily through the Bureau of Cyberspace and Digital Policy (CDP). CDP leads efforts to promote "responsible state behavior in cyberspace" and advance U.S. policies abroad. Complementing CDP is the Directorate of Cyber and Technology Security (CTS), focused on safeguarding the department's personnel, critical infrastructure, and information assets.[98] Similarly, the Bureau of Information Resource Management (IRM) supports the department's IT infrastructure and defends it from cyber threats.[99]

Bureau of Cyberspace and Digital Policy (CDP)

According to its mission statement, CDP aims to "promote U.S. national and economic security by leading, coordinating, and elevating foreign policy on cyberspace and digital technologies."[100] It achieves this through one ambassador-at-large and, separately, four policy units, each focusing on a specific mission area and aspect of cyberspace (Figure 4).[101]

Figure 4: U.S. Department of State Cyber Entities



Source: U.S. Government Accountability Office, Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities, GAO-24-105563 (Washington, DC: GAO, January 2024), https://www.gao.gov/assets/d24105563.pdf.

DIGITAL FREEDOM TEAM

The Digital Freedom Team is responsible for spearheading the State Department's initiatives to promote "privacy, security, human rights, and civic engagement," as well as "Internet Freedom."[102] Additionally, the team collaborates with international partners to combat repressive and authoritarian practices in cyberspace.

INTERNATIONAL INFORMATION AND COMMUNICATIONS POLICY (ICP)

The International Information and Communications Policy (ICP) team aims to promote competitive and secure networks while safeguarding telecommunications services and infrastructure through activities such as "licensing, sanctions enforcement, and supply chain security."[103] Additionally, ICP supports internet governance initiatives and international technical standards by engaging with stakeholders. Moreover, the team works to promote personal data protection and privacy in partner countries and frequently works with U.S. private businesses, civil society members, and foreign governments.

INTERNATIONAL CYBERSPACE SECURITY (ICS)

The International Cyberspace Security (ICS) team primarily leads the State Department's efforts to "promote cyberspace stability and security and protect U.S. national security interests in cyberspace," which it does by engaging "in multilateral, regional, and bilateral forums" to coordinate multicountry responses to cyber threats.[104] ICS also collaborates with international partners, including the United Nations and Internet Governance Forum, to counter malicious actors abroad. Additionally, it coordinates the department's involvement in cyber policy discussions and leverages "foreign assistance funding to build cybersecurity capacity globally."[105] In 2023, ICS collaborated with the UN Group of Governmental Experts and Open-Ended Working Group to develop a framework on behavior in cyberspace, as well as "peacetime norms and confidence-building measures" for cyberspace.[106] Furthermore, in June 2023, ICS led a delegation of officials from USCYBERCOM, ONCD, and CISA to meet with Ukrainian deputy ministers and announce a $37 million nonmilitary cyber assistance package for Kyiv.[107]

STRATEGIC PLANNING AND COMMUNICATIONS (SPC) UNIT

The SPC Unit oversees the CDP's overall "strategic planning, public diplomacy, media, [and] legislative affairs activities."[108] It also manages its foreign assistance programs through the Digital Connectivity and Cybersecurity Partnership.

STRENGTHS OF CDP

A 2024 Government Accountability Office (GAO) report notes that CDP has "helped to better position State to achieve its cyber diplomacy goals" by consolidating its efforts under one ambassador-at-large, instead of dispersing efforts across the entire department.[109] According to the report, this approach "has facilitated engagement with higher levels of foreign government officials and has elevated the U.S. profile on cyber globally." The report also mentions CDP's involvement in enhancing the cyber defenses of Ukraine, its efforts in establishing the Freedom Online Coalition, and its participation in the negotiation process of the UN Cybercrime Convention to "facilitate international cooperation to combat cybercrime." GAO commends CDP's efforts to establish or "reinforce global norms of responsible state behavior" in cyberspace, which GAO claims it has done

by providing allied nations with cyber training and technical assistance. Additionally, the bureau has allocated funding to partners "that promote cybersecurity best practices aligned with U.S. cyber objectives."[110]

Office of the Special Envoy for Critical and Emerging Technology and Ambassador at Large for Cyberspace and Digital Policy

According to former-Ambassador Nathaniel Fick's testimony on January 17, 2024, to the House Foreign Affairs Subcommittee on the Indo-Pacific, the role of the ambassador-at-large for CDP is to "oversee the organizations that lead and coordinate the Department's work on cyberspace, digital policy, digital freedom, and emerging technologies."[111] The position was created as part of an effort to align current diplomacy with technical and national security issues, aiming to make the digital world more central to U.S. foreign policy.[112] Furthermore, the role of the ambassador-at-large is public facing and serves as a visible representation of U.S. cyber support. For example, after the Iranian cyberattacks in Albania in 2022, Ambassador Fick flew to the region to demonstrate U.S. support for Albania.[113]

The ambassador-at-large also oversees the Office of the Special Envoy for Critical and Emerging Technology.[114] The office focuses on advancing U.S. interests and advantages in critical and emerging technologies, coordinates U.S. cooperation with allies on emerging technology issues, and leads international technology diplomacy efforts. Some of these technologies include advancements in artificial intelligence (AI) and quantum computing.[115]

Directorate of Cyber And Technology Security (CTS)

Separately, CTS offers cyber, technology, and investigative expertise "to address emerging cyber-based threats affecting the department's personnel, critical infrastructure, and information assets."[116] Established by the Diplomatic Security Service (DSS) in 2017, CTS is the State Department's tactical cyber unit that defends State Department networks.

CTS detects, analyzes, and responds to various cyber threats while fulfilling a number of roles:

- Maintaining a 24/7, 365-day watch over the department's global cyber infrastructure and overseeing incident response, conducting analysis of cyber intrusions, conducting vulnerability assessments, and performing technical security assessments
- Producing threat analysis reports on malicious cyber activity, issuing threat alerts, and assisting with the department's cybercrime and counterintelligence investigations
- Regularly updating, maintaining, and developing new security standards for the State Department's software and hardware systems
- Serving as the department's liaison to the U.S. Computer Emergency Readiness Team and maintaining close relationships with FBI, NSA, and other federal law enforcement and IC agencies[117]

Bureau of Information Resource Management (IRM)

IRM oversees the technology infrastructure used in global State Department operations. IRM is one of the larger bureaus within the department, with IRM-related expenses constituting the majority of the State Department's $2-$3 billion cybersecurity budget. IRM collaborates closely with other department offices, including Consular Affairs, which safeguards online services such as passport renewal, and the Bureau of Diplomatic Security.[118] IRM fulfills a number of roles:

- Operating the State Department's network (similar to DOD's DISA)
- Developing tools within the State Department's networks and systems to enhance cybersecurity and manage cybersecurity platforms
- Promoting cybersecurity standards
- Overseeing the implementation of new IT solutions and tools that safeguard IT assets against "evolving cyber threats and vulnerabilities"[119]

IRM and CTS both report to the undersecretary for management, although CTS reports through DSS. As such, they collaborate but each has a distinct management chain.

DIRECTOR OF NATIONAL INTELLIGENCE'S CYBER THREAT INTELLIGENCE INTEGRATION CENTER (DNI/CTIIC)

Director of National Intelligence (DNI)'s Cyber Threat Intelligence Integration Center (CTIIC) was created to coordinate IC cyber activities and to provide policymakers a one-stop shop for collated information about cyber threats. Then-DNI Avril Haines in 2021 immediately prioritized cyber and looked to CTIIC to determine how ODNI should lead the cyber mission.[120] According to ODNI's website, the main purpose of CTIIC is to "lead the integration of cyber threat intelligence to inform national interests, support national cyber policy and planning efforts, and coordinate an IC-wide approach to cyber collection and investment."[121] In practical terms, one key CTIIC role is to create impactful, actionable intelligence products for Principals and Deputies Committee meetings, particularly drawing on the expertise and information available in industry.[122]

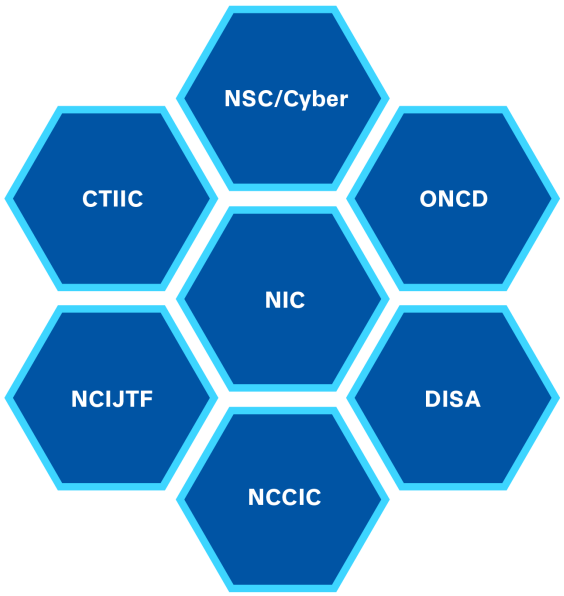
CTIIC has the following roles and objectives:

- **Cyber intelligence:** Providing both IC-obtained intelligence as well as commercial cyber intelligence to key decisionmakers and "network defenders"
- **Identifying opportunities:** Collaborating with the IC to "identify opportunities to integrate cyber collection, data exploitation, and analysis across the IC" due to its location within ODNI
- **Partnership engagement:** Collaborating with U.S. government agencies, foreign nations, and the private sector to enhance "visibility into cyber threats, support enhanced processing and sharing of cyber intelligence, and incubate new cyber capabilities"[123]

As a component of ODNI, CTIIC adopts an IC-wide perspective to countering cyber threats, in collaboration with the National Intelligence Council and various agencies across the IC.[124] In 2015, at the time of its creation, NSC wanted one entity to pull together relevant information about cyber activity to inform the NSC on a daily basis. Since then, ONCD was created in 2021, the NSC cyber

staff has gotten more robust, and entities such as the National Cyber Investigative Joint Task Force (NCIJTF) and the National Cybersecurity and Communications Integration Center (NCCIC) are engaging in similar missions.

Figure 5: U.S. Government Entities with Coordinating Roles on Cyber



Source: Authors' analysis.

CTIIC primarily functions as one cyber arm of ODNI and collaborates closely with other ODNI offices, as well as the National Intelligence Council, the IC CIO, the National Counterintelligence and Security Center, and the Foreign Malign Influence Center.[125] CTIIC is structured into four offices, although little public information exists about their responsibilities: the Office of the Director, Office of Analytic Integration, Office of the Research Director, and Office of the National Intelligence Manager (NIM) for Cyber.[126] Embedding the NIM for Cyber in the office was an attempt to limit the duplication of roles. Questions were raised at its founding regarding whether the NIM for Cyber was enough of a coordinating function, but NSC staff felt at the time that a more robust structure was needed to produce and publish coordinated intelligence products. At time of publishing, CTIIC had about 50 full time staff. [127]

In addition to classified work, CTIIC creates publicly available threat reports addressing a variety of cyber intelligence issues, including global ransomware trends and activities, foreign cyber threat actors, and the proliferation of foreign commercial spyware.[128] It also hosts a frequent "cyber response group," in which government officials review current cyber threats. [129]

CIA DIRECTORATE OF DIGITAL INNOVATION (DDI)

The Directorate of Digital Innovation (DDI) is one of five directorates within CIA. Its role is to ensure that CIA teams are equipped with the "tools and techniques they need to operate in a modern,

connected world."[130] Covering areas from cybersecurity to IT infrastructure, the DDI ensures that CIA capabilities keep pace with advancements in the digital landscape.

While the DDI's structure remains classified, a series of leaks in 2017 described a set of teams and capabilities. Because this information was illegally released and CIA has since likely changed its structure, researchers will not reprint the details here.

FEDERAL BUREAU OF INVESTIGATION (FBI)

FBI is authorized to investigate cyber incidents that blur the line between criminal activity and national security concerns, exemplified by FBI's 2024 investigation into Volt Typhoon's malicious activity. This investigation revealed Chinese hackers' successful infiltration of networks within crucial sectors such as "critical telecommunications, energy, water, and other infrastructure sectors."[131] While FBI is a domestic law enforcement agency with some intelligence authorities, it is constrained in how it can operate inside the United States by law enforcement's tightly prescribed roles.

FBI's cyber organization comprises two main sections: the cyber capabilities embedded within its field offices and the Criminal, Cyber, Response, and Services Branch (CCRSB) headquartered in the J. Edgar Hoover Building in Washington, D.C.

Field Offices

Each of FBI's 56 field offices includes a Cyber Task Force (CTF). Each CTF convenes "cyber investigators, prosecutors, intelligence analysts, computer scientists, and digital forensic technicians" from various federal, state, local, and tribal agencies.[132] They also include computer scientists and intelligence analysts who support cyber incident response efforts, cyber intelligence collection, and technical assistance. The other aim of each CTF is to cultivate local relationships with private companies and organizations and quickly deploy and respond to local cyber incidents.

Criminal, Cyber, Response, and Services Branch (CCRSB)

The CCRSB serves as FBI's primary centralized cyber branch and oversees national and international "criminal and cyber investigations worldwide, as well as international operations, critical incident responses, and assistance to victims."[133] It is further structured into the following divisions:

- **Criminal Investigative Division:** The Criminal Investigative Division functions as the investigatory arm of the CCRSB, tasked with probing all forms of illegal online activity under federal law. It primarily focuses on cyber intrusions, such as ransomware groups and online extortion operations.
- **Cyber Division:** The Cyber Division includes several branches, with the most relevant being the Cyber Operations Branch. This branch serves as the operational arm of the CCRSB and oversees both cybercriminal investigations and national security investigations. It is the frontline team tasked with executing arrests and takedowns of cybercriminals operating within the United States. This branch also works with various agencies such as NSA, FBI, CIA, DHS, CISA, and U.S. Secret Service, to "impose costs on nation states and others for engaging

in hacking activity."[134] Further, because this branch deals with nation-state actors, it also partners frequently with international bodies such as Europol.[135]

- The Cyber Action Team (CAT) falls underneath the Cyber Division. CAT is FBI's rapid response team, which provides "rapid incident response on major computer intrusions and cyber-related emergencies."[136] CAT comprises a core team stationed at the FBI headquarters in Washington, D.C., supplemented by approximately 50 special agents and computer scientists drawn from various FBI field offices. These field agents typically possess advanced training in computer languages, forensics, and malware analysis, making them the frontline responders to any "significant cyber incidents that have the potential to impact public health or safety, national security, economic security, or public confidence."[137] CAT claims the capability to deploy across the country "within hours."[138] Moreover, CAT extends its reach to international cyber incidents and is said to be able to deploy "anywhere in the world within 48 hours" to offer investigative support to partner countries and agencies.[139]
- The Cyber Operations Branch houses the NCIJTF, which comprises over 40 co-located agencies from the IC, various law enforcement agencies, and DOD. NCIJTF's primary function is to "coordinate, integrate, and share information to support cyber threat investigations [and] supply and support intelligence analysis for community decision-makers."[140] Within the NCIJTF is CyWatch, FBI's 24/7 operations center tasked with providing continuous support to monitor incidents and communicate with field offices nationwide. Specifically, CyWatch is responsible for "coordinating [the] domestic law enforcement response to criminal and national security cyber intrusions" and collaborating with other federal cyber centers around the clock. Additionally, CyWatch provides "real-time incident management and tracking" capabilities to FBI and its partner agencies.[141]
- The Critical Incident Response Group offers crisis support and incident management assistance to federal and SLTT governments and agencies.[142]

- **International Operations Division:** The International Operations Division focuses on FBI's international operations and oversees FBI's cyber assistant legal attaché (Cyber ALAT) program. The Cyber ALAT program comprises FBI cyber agents who undergo training both at FBI headquarters and alongside international counterparts across 18 locations worldwide. This program aims to have FBI agents forge relationships with international partners to improve collaboration on international cybercrime cases. Therefore, when the FBI collaborates with Europol, it primarily does so through this ALAT program.[143]

FBI stands out in its capacity to collect domestic crime data and intelligence, enabling it to support CISA in identifying vulnerable networks susceptible to techniques similar to those used in the past by adversaries. Moreover, it can help Sector Risk Management Agencies "assess and mitigate cyber threats to critical infrastructure" and furnish USCYBERCOM or NSA with "information on a piece of a malicious foreign actor's infrastructure to disrupt or exploit."[144] According to Bryan Vorndran, assistant director of FBI's Cyber Division, in a statement provided to the House Judiciary Committee,

the bureau possesses a distinctive capability to counter malicious cyberattacks on U.S. networks by leveraging its "unique authorities." This stems from FBI's adeptness in utilizing its international law enforcement ties, connections with domestic victims, and partnerships with key technology service providers to detect and thwart cyber adversaries before they compromise U.S. networks.

DEPARTMENT OF HOMELAND SECURITY'S CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (DHS/CISA)

In contrast to FBI, CISA has no law enforcement role. Instead, it has defined itself as a partner, not an investigator. In reaching out to federal and SLTT entities, as well as establishing mechanisms for coordination with the private sector, CISA is an information clearing house, an adviser, and an educator and evangelist about the necessities of cyber defense. Its official mission, according to its website, is to be the "operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience."[145] CISA fulfills its mission through its various divisions and subdivisions, with the Cybersecurity Division (CSD) at the forefront of cyber defense.[146]

Cybersecurity Division (CSD)

CSD is tasked with strengthening the country's cyber defenses "against immediate threats and vulnerabilities," as well as building "long-term capacity to withstand and operate through cyber incidents."[147] To effectively manage these responsibilities, CSD consists of the following specialized subdivisions with specific objectives:

- **Capacity building:** Enhance and centralize cybersecurity capabilities across the federal civilian executive agencies and nonfederal partners.[148]
- **Mission engineering:** Serve a largely administrative and coordination role, conducting strategic planning and providing cyber operators and analysts with "mission capabilities" to safeguard the nation's cyberspace.[149]
- **Joint Cyber Defense Collaborative (JCDC):** "Unite the global cyber community in the collective defense of cyberspace." JCDC is a CISA-led public-private cybersecurity collaborative.[150] (See the following section on the JCDC.)
- **Vulnerability management:** Minimize critical vulnerabilities and "exploitable conditions across enterprises and technologies."[151]
- **Threat hunting:** Conduct "incident response and threat hunting missions" for the division and counter malicious activity through cyber detection and forensic capabilities.[152]

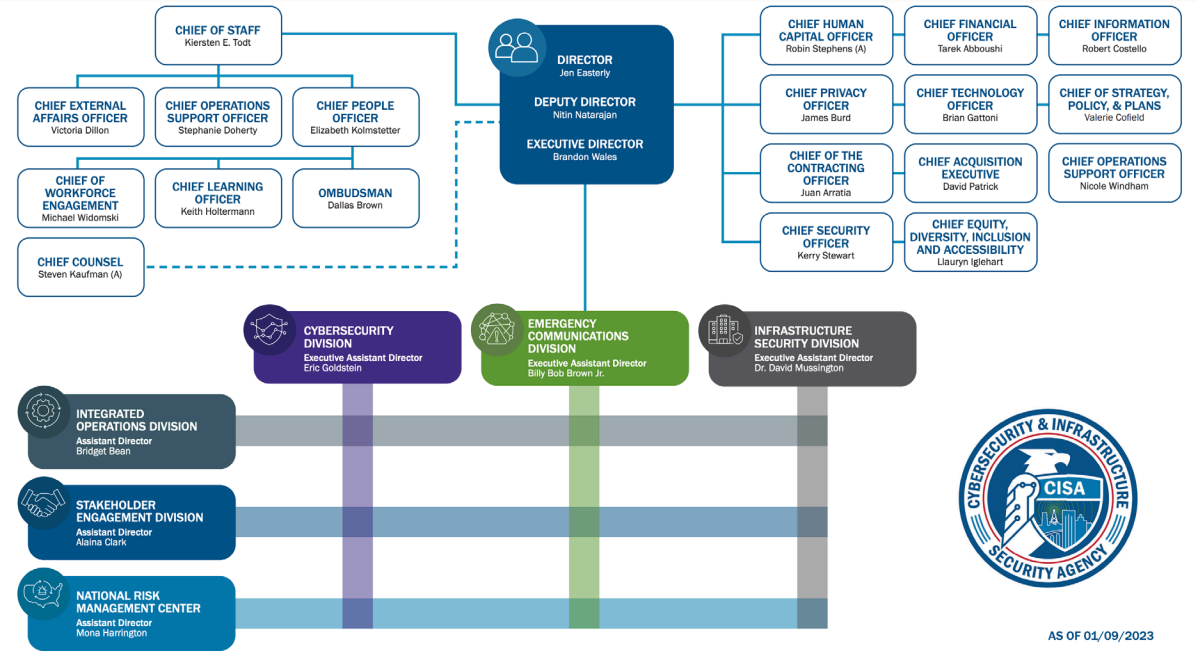
Jeff King, acting CIO at the Treasury Department, stated that CISA has the potential to be a "real catalyst" in threat hunting. However, he emphasized that CISA needs to act as a "driver and a doer rather than a coordinator."[153]

Promoting Secure by Design Principles

In April 2023, CISA launched its Secure by Design campaign, which aims to enhance the safety, security, and resilience of technology by urging software manufacturers to integrate stricter security features within their software development process from the outset. This initiative notably

drew upon suggestions and insights from its JCDC subdivision (see the section below on the JCDC).[154] It is too early to tell whether this initiative will have any real effect on cybersecurity, particularly given that the campaign is purely educational and voluntary and not mandating any change.

Figure 6: CISA Organizational Chart



Source: "CISA 101 Organizational Chart," CISA, July 6, 2021, https://www.cisa.gov/sites/default/files/publications/CISA_101_org_chart_07062021_NAMES_508.pdf.

Joint Cyber Defense Collaborative (JCDC)

JCDC, led by CISA, is a public-private cybersecurity collaborative designed to "unite the global cyber community in the collective defense of cyberspace."[155] Under authorities granted in the FY 2021 NDAA, which stemmed from a CSC recommendation, the JCDC aims to promote public-private "cyber defense planning [and] cybersecurity information fusion and analysis" through three goals[156]:

> First, establish enduring capabilities for persistent collaboration in which participants continuously exchange, enrich, and act on cybersecurity information with the necessary agility to stay ahead of our adversaries; second, to develop and jointly execute proactive cyber defense plans intended to reduce the most significant risks before they manifest; and, third, enable true co-equal partnership between government and the private sector, including through joint enrichment and development of timely cybersecurity advisories and alerts to benefit the broader community.[157]

JCDC seeks to close gaps between the federal government, critical infrastructure providers, industry, and SLTT governments, along with international partners when needed.[158] Participants in the JCDC include service providers, infrastructure operators, cybersecurity firms, and companies

across various critical infrastructure sectors. Together, they work to coordinate cybersecurity planning, defense, and response efforts. The JCDC also incorporates specific government agencies designated by Congress for the joint cyber planning office, which includes DHS, USCYBERCOM, FBI, the Department of Justice, and ODNI. Furthermore, the JCDC also has collaboration provisions with DOD, the Transportation Security Administration, the EPA, the Federal Aviation Administration, the Department of Energy, and the Department of Transportation. JCDC had about 150 full-time staff at time of publishing, heading toward about 175 to be fully staffed.[159]

JCDC's first step was to define "joint cyber defense planning." Leadership saw JCDC's role as charting a new course for what true collaboration might look like, including two-way information sharing and letting industry drive the workstream. Its second mission was to think through how to unify public and private national resources in response to a massive cyber incident; the log4j vulnerability proved to be an early, real-world test. Their third step was meant to be an evolution in shaping the information-sharing ecosystem, beginning with some of the largest key players in three areas: cloud providers, internet service providers, and cyber threat intelligence companies.[160]

Some criticisms of the JCDC remain, however. At a CSIS event in February 2024, Jeff Spaeth, the deputy CISO at the Department of Veterans Affairs, noted that the JCDC is "still in its infancy, with some kinks that still need to be worked out."[161] One criticism Spaeth highlighted is the delay that the JCDC often experiences when relaying information from private sources, typically major vendors, to other departments. Jeff King, the acting CIO at the Treasury Department, noted that the "ingredients are there" for the JCDC to be a leading figure in cybersecurity; yet he also pointed out that the JCDC is "still in a very early stage" and that much work remains to develop it into a "repeatable and reliable apparatus."[162]

The JCDC has achieved some notable successes over the past two years. These include providing valuable feedback to CISA's Secure by Design and Secure by Default initiatives, coordinating a large-scale cyber vulnerability exploitation exercise, and leading efforts against an emerging Chinese advanced persistent threat (APT) campaign.[163] Furthermore, over the past year, CISA has expanded the JCDC's focus to include "open-source software security" and cybersecurity protecting high-risk communities, such as journalism and civil society organizations, according to a House Committee on Homeland Security hearing.[164]

Between 2021 and 2022, CISA identified an emerging Chinese APT campaign and collaborated with JCDC members "to better understand the nature of the activity and identify multiple zero-day vulnerabilities used as initial intrusion vectors." The JCDC also shared network defense information with SLTT governments and partnered with CISA to develop two network defense advisories in response to this emerging APT.[165]

To enhance the cybersecurity and resilience of industrial control systems (ICSs), which are a critical component of modern critical infrastructure systems, the JCDC established a subgroup named JCDC-ICS. The group comprises ICS industry experts from 10 new companies, including security vendors and distributors, and two existing JCDC partners experienced in ICS. The aim of this collaboration is to take "advantage of the knowledge, visibility, and capabilities of the ICS

community" to better protect and defend control systems and "inform U.S. government guidance on ISC/OT cybersecurity."[166]

Private Sector Actors

A major strength of the U.S. system is its robust private sector. A host of cyber researchers and threat hunters protect industry and, often, government systems. Many of these employees are former government officials who saw a need that industry could fill and left to start that business. They play a critical role in overall cyber defense: because U.S. ICT is largely privately owned and comparatively open (i.e., not protected by a great firewall or cordoned off from the outside internet), industry has stepped up to fill a security void.

Cybersecurity companies often include robust cyber threat analysis research capabilities and teams. New companies emerge frequently, leading to a growing and changing ecosystem of cybersecurity providers. Private sector entities may be categorized by their role: cyber defenders such as CrowdStrike or Dragos; software providers who create the product and thus the attack surface such as Microsoft; and critical infrastructure vendors such as Siemens. Those who create the software packages have a mission: provide the best product to the customer. But they also must provide a safe product. The defenders then protect the customer despite flaws in the software packages.

An incident in July 2024, where a CrowdStrike software update resulted in perhaps the largest IT outage in history, demonstrated how much global entities rely on private cybersecurity firms. The way the update interacted with Windows led to a massive, unresolvable malfunction, causing the dreaded "blue screen of death" across the globe. The update existed for a mere 90 minutes before CrowdStrike pulled it back, but in that brief time it disrupted global travel, commerce, healthcare, and other industries, and it caused an estimated $5.4 billion in losses.[167] The outage will cause "renewed attention around the world to anti-trust regulation, tech competition, and cloud services standards," according to CSIS's James Andrew Lewis.[168]

Case Study

Operation Glowing Symphony

"Neil could see login screens—the actual login screens of ISIS members half a world away. Each one carefully preselected and put on a target list that, by Operation Day, had become so long it was on a 3-foot-by-7-foot piece of paper hung on the wall."[169]

—Dina Temple-Raston, "How the U.S. Hacked ISIS"

In Operation Glowing Symphony, cyber operators from Australia, the United Kingdom, and the United States disrupted ISIS networks, preventing online recruitment and preempting propaganda operations. As members of the terrorist group slept, a room full of military cyber operators at Fort Meade were ready to take over and crash ISIS accounts.[170] For months in 2016 and 2017, the Glowing Symphony team—otherwise known as Joint Task Force ARES—deleted content, crashed servers, misconfigured networks, changed passwords, drained cell phone batteries, and found ways to sow discord among fighters from inside their own systems.[171]

The operation was generally seen as successful. The IC's self-assessment at the 30-day mark was typically reserved, determining that ISIS media had been "disrupted."[172] NPR reported that, according to three people privy to details, six months after the initial attack, "ISIS's media operation was a shadow of its former self. . . . Most of the media operations servers were down and the group had not been able to reconstitute them." In the medium to long term, the mission shifted into a maintenance phase, keeping pressure on ISIS, complicating its cyber operations, and hobbling its ability to raise funds. NPR reported that ARES was still in ISIS networks three years after the operation launched.[173] However, some private sector cyber researchers downplayed the success, saying that battlefield losses may have contributed to the downturn in quantity of propaganda and

that other pro-ISIS channels continued to publish.[174] The operation was considered complex and highly instructive on how to bring a multitude of resources and partners to bear for results against a relatively unsophisticated target.[175]

Part of what made the operation both successful and complex was the coalition of allies who collaborated to take ISIS down. Australian news sources reported, "Working in a windowless room in Canberra, [the Australian Signals Directorate's] cyber fighters tapped away at their keyboards, targeting a list of targets pinned to the wall. For 12 hours they accessed accounts, locked Islamic State members out, stole the contents and deleted backups of the files."[176] In the United States, support came from Joint Forces Headquarters, an Army cyber group based in Georgia, and from experts in counterterrorism in general and in ISIS in particular.[177] According to a heavily redacted 30-day assessment, NSA worked in "close coordination between Joint Task Force Ares, USCYBERCOM, [and] FBI" to attack ISIS networks.[178] USCYBERCOM also coordinated across combatant commands, including with Combined Joint Task Force Inherent Resolve, Operation Inherent Resolve, and U.S. Central Command.[179]

An Opportunity, as Part of a Campaign

JTF-ARES operators seized an opportunity to hit ISIS networks as part of the larger campaign to take down ISIS. In examining ISIS networks, cyber operators learned that 10 core accounts and servers managed all ISIS content:

> The group's network administrators weren't as careful as they should have been. They took a shortcut and kept going back to the same accounts to manage the whole ISIS media network. They bought things online through those nodes; they uploaded ISIS media; they made financial transactions. They even had file sharing through them. "If we could take those over," [a U.S. Marine operator named] Neil said, grinning, "we were going to win everything."
>
> The young Marine ran into his leadership's office at NSA, grabbed a marker and started drawing crazy circles and lines on a whiteboard. . . . As Neil kept explaining and drawing he could see the leaders begin to nod. "I drew this bicycle tire with spokes and all the things that were tied to this one node and then there was another one," he said. "It was a house of cards."[180]

Surveillance started, and operators spent months practicing on cyber ranges. At the same time, operators started running the traps on the policy process to be sure they had interagency buy-in.

Problems Encountered: Taking a New Idea Through the Interagency Process

Securing approval through the interagency proved more difficult than anticipated. Several agencies did not concur when the planning document went through coordination. These concerns were related to intelligence loss (ability to collect in the future), exposure of human sources, and

objections related to bouncing through servers located in third countries. Under Presidential Policy Directive 20 (PPD-20), these agencies had veto power over cyber operations.[181] Over several weeks, a series of Deputies Committee meetings and Principals Committee meetings ensued to adjust the plan and resolve concerns from CIA, the State Department, and FBI. Those delays and changes to operational design probably reduced the overall effectiveness of the operation, although the public 30-day review documents are heavily redacted in this area.[182] In the cyber domain, any delay risks losing fragile accesses, as the adversary may patch or even restructure its networks.

The interagency concerns were largely around operating on networks located in foreign countries without prior notification.[183] While the ISIS actors were physically in Syria, the servers and other ICT infrastructure were global. The *Washington Post* reported, "The Pentagon drew up a list of about 35 countries outside of the war zones of Iraq and Syria that might have hosting services with videos and other Islamic State content to remove." CIA director John Brennan, Secretary of State John F. Kerry, FBI director James B. Comey, and Director of National Intelligence James R. Clapper Jr. argued in favor of notifying countries that a cyber action was about to take place in order to preserve relationships. Pentagon officials countered that they could take action under existing authorities to counter terrorists' use of the internet and that notice was not required. Some also pointed out the possibility of leaks, which could prove disastrous to the operation. In the final accounting between what the United States is "required to" and "should" do when conducting an offensive cyber operation, about 15 countries were notified, but action took place only in 5 or 6, according to the *Washington Post*.[184]

Part of the risk calculation was to gauge the extent to which a cyber strike could be surgical, or specifically targeted to affect only ISIS operations and not any other functions. Air Force general Tim Haugh explained, "On every server there might be things from other commercial entities. . . . We were only going to touch that little sliver of the adversary space and not perturb anyone else." The stakes were particularly high in allied nations such as France and Germany, where harm to a commercial entity likely would be met with frustration by a close ally.[185] Planning with precision, then reassuring policymakers that the action could be precise, all took time.

Also compounding the time delay was an additional approval process. In a kinetic strike, there is a well-established process for nominating a target and clearing it. In the relatively new realm of cyber warfare, however, ARES operators had to complete their own vetting and deconfliction process, on top of the combatant command's target designation. In addition, kinetic operations were ongoing in Mosul, and the two lines of effort needed to work in concert, not in opposition.[186] After-action reports later indicated that Glowing Symphony forced new processes for target validation, operational deconfliction, and interagency coordination.[187]

One additional, absurdly pedestrian problem bears mentioning: version control over planning documents became an issue. Given a handful of allies, with several agencies participating from each, finding a software solution that keeps everyone up to date and on the same page was a challenge. The common operating picture was simply text documents, demonstrating once again that the U.S. government takes care of its own IT needs last.[188]

The common operating picture was simply text documents, demonstrating once again that the U.S. government takes care of its own IT needs last.

Takeaways

USCYBERCOM and NSA learned considerable lessons from Glowing Symphony. Several key takeaways emerged from this largely successful endeavor.

The task force model works. USCYBERCOM leaders have discussed the benefit accrued to a mission by pulling together a small group of operators in a task force. In 2016, when USCYBERCOM was involved in countering the Russian threat to elections, General Nakasone elected to adopt the same approach. The U.S. government created a Russia Small Group rather than working through Joint Force Headquarters Cyber (Air Force) assigned to support U.S. European Command.[189]

Coordination has become the expectation rather than the exception in U.S. policymaking. The 30-day assessment of Glowing Symphony states, "Key to this operation was close coordination between Joint Task Force (JTF) ARES, USCYBERCOM, the Federal Bureau of Investigation (FBI), the National Security Administration (NSA), and [redacted]."[190]

Still, the after-action report acknowledges bumpy roads in the approval process: "Interagency policies and processes are not established to meet the demand for speed, scale, and scope required for effective cyberspace operations."[191] Further, it called for normalizing interagency processes to adjudicate nonconcurrence "expeditiously, in a manner that supports dynamic targeting within the cyber domain." This is a key point for any interagency process, but when the domain is new and practices are yet to be fully established, it is additionally difficult, even more so when it is unclear exactly what qualifies as an appropriate, proportional, or low-risk activity. The assessment states, "The time required to elevate and negotiate the interagency non-concurs prevented USCYBERCOM from [redacted] as originally designed."[192] By the time USCYBERCOM navigated the gauntlet, interagency members had reduced operations to a shell of what was intended, costing months or even years in delays. Both Congress and DOD were very critical of USCYBERCOM's lack of action, when in reality its hands were tied by the interagency. Some of these concerns were addressed by NSPM-13, which delegates some authority to the secretary of defense, but the Biden administration reinstated requirements to coordinate.[193]

Further, the coordination took human hours that could have been spent on mission research and execution. The after-action report states, "The amount of informal meetings, briefings, and overall information sharing that occurred was extremely in-depth and time consuming for both USCYBERCOM and JTF-ARES staffs. If this same level of detail is required for each proposed action during an OCO mission . . . [redacted]."[194] The redacted portion may be something along the lines of "it will severely restrict USCYBERCOM's capacity to act." The report then follows with these comments: "Absent of significant policy changes from OSD, USCYBERCOM is limited in its ability to

challenge ISIS [redacted]. . . . The updated version of [redacted] seeks to provide [redacted].” The redacted portions may be a reference to a planned policy intended to smooth some of the frictions of the coordination process—almost certainly NSPM-13.

Finally, a relatively flat hierarchy seems to have helped operators overcome some of the communication and comprehension challenges. General Edward Cardon, the first commander of JTF-ARES, pointed to the gulf between the junior operators on the task force and the seniors. NPR reported that the juniors “understood hacking in a visceral way and, in many respects, understood what was possible in cyberspace better than commanding officers did.”[195] This dynamic necessitated a relatively flat structure, by military standards, whereby the operators and juniors needed direct access to the senior officers so that decisions could be made accurately and quickly, with minimal lost in translation along the way.

Glowing Symphony was a complex operation against a relatively unsophisticated opponent who took little care to secure its networks. Policymakers most likely were willing to engage in the operation precisely because it was low risk. The United States and its allies were already engaged in kinetic conflict, so calculations about escalation were unnecessary. The actor was not really sophisticated enough to engage in counterattacks in the cyber domain. This operation both fit within the U.S. risk tolerance and had little downside.

On the positive side, it allowed U.S. government entities to test new tools, structures, and ways of running old policy processes. Those lessons led to changes within months, as NSA and USCYBERCOM ramped up to confront a far more sophisticated adversary intent on disrupting the foundations of democracy: Moscow.

Conclusion

Generally, U.S. offensive and espionage capabilities in the cyber domain are considered superior—among the best in the world. The IISS report from 2021 presumes that the United States can target an enemy's command and control assets, weapons navigation and delivery systems, and critical national infrastructure such as power and transportation, but U.S. "capabilities have not yet been demonstrated at their full potential."[196] IISS attributes this overall excellence to "a high-grade cyber-intelligence capability complemented by high-grade human intelligence collection; leadership of the technologically advanced Five Eyes intelligence alliance; a powerful cyber-industrial and academic base; and mature doctrine and legal authorities."[197] Still, a relatively weak defensive posture hampers this offensive capability significantly, at least in the minds of policymakers who are hesitant to climb an escalation ladder, knowing full well that the foundations that ladder rests upon are weak. Uneven cyber hygiene, underfunded federal and SLTT IT budgets, and a lack of effective deterrence collide to create low, pockmarked castle walls. ONCD and CISA have worked to create initiatives such as Secure by Design to instill in those who write software both an urgency and a sense of responsibility for the common defense. Insurance companies have learned more about the risk picture and have adjusted their premiums for ransomware attacks, encouraging individual entities to do better on basic defense.

Resource constraints play a role. According to retired U.S. Army colonel George Corbari, the United States is significantly more focused on offensive capabilities than defensive ones:

> Offensive capabilities are sexy and are preferred over the ability to defend ourselves adequately. Seems ridiculous, but completely true. Resource allocation decisions are complex

> and difficult; no senior leader wants to cut or pull back on pursuit of offensive capability or capacity, but they will quickly reduce the same for defense in order to grow offense.[198]

This combination of factors means that the U.S. system has stumbled into a de facto cyber strategy—one that fails to mirror U.S. global dominance in other domains. It entails exquisite, surgical offense marked by risk aversion and deniability. But it also includes a lack of effective response to attacks by hostile foreign powers and a certain degree of denial when it comes to the severity of those attacks. Trend lines are particularly disturbing: adversaries are less and less deterred, and defense is not catching up fast enough.

Uneven cyber hygiene, underfunded federal and SLTT IT budgets, and a lack of effective deterrence collide to create low, pockmarked castle walls.

The U.S. national security enterprise needs to immediately increase the level of urgency and brief non-national security entities on the clear and present danger in the cyber domain. Meanwhile, policymakers need to put serious emphasis on developing a new strategy of proportionality and deterrence in the cyber domain, working to embed this set of tools alongside other foreign policy options. See Part 7: How the United States Can Win for mindset shifts and policy changes that are urgently needed in this space.

About the Authors

Emily Harding is director of the Intelligence, National Security, and Technology (INT) Program and vice president of the Defense and Security Department at CSIS. As the head of the INT Program, she provides thought leadership on the most critical issues facing intelligence professionals and on the future of intelligence work. She also serves as vice president of the Defense and Security Department, where she is responsible for leading a team of world-renowned scholars providing policy solutions that shape national security. Drawing on her decades of experience in national security, Emily has established herself as an expert on how technology is revolutionizing national security work. Harding has served in a series of high-profile national security positions at critical moments. While serving as deputy staff director on the Senate Select Committee on Intelligence, she led the committee's investigation into Russian interference in the 2016 elections, which was lauded for its bipartisanship. At CIA, she led analysts and analytic programs through moments of crisis, including shepherding the Iraq Group during the attempted Islamic State takeover. During a tour at the National Security Council, she served as director for Iran. After leaving the White House, her team ran the first Office of the Director of National Intelligence-led presidential transition, where she was responsible for briefing the incoming administration. Harding is an adjunct lecturer at the Johns Hopkins School of Advanced International Studies. Her analysis has appeared in the Wall Street Journal, BBC, NPR, Bloomberg, and other outlets. Harding holds a master's degree from Harvard University's Kennedy School of Government and a bachelor's degree from the University of Virginia.

Aosheng Pusztaszeri is a research assistant with the Intelligence, National Security, and Technology (INT) Program at CSIS, where he focuses on emerging technologies and their implications for national security. Prior to joining CSIS, Aosheng interned in the U.S. Senate

and the U.S. House of Representatives and worked as an undergraduate research assistant in Cornell University's Department of Government. He holds a BA in government and history from Cornell University.

Julia Dickson is a research associate with the Intelligence, National Security, and Technology (INT) Program at CSIS. Her research interests include cybersecurity and cybercrime and the role of technology in conflict. Prior to joining CSIS, she was awarded a Fulbright grant and spent a year teaching English in Osh, Kyrgyzstan. She was also previously a research assistant at the Wilson Center, an intern for the Conventional Defense Program at the Stimson Center, and a communications and outreach intern at the International Crisis Group. She holds a BA in international studies with a minor in French from the Johns Hopkins University.

Endnotes

1 The authors acknowledge that the vast majority of U.S. offensive cyber capabilities remain classified. However, enough open-source materials exist to draw certain conclusions about U.S. strategy in this space, and the authors interviewed current and recent former cyber professionals to test these conclusions.

2 International Institute for Strategic Studies (IISS), *Cyber Capabilities and National Power: A Net Assessment* (London: IISS, June 2021), https://www.iiss.org/research-paper/2021/06/cyber-power---tier-one/.

3 Cybersecurity and Infrastructure Security Agency (CISA), "CISA Releases 2023 Year in Review Showcasing Efforts to Protect Critical Infrastructure," press release, January 17, 2024, https://www.cisa.gov/news-events/news/cisa-releases-2023-year-review-showcasing-efforts-protect-critical-infrastructure.

4 James Pearson and Raphael Satter, "What Is Volt Typhoon, the Chinese Hacking Group the FBI Warns Could Deal a 'Devastating Blow?'," Reuters, April 19, 2024, https://www.reuters.com/technology/what-is-volt-typhoon-alleged-china-backed-hacking-group-2023-05-25/.

5 David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled into Ukraine, So Did Malware. Then Microsoft Entered the War," *New York Times*, February 28, 2022, https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html; and Ken Proska et al., "Sandworm Disrupts Power in Ukraine Using a Novel Attack against Operational Technology," Google Cloud, November 9, 2023, https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology.

6 "Significant Cyber Incidents," CSIS, last updated July 2024, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. Espionage has long lived in a different category than acts of war. Espionage tends to inflict not physical damage but rather embarrassment and the loss of secrets that can damage national security. The difference between cyber for espionage and cyber for physical damage is explored in depth in this chapter, along with the complicating fact that discerning the difference between the two is particularly difficult in the cyber domain.

7 U.S. Department of the Treasury, "Treasury Sanctions Actions Responsible for Malicious Cyber Activities on Critical Infrastructure," press release, February 2, 2024, https://home.treasury.gov/news/press-releases/jy2072.

8 Grant Schneider, "President Trump Unveils America's First Cybersecurity Strategy in 15 Years," Trump White House Archives, September 20, 2018, https://trumpwhitehouse.archives.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.

9 IISS, *Cyber Capabilities*.

10 Jan Wolfe and Brendan Pierson, "Explainer—U.S. Government Hack: Espionage or Act of War?," Reuters, December 21, 2020, https://www.reuters.com/article/global-cyber-legal/explainer-us-government-hack-espionage-or-act-of-war-idUSKBN28T0HH/.

11 Joshua Rovner, "Cyber War as an Intelligence Contest," War on the Rocks, September 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

12 Tom Uren, Bart Hogeveen, and Fergus Hanson, "Defining Offensive Cyber Capabilities," Australian Strategic Policy Institute, July 4, 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities.

13 It is worth noting that the terms "cybersecurity" and "cyber defense" are often used as close synonyms. Cybersecurity is defensive by nature—it means securing one's systems to ensure that an adversary cannot get in, or, if it does, that it cannot cause much damage. Cyber defense is a broader term, and according to government documents such as Presidential Policy Directive 20, offensive tools can defend forward against an adversary's attempts to penetrate a system.

14 Wolfe and Pierson, "Explainer."

15 David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html. According to interviewee 1, Bolton tended to overplay the ability to deploy cyber for immediate physical consequences. This quote reflects that tendency but still communicates the more aggressive approach.

16 Dina Temple-Raston, "How the U.S. Hacked ISIS," NPR, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

17 Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *Washington Post*, February 27, 2024, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

18 David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *New York Times*, March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html.

19 Ellen Nakashima, "Trump Approved Cyber-Strikes against Iranian Computer Database Used to Plan Attacks on Oil Tankers," *Washington Post*, June 22, 2019, https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.

20 Sanger and Perlroth, "U.S. Escalates Online Attacks."

21 Ellen Nakashima, "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *Washington Post*, September 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

22 Sanger and Perlroth, "U.S. Escalates Online Attacks."

23 Ibid.

24 Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92, no. 1 (2019): 10–14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

25 Ibid.

26 Interview with retired U.S. Army colonel George Corbari, June 22, 2024.

27 IISS, *Cyber Capabilities*, 8.

28 Ibid., 9.

29 NATO, *NATO Standard AJP-3.20: Allied Joint Doctrine for Cyberspace Operations* (Brussels: NATO Standardization Office, January 2020). https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

30 IISS, *Cyber Capabilities*, 2.

31 CISA, "CISA Releases 2023 Year in Review."

32 "Water and Wastewater Systems," CISA, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector; Elena H. Humphreys and Mary Tiemann, "Safe Drinking Water Act (SDWA): Draft Amendment Authorizing Voluntary Water Partnerships and Related SDWA Compliance Development Provisions," Congressional Research Service, memorandum, July 17, 2020, https://www.duckworth.senate.gov/imo/media/doc/Voluntary%20Water%20Partnerships%20for%20Distressed%20Communities%20Act%20Congressional%20Research%20Service%20Analysis.pdf; and March Levy, "States and Congress Wrestle with Cybersecurity after Iran Attacks Small Town Water Utilities," AP News, January 2, 2024, https://apnews.com/article/water-utilities-hackers-cybersecurity-1c475f5d2ef3b5d52410c93bdeab3aad.

33 Levy, "States and Congress Wrestle."

34 Ibid.

35 Azadeh Moshiri, "US Sanctions Iranian Officials over Cyber-Attacks on Water Plants," BBC News, February 2, 2024, https://www.bbc.com/news/world-us-canada-68186945.

36 Aamer Madhani, "Top White House Cyber Aide Says Recent Iran Hack on Water System Is Call to Tighten Cybersecurity," AP News, December 8, 2023, https://apnews.com/article/iran-hack-water-biden-anne-neuberger-cybersecurity-51886faab07edb61a4459fde0dabbbac.

37 Levy, "States and Congress Wrestle."

38 Interview with Rex Booth, June 17, 2024.

39 Miranda Bruce et al., "Mapping the Global Geography of Cybercrime with the World Cybercrime Index," *PLOS ONE* 19, no. 4 (April 2024): e0297312, https://doi.org/10.1371/journal.pone.0297312.

40 Joe Tidy, "74% of Ransomware Revenue Goes to Russia-Linked Hackers," BBC, February 14, 2022, https://www.bbc.com/news/technology-60378009; and Chainanalysis Team, "Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-Based Money Laundering Activity," Chainanalysis, February 14, 2022, https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/.

41 Sanger and Perlroth, "U.S. Escalates Online Attacks."

42 Erica D. Lonergan and Shawn W. Lonergan, *Escalation Dynamics in Cyberspace* (Oxford, UK: Oxford

University Press, 2023), 6.

43 Ibid.

44 Interviewee 1, June 22, 2024.

45 Lonergan and Lonergan, *Escalation Dynamics in Cyberspace*; Judy Franko, "NotPetya: The Cyberattack That Shook the World," *Economic Times*, March 4, 2022, https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms?from=mdr.

46 Lonergan and Lonergan, *Escalation Dynamics in Cyberspace*.

47 U.S. Cyberspace Solarium Commission (CSC), *United States of America Cyberspace Solarium Commission Report* (Washington, DC: CSC, March 2020), https://www.solarium.gov/report.

48 Ibid.

49 U.S. Department of Defense, *Department of Defense Cyber Strategy 2018: Summary* (Washington, DC: DOD, 2018), 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

50 Ibid.

51 Interviewee 1, June 22, 2024.

52 "Remarks by President Biden in Press Conference," White House, June 16, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/16/remarks-by-president-biden-in-press-conference-4/.

53 Stephanie Pendino, Robert K. Jahn Sr., and Kirk Pedersen, "U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light," *Campaigning: The Journal of the Joint Forces Staff College*, September 7, 2022, 3, https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/; and Vladimir Soldatkin and Humeyra Pamuk, "Biden Tells Putin Certain Cyberattacks Should Be 'Off-Limits'," Reuters, June 16, 2021, https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/.

54 Soldatkin and Pamuk, "Biden Tells Putin."

55 "Significant Cyber Incidents," CSIS.

56 Interviewee 1, June 22, 2024.

57 Ibid.

58 U.S. Department of Defense, *2023 Cyber Strategy of the Department of Defense: Summary* (Washington, DC: DOD, September 2023), https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

59 U.S. Air Force, *Air Force Doctrine Publication 3-12: Cyberspace Operations* (Washington, DC: USAF, February 2023), 7, https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf; and Joint Chiefs of Staff, *Joint Publication 3-12: Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, June 2018), 49, https://irp.fas.org/doddir/dod/jp3_12.pdf.

60 Joint Chiefs of Staff, *Joint Publication 3-12*, 11.

61 Nakashima, "White House Authorizes."

62 Joint Chiefs of Staff, *Joint Publication 3-12*, 50.

63 Catherine A. Theohary, "Defense Primer: Cyberspace Operations," Congressional Research Service, IF10537, updated December 14, 2023, 1, https://crsreports.congress.gov/product/pdf/IF/IF10537/11 (emphasis in original).

64 Ibid.

65 Ibid.

66 Joint Chiefs of Staff, Joint Publication 3-12, 50.

67 Ibid.

68 U.S. Cyber Command Public Affairs, "CYBER 101—Cyber Mission Force," U.S. Cyber Command, November 1, 2022, https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/.

69 "Posture Statement of Gen. Paul M. Nakasone, Commander, U.S. Cyber Command before the 117th Congress," U.S. Cyber Command, April 5, 2022, https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/.

70 Ibid.

71 Theohary, "Defense Primer: Cyberspace Operations."

72 "Cyber Mission Force," U.S. Army Cyber Command, November 14, 2023, https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/2079661/cyber-mission-force/.

73 Joint Chiefs of Staff, *Joint Publication 3-12*, 9; and Andrew J. Schoka, "Prioritizing Strategic Cyberspace Lethality," *Military Cyber Affairs* 4, no. 1 (October 2019): 4, https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1049&context=mca.

74 Joint Chiefs of Staff, Joint Publication 3-12, 29; Erica Lonergan and Mark Montgomery, United States Cyber Force: A Defense Imperative (Washington, DC: Foundation for Defense of Democracies Press, March 2024), https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf; and U.S. Department of Defense, *Department of Defense Cyber Strategy 2018*.

75 Joint Chiefs of Staff, *Joint Publication 3-12*, 29; "Our History," U.S. Cyber Command, accessed December 14, 2023, https://www.cybercom.mil/About/History/; and Lonergan and Montgomery, *United States Cyber Force*.

76 Joint Chiefs of Staff, *Joint Publication 3-12*, 29.

77 Ibid., 30; and Lonergan and Montgomery, *United States Cyber Force*.

78 Joint Chiefs of Staff, *Joint Publication 3-12*, 29; and Lonergan and Montgomery, *United States Cyber Force*.

79 "Our Units," U.S. Army Cyber Command, accessed November 14, 2023, https://www.arcyber.army.mil/Organization/Units/.

80 Joint Chiefs of Staff, *Joint Publication 3-12*, 30.

81 "Our History," U.S. Cyber Command. Additional clarification provided by an interview on background in June 2024.

82 "Our History," U.S. Cyber Command; and Joint Chiefs of Staff, *Joint Publication 3-12*, 3.

83 "Memorandum of Agreement between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations," Department of Defense, January 19, 2017, https://media.defense.gov/2017/

Jul/19/2001780017/-1/-1/0/DHS-DOD%20USCG%20CYBER%20MOA.PDF.

84 Shannon Vavra, "NSA to Establish New Cybersecurity Directorate to Boost Defense," CyberScoop, July 23, 2019, https://cyberscoop.com/nsa-cybersecurity-directorate/.

85 Ibid.

86 Olivia Gazis, "Secretive NSA Opens Doors to New 'Collaboration Center' as Cyberthreats Mount," CBS News, June 23, 2021, https://www.cbsnews.com/news/nsa-cybersecurity-collaboration-center/.

87 Vavra, "NSA to Establish."

88 Shaun Waterman, "NSA Seeks to Reassure on Merging Cyber Defense, Offense," FedScoop, August 16, 2016, https://fedscoop.com/nsa-reorganization-nsa21-august-2016/.

89 Theohary, "Defense Primer: Cyberspace Operations."

90 Joint Chiefs of Staff, Joint Publication 3-12, 29.

91 Office of Strategic Communication and Public Affairs, "DISA Intelligence Director Speaks about Emerging Cybersecurity Threats," Defense Information Systems Agency, March 1, 2024, https://www.disa.mil/NewsandEvents/2024/Digital-Protection-Summit.

92 "DISA's Budget," Defense Information Systems Agency, n.d., https://www.disa.mil/about/our-work/budget.

93 Interviewee 1, June 22, 2024.

94 The White House, *A Strategic Intent Statement for the Office of the National Cyber Director* (Washington, DC: October 2021), 8, https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf.

95 Ibid.

96 Matt Kapko, "Senate Confirms Harry Coker Jr. as National Cyber Director," Cybersecurity Dive, December 13, 2023, https://www.cybersecuritydive.com/news/senate-confirms-harry-coker-national-cyber-director/702395/.

97 Justin Doubleday, "Federal Efforts on Critical Infrastructure Cybersecurity Come under White House Review," Federal News Network, April 1, 2022, https://federalnewsnetwork.com/cybersecurity/2022/04/federal-efforts-on-critical-infrastructure-cybersecurity-come-under-white-house-review/; and Sam Sabin, "The National Cyber Director's First Hurdles," *Politico*, June 21, 2021, https://www.politico.com/newsletters/weekly-cybersecurity/2021/06/21/the-national-cyber-directors-first-hurdles-796031.

98 "Joint Statement on Advancing Responsible State Behavior in Cyberspace," U.S. Department of State, September 23, 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

99 "Cyber Issues," U.S. Department of State, https://www.state.gov/policy-issues/cyber-issues/; "Cybersecurity," U.S. Department of State, https://www.state.gov/cybersecurity/; "About Us," Bureau of Diplomatic Technology, U.S. Department of State, https://www.state.gov/about-us-bureau-of-diplomatic-technology/; and U.S. Government Accountability Office (GAO), *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities*, GAO-24-105563 (Washington, DC: GAO, January 2024), https://www.gao.gov/assets/d24105563.pdf.

100 "Bureau of Cyberspace and Digital Policy," U.S. Department of State, https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/.

101 Gregory D. Hillebrand and Bill Ault, *Strategic Cyberspace Operations Primer* (Philadelphia, PA: U.S.

Army War College, December 2023), https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf.

102 Ibid.

103 "Bureau of Cyberspace and Digital Policy: About Us," U.S. Department of State, https://www.state.gov/about-us-bureau-of-cyberspace-and-digital-policy/.

104 Ibid.

105 Ibid.

106 GAO, *Cyber Diplomacy*.

107 Ibid.

108 Ibid.

109 Edward Graham, "State's Cyber Bureau Has 'Raised the U.S. Profile on Cyber Globally,' Watchdog Says," Nextgov/FCW, January 12, 2024, https://www.nextgov.com/cybersecurity/2024/01/states-cyber-bureau-has-raised-us-profile-cyber-globally-watchdog-says/393336/.

110 Ibid.

111 Nathaniel Fink, "Statement for the Record Nathaniel Fick Ambassador at Large for Cyberspace and Digital Policy House Foreign Affairs Subcomm. on Indo-Pacific," 118th Cong., 2nd sess., January 17, 2024, https://www.congress.gov/118/meeting/house/116740/witnesses/HHRG-118-FA05-Wstate-FickN-20240117.pdf.

112 Ibid.

113 E. B. Boyd, "Meet Nate Fick, the State Department's First-Ever Ambassador for Cyberspace," Fast Company, April 30, 2023, https://www.fastcompany.com/90888898/nate-fick-state-department-first-ambassador-cyberspace.

114 Nathaniel Fink, "Statement for the Record Nathaniel Fick."

115 "Office of the Special Envoy for Critical and Emerging Technology," U.S. Department of State, https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-special-envoy-for-critical-and-emerging-technology/.

116 "Cybersecurity," U.S. Department of State.

117 Ibid.

118 Kimberly Underwood, "The State Department Improves Its Cyber State," AFCEA, Cyber Edge, June 29, 2023, https://www.afcea.org/signal-media/cyber-edge/state-department-improves-its-cyber-state.

119 "About Us," Bureau of Information Resource Management, https://2017-2021.state.gov/about-us-bureau-of-information-resource-management/.

120 Interview with Laura Galante, Director of CTIIC, August 21, 2024.

121 "Cyber Threat Intelligence Integration Center," Office of the Director of National Intelligence (ODNI), https://www.dni.gov/index.php/ctiic-home.

122 Interview with Laura Galante, Director of CTIIC, August 21, 2024.

123 Ibid.

124 Ibid.

125 "Cyber Threat Intelligence Integration Center," ODNI.

126 "Organization," Cyber Threat Intelligence Integration Center (CTIIC), https://www.dni.gov/index.php/ctiic-who-we-are/ctiic-organization.

127 Interview with Laura Galante, Director of CTIIC, August 21, 2024.

128 "CTIIC Products," CTIIC, https://www.dni.gov/index.php/ctiic-what-we-do/ctiic-products; and CTIIC, *North Korean Tactics, Techniques, and Procedures for Revenue Generation* (Washington, DC: ODNI, July 2023), https://www.dni.gov/files/CTIIC/documents/products/North-Korean-TTPs-for-Revenue-Generation.pdf.

129 Interview with Laura Galante, Director of CTIIC, August 21, 2024.

130 "About CIA—Organization," Central Intelligence Agency, https://www.cia.gov/about/organization/#directorate-of-digital-innovation.

131 "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says," Federal Bureau of Investigation (FBI), April 18, 2024, https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says.

132 Nathaniel Fink, "Statement for the Record Nathaniel Fick"; and Scott S. Smith, "Roles and Responsibilities for Defending the Nation from Cyber Attack: Statement for the Record Before the Senate Armed Services Committee," 115th Cong., 1st sess., October 19, 2017, https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities.

133 FBI, "Brian C. Turner Named Executive Assistant Director of the Criminal, Cyber, Response, and Services Branch," press release, May 7, 2021, https://www.fbi.gov/news/press-releases/brian-c-turner-named-executive-assistant-director-of-the-criminal-cyber-response-and-services-branch.

134 Natalie K. Orpett et al., "The Lawfare Podcast: How the FBI Is Combating Cyberattacks, with Brett Leatherman," *Lawfare*, March 28, 2024, https://www.lawfaremedia.org/article/the-lawfare-podcast-how-the-fbi-is-combating-cyberattacks-with-brett-leatherman.

135 Brett Leatherman, "FBI Cyber Deputy Assistant Director Brett Leatherman's Remarks at Press Conference Announcing the Disruption of the LockBit Ransomware Group," FBI, February 20, 2024, https://www.fbi.gov/news/speeches/fbi-cyber-deputy-assistant-director-brett-leathermans-remarks-at-press-conference-announcing-the-disruption-of-the-lockbit-ransomware-group; and FBI, "Operation Endgame: Coordinated Worldwide Law Enforcement Action against Network of Cybercriminals," press release, May 30, 2024, https://www.fbi.gov/news/press-releases/operation-endgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals.

136 "The Cyber Action Team: Rapidly Responding to Major Computer Intrusions," FBI, March 4, 2015, https://www.fbi.gov/news/stories/the-cyber-action-team.

137 Smith, "Roles and Responsibilities."

138 "The Cyber Threat," FBI, https://www.fbi.gov/investigate/cyber.

139 "The Cyber Action Team," FBI.

140 "The Cyber Threat," FBI; "National Cyber Investigative Joint Task Force," FBI, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force; and Orpett et. al., "The Lawfare Podcast."

141 Smith, "Roles and Responsibilities"; and "The Cyber Threat," FBI.

142 Smith, "Roles and Responsibilities."

143 Europol, "Cybercriminal Darkode forum taken down through global action," press release, July 15, 2015,

https://www.europol.europa.eu/media-press/newsroom/news/cybercriminal-darkode-forum-taken-down-through-global-action; "National Cyber Security Awareness Month FBI Deploys Cyber Experts to Work Directly with Foreign Partners," FBI, October 26, 2016, https://www.fbi.gov/news/stories/fbi-deploys-cyber-experts-to-work-directly-with-foreign-partners; AJ Vicens, "The FBI is adding more cyber-focused agents to U.S. embassies," CyberScoop, January 3, 2024, https://cyberscoop.com/the-fbi-is-adding-more-cyber-focused-agents-to-u-s-embassies/; Europol, "Takedown of notorious hacker marketplace selling your identity to criminals," press release, April 5, 2023, https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals; and Eva Nagyfejeo, "Transatlantic Collaboration in Response to Cyber Crime" (master's thesis, University of Warwick, 2016), https://wrap.warwick.ac.uk/id/eprint/89818/1/WRAP_Theses_Nagyfejeo_2016.pdf.

144 Bryan A. Vorndan, "Oversight of the FBI Cyber Division: Statement Before the House Judiciary Comm.," 117th Cong., 2nd sess., March 29, 2022, https://www.fbi.gov/news/testimony/oversight-of-the-fbi-cyber-division-032922.

145 "About CISA," CISA, https://www.cisa.gov/about.

146 "Divisions & Offices," CISA, https://www.cisa.gov/about/divisions-offices.

147 "Cybersecurity Division," CISA, https://www.cisa.gov/about/divisions-offices/cybersecurity-division.

148 "Capacity Building," CISA, https://www.cisa.gov/about/divisions-offices/cybersecurity-division/capacity-building.

149 "Mission Engineering," CISA, https://www.cisa.gov/mission-engineering.

150 "Extending the Breadth and Depth of our Partnerships- JCDC 2024 Priorities," CISA, February 12, 2024, https://www.cisa.gov/news-events/news/extending-breadth-and-depth-our-partnerships-jcdc-2024-priorities; Eric Goldstein, "Mobilizing Our Cyber Defenses: Maturing Public-Private Partnerships to Secure U.S. Critical Infrastructure: Testimony Before the U.S. House of Representatives Comm. on Homeland Security Subcomm. on Cybersecurity, Infrastructure Protection & Innovation," 117th Cong., 2nd sess., April 6, 2022, https://www.congress.gov/117/meeting/house/114611/witnesses/HHRG-117-HM08-Bio-GoldsteinE-20220406.pdf.

151 "Vulnerability Management," CISA, https://www.cisa.gov/vulnerability-management; and "Infrastructure Security Division," CISA, https://www.cisa.gov/about/divisions-offices/infrastructure-security-division.

152 "Threat Hunting," CISA, https://www.cisa.gov/threat-hunting.

153 Cate Burgan, "Feds: CISA's JCDC Promising, but Still in 'Infantile State'," MeriTalk, February 7, 2024, https://www.meritalk.com/articles/feds-cisas-jcdc-promising-but-still-in-infantile-state/; and Benjamin Jensen et al., "Shaping the Future of Federal Cybersecurity: Insights from FCEBs," (public event, CSIS, Washington, DC, February 6, 2024), https://www.csis.org/events/shaping-future-federal-cybersecurity-insights-fcebs. Separate from the Cybersecurity Division (CSD), CISA's Infrastructure Security Division (ISD) conducts vulnerability assessments on critical infrastructure systems and "provides information on emerging threats and . . . training to help partners in government and industry manage risks to their assets, systems, and networks." "Infrastructure Security Division," CISA. More specifically, ISD is charged with protecting 16 critical sectors identified by CISA: chemicals; commercial facilities; communications; critical manufacturing; dams; the defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater sectors. However, as the U.S. system of cyber defenses continues to evolve, some question whether or not ISD belongs within CISA.

154 CISA, "CISA Releases 2023 Year in Review."

155 "Extending the Breadth and Depth of our Partnerships- JCDC 2024 Priorities," CISA, February 12, 2024, https://www.cisa.gov/news-events/news/extending-breadth-and-depth-our-partnerships-jcdc-2024-priorities.

156 Goldstein, "Mobilizing Our Cyber Defenses."

157 "JCDC FAQs," CISA, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-faqs (italics in the original).

158 Interview with JCDC, Clayton Romans, August 27, 2024.

159 Ibid.

160 Ibid.

161 Jensen et al., "Shaping the Future."

162 Burgan, "Feds: CISA's JCDC Promising."

163 "JCDC Success Stories," CISA, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-success-stories.

164 Eric M. Swalwell, "CISA 2025: The State of American Cybersecurity from CISA's Perspective: Hearing Before the Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection," 118th Cong., 1st sess., April 27, 2023, https://www.congress.gov/event/118th-congress/house-event/115820/text?s=1&r=58.

165 Ibid.

166 "CISA Expands the Joint Cyber Defense Collaborative to include Industrial Control Systems Industry Expertise," CISA, April 20, 2022, https://www.cisa.gov/news-events/news/cisa-expands-joint-cyber-defense-collaborative-include-industrial-control-systems.

167 Brian Fung, "We Finally Know What Caused the Global Tech Outage - and How Much It Cost," CNN, July 7, 2024, https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html.

168 James Andrew Lewis, "Blackout Scorecard," CSIS, *Commentary*, July 25, 2024, https://www.csis.org/analysis/blackout-scorecard.

169 Dina Temple-Raston, "How the U.S. Hacked ISIS," NPR, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

170 Ibid.

171 Ibid.

172 Michael Martelle, ed., "USCYBERCOM after Action Assessments of Operation GLOWING SYMPHONY," National Security Archive, January 21, 2020, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony.

173 Temple-Raston, "How the U.S. Hacked ISIS."

174 Ellen Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies," *Washington Post*, May 9, 2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html.

175 Martelle, "USCYBERCOM after Action Assessments."

176 Stephanie Borys, "Australian Cyber Soldiers Hacked Islamic State and Crippled Its Propaganda Unit–

Here's What We Know," ABC News, December 17, 2019, https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426.

177 Temple-Raston, "How the U.S. Hacked ISIS."

178 "USCYBERCOM, USCYBERCOM 30-Day Assessment of Operation Glowing Symphony, December 13, 2016. Top Secret," National Security Archive, December 13, 2016, https://nsarchive.gwu.edu/document/19821-national-security-archive-5-uscybercom.

179 Ibid.

180 Temple-Raston, "How the U.S. Hacked ISIS."

181 Interviewee 1, June 22, 2024.

182 Martelle, "USCYBERCOM after Action Assessments."

183 Nakashima, "U.S. Military Cyber Operation."

184 Ibid.

185 Temple-Raston, "How the U.S. Hacked ISIS."

186 Martelle, "USCYBERCOM after Action Assessments."

187 Ibid.

188 "USCYBERCOM, Operation Glowing Symphony J3 AAR Observations, November 22, 2016. Top Secret," National Security Archive, November 22, 2016, https://nsarchive.gwu.edu/document/19820-national-security-archive-4-uscybercom-operation.

189 Martelle, "USCYBERCOM after Action Assessments."

190 "USCYBERCOM 30-Day Assessment," National Security Archive.

191 Ibid.

192 Ibid.

193 Interviewee 1, June 22, 2024.

194 "USCYBERCOM 30-Day Assessment," National Security Archive.

195 Temple-Raston, "How the U.S. Hacked ISIS."

196 IISS, *Cyber Capabilities*, 23.

197 Ibid., 22.

198 Interview with retired U.S. Army colonel George Corbari, June 22, 2024.

COVER PHOTO LEENA MARTE/CSIS; MOCKO/ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**