

# The Cyber Gap

## How to Counter China's Threat to America's Critical Networks

Matthew Ferren, Adam Segal, and Rush Doshi

September 2026



## Executive Summary

Over the past decade, China has built a sophisticated hacking apparatus to penetrate the water systems, energy grids, telecommunications networks, and transportation systems that underpin American society. The goal is not simply espionage. China is pre-positioning malware and maintaining dormant access to critical systems so it can gain leverage in peacetime and wreak havoc during a conflict.

The United States has failed to meet this threat. Its networks have been left exposed thanks to poorly secured hardware and software, chronic underinvestment in infrastructure modernization, and unsteady government policy. U.S. efforts to deter China's cyberattacks have not changed its behavior. The U.S. government's offensive cyber operations have disrupted individual Chinese campaigns but have not meaningfully degraded Beijing's capacity. The result is a widening asymmetry: China can threaten systems the United States depends on to fight, govern, and function, while Washington lacks the defenses or the credible deterrent to change that calculus.

The emergence of artificial intelligence (AI) models with advanced coding and cybersecurity capabilities has injected new urgency into this competition. These tools can now find and exploit software vulnerabilities faster than defenders can patch them. They can also harden that same software at scale. The United States currently leads China in AI capabilities, but only by months.

Countering China's digital threat requires a strategy built on four pillars. The first is building shared visibility into Chinese campaigns. The United States and its private-sector partners have limited insight into the scope and methods of Chinese cyber activity. To give defenders a clearer picture of the threat, Washington needs to mandate information sharing by major technology providers, deploy sensors on the technical systems that control vital physical infrastructure, and establish a national system for real-time threat information sharing.

The second pillar is imposing costs on Chinese operations. The United States needs to prioritize offensive cyber operations against Chinese campaigns and their supporting infrastructure and scale

court-authorized takedowns of Chinese networks. It also needs to develop credible options for raising the price of continued aggression, including sanctions, export controls, and coordinated allied measures.

The third pillar is enhancing resilience. The United States should make its networks easier and cheaper to defend by holding technology vendors liable for shipping insecure products, using AI-enabled tools to harden software before adversaries have the chance to exploit it, and establishing mandatory cybersecurity baselines for critical sectors backed by meaningful enforcement.

The fourth pillar is rebuilding federal capacity. None of the other measures can succeed if the government cannot execute them. Restoring, and eventually expanding, that capacity is a prerequisite for any coherent cyber strategy.

Even if they are fully implemented, those measures will not make U.S. networks impenetrable. China, a determined adversary with ample resources and patience, will continue to find ways in. But with sustained effort, the United States can make itself a far costlier target, ensure that individual intrusions no longer cascade across thousands of downstream victims, and deny China leverage over American decision-making.

## **Introduction**

U.S. infrastructure has never been at greater risk. The water treatment facilities, gas pipelines, power installations, telecommunications networks, and transportation nodes that underpin the United States' society and economy are under digital siege. The country will court disaster if it does not reverse this trend—and the window to do so is shrinking.

Two factors are responsible for this situation. The first is China. Over the past decade, China has built a cyber apparatus whose sophistication, scale, and strategic alignment rivals that of the United States. Although China's economic and political espionage campaigns remain an enduring challenge, its

growing capacity and willingness to compromise civilian critical infrastructure at scale represents a new and particularly dangerous threat.

The second factor is U.S. neglect. Despite decades of effort, American technology remains defined by its vulnerability to cyber intrusions. The failure is a shared one between the private and public sectors, and its roots lie in widely used yet poorly secured hardware and software products, deficient cybersecurity practices, underinvestment in information technology (IT) modernization across critical infrastructure, and the lack of a clear national strategy for addressing the threat.

The result is a fundamental asymmetry in cyberspace. China is willing and able to threaten U.S. interests, while the United States has neither raised its defenses nor threatened credible consequences that could change China's calculus. If the United States fails to close this gap, then this asymmetry threatens to limit its ability to innovate and compete economically, support allies in times of need, and project power abroad.

The emergence of artificial intelligence (AI) models with advanced cyber capabilities has turbocharged the policy debate on cyber risk and could shift the balance of power in cyberspace. These models can automate and accelerate the exploitation of software vulnerabilities and, in the hands of bad actors, could exacerbate the cyber threat facing the United States. But by the same token, defenders could use AI tools to harden that same software against compromise and, over the long term, reverse some of the underlying dynamics that currently serve the offense.

China's practice of "pre-positioning" on U.S. critical infrastructure, exemplified by the Volt Typhoon campaign, presents a particularly serious threat to U.S. interests. Chinese actors have gained and maintained surreptitious access to water utilities, energy systems, transportation networks, and other civilian infrastructure in the United States and throughout the Indo-Pacific. Once inside these networks, Chinese actors maneuver to key locations and disguise their footholds. The ostensible purpose of this access is not to gain economic advantage or collect intelligence but to preserve the capacity to disrupt critical systems in the future.<sup>1</sup>

The United States needs a new strategy to reduce China's leverage in cyberspace. This starts with improving visibility into Chinese campaigns and developing new tools for disrupting them. Sustaining friction on Chinese operations will erode Beijing's confidence in its ability to leverage them. Accomplishing that, in turn, should give the United States the time needed to address the most critical vulnerabilities afflicting its critical infrastructure. Those measures are designed to make U.S. networks easier to defend and reduce the real-world harm of cyberattacks. Closing the asymmetry in cyberspace will demand bold leadership and hard choices to reverse decades-long structural trends.

### **China's Cyber Evolution**

In 2013, disclosures from the National Security Agency (NSA) contractor Edward Snowden revealed to China how advanced U.S. cyber capabilities had become and how far behind it had fallen. In the decade that followed, Chinese leader Xi Jinping launched a campaign to overhaul China's cyber capabilities and close the gap with the United States. Xi's goal, as he put it, was to move China from a big-internet country to a "cyber superpower."<sup>2</sup>

Beijing focused first on strengthening its own defenses. Chinese officials created new institutions such as the Cyberspace Administration of China and new cybersecurity regimes through the national cybersecurity law, data security law, and personal information protection law. The Great Firewall, an interlocked system of legal and technological censorship and surveillance, allowed Chinese security services to control and monitor traffic into and out of the country.<sup>3</sup> Designed as a tool of population control, it also provided significant security benefits, making Chinese networks difficult to penetrate.

At the same time, Beijing expanded and reorganized both military and security service cyber units to improve its offensive capabilities. It also cultivated a network of private technology firms, state-sponsored research institutions, and academic talent who further augmented the scale of China's cyber apparatus.

Initially, this ecosystem was known for its relatively noisy and unsophisticated activity that defenders could readily detect and disrupt. But over time, Chinese operators have become increasingly adept at mounting stealthy, persistent campaigns. Their operations now regularly employ “living-off-the-land” techniques that use native, preinstalled software on the victim’s machine in lieu of custom, easier-to-detect malware, and use botnets of compromised devices in third countries to hide their malicious activity within legitimate network traffic.<sup>4</sup> According to the cybersecurity firm CrowdStrike, China-based activity increased by 38 percent from 2025 to 2026, and in several cases, newly discovered vulnerabilities were weaponized within days of their public release.<sup>5</sup> China’s cyber ecosystem has developed a mature pipeline for acquiring and weaponizing “zero-day” software vulnerabilities—flaws unknown to the vendor and thus unpatched at the time of discovery—further underscoring its technical and structural maturity.<sup>6</sup>

Today, China is a peer competitor of the United States in cyberspace. In the words of Anne Keast-Butler, director of Britain’s signals intelligence agency, Government Communications Headquarters, “China is now a science and tech superpower with sophisticated capabilities across their intelligence, cyber and military agencies.”<sup>7</sup> Its strong defenses at home are now complemented by a mature offensive cyber program built on a vast ecosystem of state intelligence services, military cyber units, and private-sector contractors and researchers.<sup>8</sup> This apparatus extends Beijing’s operational reach, complicates attribution, and makes its cyber program resilient to disruption.

Chinese cyber operations serve overlapping and mutually reinforcing strategic objectives: economic advantage through intellectual property theft and industrial espionage, intelligence collection against foreign leaders and institutions, and coercive leverage through pre-positioning on civilian infrastructure worldwide.

The sustained theft of intellectual property and proprietary research amounts to an ongoing transfer of American competitive advantage to Chinese firms and state institutions. Chinese economic espionage has continued for over a decade, targeting the U.S. technological advantage in sectors such as

pharmaceutical research, semiconductor designs, aerospace technology, and advanced large language models (LLMs).<sup>9</sup> This theft is a persistent drag on U.S. economic competitiveness that continues today.

In 2024, cybersecurity officials and media discovered Salt Typhoon, a sprawling compromise of global telecommunications networks that demonstrated just how much Beijing's cyber-enabled espionage capabilities had matured. Attributed to the Ministry of State Security, the campaign compromised at least nine major U.S. carriers, exposed communications involving millions of Americans, and accessed lawful-intercept systems used for court-authorized surveillance.<sup>10</sup> The compromise gave Chinese intelligence services access to communications among American political and national security leaders, including presidential candidate Donald Trump, vice presidential candidate JD Vance, and presidential candidate Kamala Harris during the 2024 campaign.<sup>11</sup> This collection may still be ongoing and provides Beijing with a level of intelligence that experts may not fully understand for years.

The most urgent dimension of China's threat is the practice of pre-positioning. Pre-positioned access provides China with leverage across the spectrum of competition. During a war, disrupting essential services could cause societal turmoil and reduce leaders' room to maneuver. Degrading military networks and enabling infrastructure would hinder the U.S. military's ability to project power and coordinate with allies. In scenarios short of conflict, pre-positioned accesses give China options to escalate in deniable and reversible ways. And in peacetime, the latent threat of disruption gives China a bargaining chip it can exploit across the bilateral relationship, while the ambiguity of pre-positioning complicates the response of U.S. decision-makers.

## **How the United States Fell Behind**

The United States still possesses formidable cyber power, but its capabilities do not confer strategic advantage in the way that China's do. They have not deterred Chinese cyber activity, consistently disrupted adversary campaigns, or protected U.S. critical infrastructure at scale. Today, the United States

suffers from an accumulation of structural vulnerabilities, misaligned economic incentives, and policy shortfalls that have left U.S. networks vulnerable.

The technology products and services available to American customers are not routinely secure. Vendors ship hardware and software with insecure default settings and unpatched vulnerabilities. Legacy systems running outdated firmware remain embedded in operational environments for decades, long after their developers have stopped supporting them. Competitive pressure rewards speed-to-market over security, imposes few penalties for vulnerability-ridden products, and leaves buyers without the information needed to demand more secure products. The result is a shared digital terrain that is inherently vulnerable and difficult to defend.

Cybersecurity capacity across U.S. critical infrastructure varies widely, and defensive practices are inconsistent. Well-resourced actors in sectors with established regulatory frameworks, such as large companies in the financial services and energy sectors, have made measurable progress toward cyber resilience. But many other operators fail to implement even basic cybersecurity practices. In water delivery, health care, and transportation, operators have not implemented best practices, such as multifactor authentication, timely patching, appropriate access management, and segmentation between IT and operational technology (OT) networks.

Government policy has not addressed the underlying causes of these structural weaknesses. Instead, the U.S. defensive approach has largely relied on voluntary compliance with nonbinding cybersecurity guidelines and public-private partnerships for sharing threat information, while refusing to impose rules on the tech companies whose actions determine systemic risk. Past efforts to hold software developers liable for defects in their products or establish cybersecurity requirements for critical infrastructure failed because they lacked political support and a sustained focus on implementation. Consequently, decision-makers have accepted poor cybersecurity as an enduring aspect of the U.S. technology landscape and prefer defense through offense—stopping threats before they reach U.S. networks—rather than making costly investments in security.

Sporadic attempts to deter Chinese cyberattacks have failed. A 2015 diplomatic agreement between Xi and U.S. President Barack Obama resulted in a temporary decline in Chinese commercial cyber espionage.<sup>12</sup> But as political pressure decreased, Beijing resumed its spying.<sup>13</sup> More recently, the United States has sanctioned and indicted individual Chinese hackers; publicly identified China as behind specific cyber campaigns, alone and with allies; and warned Chinese leaders at the highest levels that pre-positioning would carry consequences. Across administrations, however, the United States has not consistently communicated which categories of cyber activity it considers most dangerous and what specific consequences would follow, or backed those signals with credible consequences. Consequently, Chinese conduct has not changed.

Policymakers have also tried to use the United States' formidable cyber power to disrupt Chinese campaigns. The *2018 Defense Cyber Strategy* directed U.S. cyber forces to seize the initiative in cyberspace by proactively disrupting adversary infrastructure and campaigns before an attack on U.S. networks could be launched.<sup>14</sup> This approach has worked against criminal groups and terrorist networks, but it has not degraded China's ability to mount sophisticated campaigns at scale.<sup>15</sup> Nonetheless, *President Trump's Cyber Strategy for America* (2026) centers U.S. strategy on cyber offense, stating that greater AI use and private-sector enablers will facilitate a level of operational reach to counter adversary campaigns.<sup>16</sup>

Perhaps the central failure of American cyber policy has been an inability to commit to any approach long enough for it to work. Policy has cycled among deterrence, defense, and offense without settling on a coherent framework or priorities across administrations. Within the executive branch, responsibilities are scattered across agencies with conflicting missions, competing interests, and unclear authorities. Individual initiatives launch with urgency, lose political attention, and are overtaken by the next crisis before they produce results. U.S. policymakers have treated cyberspace as an isolated technical domain rather than integrating it into industrial, trade, foreign, and military policy as part of the broader competitive strategy with China. Congress has not passed comprehensive cybersecurity legislation, and oversight is fragmented across dozens of committees.

## The Promise of AI

The emergence of sophisticated LLMs has injected new urgency into the U.S.-China competition. Models such as Anthropic's Mythos and OpenAI's GPT 5.5 contain advanced coding and cybersecurity capabilities and reduce the time, labor, resources, and expertise such activities previously required. Already, these models have found and fixed previously undiscovered vulnerabilities in widely used software. In the hands of adversaries, however, they could enable attackers to exploit vulnerabilities faster than defenders can patch them.

For now, the United States holds an advantage in cutting-edge capabilities over China that is measured in months. This presents an opportunity for the defense community to harden widely used software products at scale, before adversaries acquire and weaponize AI tools.

Though Chinese AI models lag behind American ones, Chinese operators have still found ways to use AI to augment their operations. In November 2025, Anthropic reported that it had discovered a Chinese state-sponsored group using agentic tools to infiltrate thirty global targets. The attack was 80 to 90 percent automated, with humans only intervening in a handful of decision points.<sup>17</sup> The cybersecurity firm Volexity has documented Chinese operators using large language models to target victims, craft phishing emails, and write malicious software.<sup>18</sup> According to a report from the Center for Security and Emerging Technology, the People's Liberation Army (PLA) is also looking for commercial suppliers of AI for various offensive and defensive cyber uses, including intrusion detection and prevention, data collection, network monitoring, and defensive action against discovered vulnerabilities.<sup>19</sup>

China is developing LLMs that will match the capabilities currently available only to the top U.S. AI labs. In June 2026, Chinese start-up Z.ai released an AI model, GLM 5.2, that is particularly good at generating computer code and nearly as powerful as leading U.S. models. In July 2026, the Chinese firm Moonshot released Kimi K3, an open weight model that matches, and in some cases outperforms, OpenAI's and Anthropic's advanced models. As the technological gap narrows and then disappears,

strategic advantage will accrue to the country that can better employ these capabilities widely. The United States has an early lead, but victory is not guaranteed.

To its credit, the Trump administration has recognized the cybersecurity risks and opportunities presented by frontier AI. A June 2026 executive order outlined a framework for accelerating AI use for cyber defense and assessing risks posed by models with advanced cyber capabilities. An accompanying National Security Presidential Memorandum directed the federal government to accelerate adoption of AI capabilities for national security purposes. At the same time, the administration has become embroiled in disputes with Anthropic about the conditions under which a model is too dangerous to release to the public and what restrictions are appropriate for a lab to apply to an AI system employed by the military, heightening uncertainty about the regulatory environment and access to models.<sup>20</sup>

The rapid emergence of AI tools with advanced cyber capabilities has brought new attention to long-standing cybersecurity challenges and could provide significant advantages to defenders. Policymakers, AI labs, and the companies deploying AI systems will need to reach consensus on how to balance these opportunities with the risks of misuse, the need for government to have the final say on national security, and the imperative that U.S. companies remain free to innovate and continue to push the frontier forward.

### **How to Leverage the U.S. Position**

The current trajectory is unsustainable. Changing it will require hard choices, costly investments, and difficult trade-offs. Some measures we recommend will impose new burdens on industry. Others will expand government authorities in ways that demand careful oversight. And some carry real risks of retaliation from Beijing. None will be sufficient on its own, but they are necessary because every year the United States delays structural reform, the asymmetry widens and the range of available responses narrows.

The United States cannot and should not replicate China's approach to cyberspace. Building a centralized surveillance system or imposing state control over the technology ecosystem is incompatible with U.S. law and American values. But the United States does have advantages that China lacks. It is home to the largest technology companies in the world, and these firms lead in AI, cloud computing, and semiconductor design. It boasts numerous alliances, which provide a foundation for coordinated action that China's transactional diplomacy does not. It has a strong economy and the bureaucratic and regulatory tools needed to impose costs on adversaries across domains. Our recommendations are designed to leverage these advantages and are organized around four lines of effort:

- **Build shared visibility into Chinese campaigns.** The U.S. government and American companies have poor visibility into Chinese cyber activity, which undermines U.S. strategic planning and defensive investments. The United States can reverse this trend through deeper integration with private-sector partners, investments in targeted sensing and automated threat sharing, and measures to shield critical infrastructure networks from foreign threats.
- **Impose costs on Chinese operations.** The United States should focus its offensive cyber operations on degrading Chinese campaigns and the enabling infrastructure that sustains them, buying time for structural reforms. At the same time, the United States needs to develop credible economic, diplomatic, and cyber responses to manage competition in cyberspace and shift China's decision calculus.
- **Enhance critical infrastructure resilience.** The United States must make its networks easier and cheaper to defend. That will require shifting the incentives that currently produce insecure technology products and services, restructuring key internet infrastructures not designed for security, and ensuring that AI becomes a tool of enduring defensive advantage. Those measures will in turn make it feasible to establish baseline cybersecurity requirements for critical infrastructure.
- **Rebuild U.S. government capacity.** None of these recommendations is possible without an empowered federal government. Department of Government Efficiency contract terminations and cost-cutting measures hollowed out the agencies most central to cyber defense and compounded structural shortfalls that predate the second Trump administration. The United States needs a

government that can set and implement a clear strategic vision, engage in operational collaboration with every sector, and hire and retain technical experts to fill both civilian and military roles.

### *Pillar One: Build Shared Visibility Into Chinese Campaigns*

The United States lacks the insight into Chinese campaigns necessary to inform disruptive or defensive actions. Volt Typhoon actors maintained access to U.S. critical infrastructure networks for at least five years before public disclosure.<sup>21</sup> Salt Typhoon compromised at least nine U.S. telecommunications providers and reached more than two hundred organizations across roughly eighty countries before the campaign came to light, and it may still have an undetected presence in U.S. networks.<sup>22</sup> This visibility gap is partly the product of improved Chinese tradecraft but is compounded by deficiencies in detection, sharing, and analysis.

Operators are too often unaware of an adversary's presence on or through their networks. In many intrusions, the victims discover they are compromised long after the initial penetration and often after an outside party alerts them. Industrial control systems and consumer-grade edge devices, which are particularly difficult to monitor, have become favored targets of Chinese threat actors seeking to disguise their presence.<sup>23</sup> According to CrowdStrike, 40 percent of vulnerabilities exploited by China-nexus threat actors targeted edge devices.<sup>24</sup>

Infrastructure operators, telecommunications providers, and security vendors frequently have information on Chinese activity that could strengthen collective defense, but the information does not flow to all who need it. The cyber defense ecosystem operates on a hub-and-spoke model in which federal agencies, information sharing and analysis centers (ISACs), and security vendors each sit at the center of their own data flows. This system hinders rapid, broad, and consistent sharing of actionable information. New information-sharing mechanisms such as the Joint Cyber Defense Collaborative of the Cybersecurity and Infrastructure Security Agency (CISA) and the NSA's Cybersecurity Collaboration Center have not fully addressed this challenge.<sup>25</sup>

Divergent incentives further limit sharing. Inside the government, the intelligence community classifies indicators at levels that preclude broad operational use; in the private sector, tactics, techniques, and procedures (TTPs) are treated as proprietary trade secrets and made public selectively through marketing reports or paid feeds. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 is a step in the right direction, but CISA will still implement it as a manual process better suited to post hoc autopsy than real-time defense. And even when individual technical indicators are shared, too rarely are they combined with other data to inform campaign-level analysis. The United States still tends to treat individual intrusions as discrete technical phenomena divorced from broader geostrategic dynamics.

### 1.1 Leverage Commercial Visibility Into Chinese Campaigns

Shared reliance on a handful of technology service providers is often framed as a weakness, but it can be made an asset for cross-sector visibility. The companies that operate shared infrastructure and services have a clearer view into Chinese campaign activity than any government agency could achieve on its own, and they have provided the most significant public disclosures of Chinese cyber campaigns. Fully leveraging their visibility requires creating legal and governance conditions to integrate that data into a coherent nationwide picture.

Congress should impose information-sharing requirements on providers whose infrastructure offers privileged visibility into Chinese campaigns. These include major cloud providers, large internet service providers (ISPs) and backbone carriers, mobile and satellite communications operators, security vendors, and domain name system (DNS) operators. Covered providers should be required to report, on a machine-readable and near-real-time basis, indicators of compromise, attacker infrastructure, observed TTPs, and anomalous traffic patterns transiting their networks. Reporting should flow to a single government entity, which would be responsible for fusing the inputs, declassifying and integrating relevant intelligence-derived indicators, and sharing actionable insights across the defender community.

These obligations should contain three guardrails. The first is a vendor liability shield that protects sharing entities from civil liability arising from data shared in good faith, modeled on protections in the Cybersecurity Information Sharing Act of 2015. Second, there should be a statutory bar on any federal

agencies using shared data for regulatory action. Third, Congress should appropriate matching funding for federal agencies responsible for implementing this program, such as CISA, the FBI, and Department of Defense (DoD).

## 1.2 Deploy Sensors in OT and ICS Environments

OT and industrial control systems (ICS)—the programmable logic controllers, remote terminal units, and supervisory systems that run the physical layer of critical infrastructure—generate little native telemetry and are typically operated by small utilities and authorities without dedicated security staff. As a result, OT and ICS have become ripe targets for pre-positioning. Existing programs to sense and monitor these systems, including CISA’s CyberSentry and the Cybersecurity Risk Information Sharing program of the Department of Energy (DoE), create a foundation for further expansion.<sup>26</sup>

Congress should authorize and fund a cross-sector cyber sensing program to detect Chinese pre-positioning on priority assets in the energy, communications, transportation, and water and wastewater sectors—the four sectors in which Volt Typhoon compromises have been confirmed. The program would fund the installation and integration of passive network sensors at designated assets, capturing indicators of compromise associated with China-attributed activity. A national laboratory would build and operate the infrastructure for transmitting, analyzing, and storing sensor-derived telemetry. CISA, working with the sector risk management agencies (SRMAs), would aggregate the resulting data with commercial information, conduct campaign-level analysis, and provide strategic warning to the defender community.

Because many OT and ICS operators lack the staff to install, maintain, and respond to sensor data, hardware deployment alone will not produce defensive benefit at these sites. The program should therefore pair hardware funding with need-based resourcing for managed security services, executed through state-level cybersecurity programs partnered with the relevant regional-sector ISACs.

Participation should be voluntary for covered entities but subsidized at a level that makes opting in the default choice.

### 1.3 Establish a National Collective Defense System

Today, when one U.S. organization detects Chinese activity, indicators reach other prospective victims through ISAC bulletins, vendor advisories, and government alerts that arrive days or weeks later. The United States needs a system that rapidly turns one defender's discovery into shared defensive outcomes.

Congress should authorize and fund a National Collective Defense System (NCDS), administered by CISA, that would guarantee near-real-time, machine-to-machine dissemination of cyber threat indicators and TTPs to every participating defender. NCDS should be built on top of existing information-sharing infrastructure where possible. Sector ISACs and information-sharing-and-analysis organizations, as well as federal platforms such as the Joint Cyber Defense Collaborative (JCDC), would serve as the distribution channels through which fused indicators reach their members, with CISA acting as the central fusion and routing point for inputs from the commercial reporting regime, OT and ICS sensors, federal collection, and allied partners.

The system should incorporate performance metrics that track dissemination speed, measure where TTPs are being reused, and identify bottlenecks that limit effectiveness. Results should be published to maintain accountability and assess the impact of defensive measures on Chinese campaigns and TTPs. Over time, this platform will dissuade Chinese actors from reusing TTPs and create a national framework for assessing cybersecurity progress.

### 1.4 Establish a Defensive Shield to Block Foreign Threats

A shared view into adversary campaigns creates an opportunity to block those campaigns at the network edge and prevent them from reaching their intended victims. China's Great Firewall, though built for censorship, confers defensive advantages through visibility into cross-border traffic and a centralized mechanism for blocking suspected malicious activities. The United States cannot and should not replicate that model writ large, but the building blocks for a privacy-preserving defensive shield already exist. CISA's protective DNS and the NSA Cybersecurity Collaboration Center's signature-sharing services for the defense industrial base enable threat blocking, but each is voluntary, too narrowly scoped,

or confined to federal networks.<sup>27</sup> Allied efforts, particularly the United Kingdom's Active Cyber Defence program and Israel's Cyber Dome, demonstrate that this approach can scale beyond government to private-sector critical infrastructure within democracies.<sup>28</sup>

Congress and the executive branch should establish a defensive shield available to defense industrial base companies and to operators in a designated set of critical infrastructure sectors, beginning with the four sectors in which Volt Typhoon compromises have been confirmed. Participating entities would route covered traffic through a government-coordinated security layer operated jointly by major U.S. ISPs, backbone providers, and DNS operators. Fully implemented, the shield would combine four capabilities: protective DNS (blocking resolution of known-malicious domains); signature-based intrusion prevention; border gateway protocol-level filtering of adversary infrastructure; and, where appropriate, coordinated takedown of adversary command and control. Of these, protective DNS is the immediate priority and the easiest to scale; CISA's protective DNS service could be extended to covered private-sector entities with limited additional architecture.

### *Pillar Two: Impose Costs on Chinese Operations*

The structural reforms we recommend will take time to implement. In the meantime, Chinese operators will continue to seek access to U.S. networks. A purely defensive approach is insufficient; it cedes initiative and gives Chinese campaigns the time and space to scale. The United States must therefore act on two tracks: disrupting Chinese operations to buy time for defensive investments to take root and developing credible cross-domain options to shape China's calculus when disruption alone is not enough.

Beijing's cyber apparatus is resilient to disruption. State-led campaigns are supplemented by an ecosystem of contractors, university labs, exploit brokers, and infrastructure providers that complicates attribution and enables reconstitution when individual nodes are taken down. China has also hardened its economy against external pressure, built blocking mechanisms to counteract U.S. and allied sanctions,

and developed a sanctions regime of its own. It absorbs disruption, reconstitutes quickly, and has so far withstood U.S. and allied coercive campaigns.

Yet disruptive actions against China's cyber apparatus have still produced real if circumscribed results. Court-authorized takedowns of botnets and enabling infrastructure force Chinese operators into multiday rebuilds. Public attribution and sanctions on companies that support Chinese operations damage their commercial prospects and force state actors to find new enablers. To date, however, many of these actions have been episodic and resource-intensive, conducted by overstretched agencies and private firms with the resources to bear the costs. They would have greater success if they targeted key infrastructure that China cannot easily reconstitute and combined multiple instruments in coordination with allies and the private sector.

## 2.1 Prioritize Offensive Cyber Operations Against the China Threat

Offensive operations force adversaries to rebuild accesses and tools and degrade the infrastructure that enables their campaigns. The Cyber Mission Force (the operational arm of U.S. Cyber Command) and the Cyber National Mission Force (CNMF), a specialized command within that force tasked exclusively with defending the country from cyberattacks, lack the resources to address all cyber threats simultaneously. China, however, is the most consequential cyber adversary and thus warrants explicit prioritization by Cyber Command.

CNMF should concentrate its resources on China, drawing on intelligence, analytic support, and operational experience from the NSA, FBI, CIA, and broader intelligence community. Operations should prioritize measurable degradation of Chinese campaigns and infrastructure and avoid short-lived or symbolic effects. In the short term, this may require reassigning teams within CNMF. In the long term, Congress and the executive branch must work together to fix DoD's force generation model for the cyber domain, which is currently failing to produce skilled operators in sufficient numbers. Cyber Command must be postured to operate across the conflict continuum, including peacetime disruption of Chinese campaigns, crisis response when civilian capacity is overwhelmed, and combat support to the joint force in conflict.

*President Trump's Cyber Strategy for America* (2026) calls for unleashing the private sector to disrupt adversary networks. Private actors operating in adversary networks without statutory backing can create escalation risks and accountability gaps. Congress should pass legislation that would permit private-sector support of offensive operations in specific categories of activity, and would create approval and oversight requirements and reporting mechanisms. The same legislation should authorize and resource a program for the acquisition of exploits and other privately held enabling capabilities that government actors cannot more efficiently produce in-house.

## 2.2 Scale Takedowns of Chinese Infrastructure

Court-authorized takedowns of Chinese command-and-control nodes, botnets, and relay infrastructure have proven effective at disrupting Chinese operations. In December 2023, the FBI executed a court-authorized operation against the KV Botnet, the covert relay network that obscured Volt Typhoon activity, removing malware from hundreds of routers and forcing Chinese operators into a multiday rebuild.<sup>29</sup> The United States paired a similar operation against infrastructure enabling another Chinese campaign with public attribution and sanctions on the company providing technical support.<sup>30</sup>

These activities remain under-resourced and ad hoc, however. Federal law enforcement lacks the funds and workforce to conduct takedowns at scale, and private-sector firms do not have clear and efficient legal pathways to support them.

Congress should authorize and resource the FBI to operate a domestic public-private capability for continuous identification and disruption of infrastructure enabling Chinese cyber operations, pairing government threat intelligence with the visibility and technical reach of major infrastructure operators. Congress should mandate that the Department of Justice (DoJ) develop playbooks and training for U.S. attorney offices, also offering them to the Judicial Branch, to enable expedited judicial review and approval of infrastructure takedown operations that will protect U.S. critical infrastructure; extend liability protections to private-sector partners that participate in these takedowns, including through the reauthorization of the Cybersecurity Information Sharing Act of 2015; and increase funding to federal law enforcement agencies to support sustained takedown operations.

### 2.3 Create Incentives to Fracture the Enabler Ecosystem

China's offensive cyber apparatus depends on a decentralized ecosystem of private contractors, university research labs, vulnerability brokers, exploit developers, infrastructure resellers, and money launderers. Targeted law enforcement measures against these actors can outweigh the financial incentives that currently drive their behavior and impose cumulative costs on Chinese cyber operations. The United States should adopt a deliberate campaign to incentivize defection and exposure from inside that ecosystem.

The State Department should expand and rescope its Rewards for Justice program, with increased rewards for information leading to the identification, disruption, or prosecution of individuals and firms supporting Chinese offensive cyber operations.<sup>31</sup> Rewards should be paired with credible protections for sources, including resettlement and legal status where appropriate. The Treasury and Commerce Departments should publish reward schedules for information that supports designations by the Office of Foreign Assets Control, Entity List additions, or export control enforcement against Chinese cyber-enabling firms. The DoJ should expand whistleblower provisions to cover sanctions evasion and cyber-enabled economic espionage. The intelligence community should execute a campaign against China's enablers, focusing on cultivating sources and gathering intelligence relevant to disruptions.

### 2.4 Build a National Deception Capability

Deception can increase uncertainty and costs for Chinese operations and make U.S. networks a more hostile operating environment. By seeding critical infrastructure networks with realistic but monitored decoys, the United States can generate early warning of adversary presence, collect intelligence on tactics and tooling, and force Chinese operators to expend resources distinguishing real targets from fakes.

The federal government should establish a national deception program that develops adversary-specific decoy personas, data, and infrastructure modeled on Chinese targeting patterns; distributes them to participating critical infrastructure operators and government agencies; and aggregates the intelligence generated across deployments into actionable feedback shared back to the broader operator community.

Congress should fund the program at scale and should extend liability protection to program participants.

## 2.5 Develop Cross-Domain Response Options

*Trump's Cyber Strategy for America* (2026) makes shaping adversary behavior a central objective, but changing Chinese behavior specifically requires credible threats to impose consequences outside of cyberspace. Certain behaviors in cyberspace, such as pre-positioning on civilian critical infrastructure, may be malleable if the United States is willing to make cyber a priority issue in the bilateral relationship. This would require signaling that the most destabilizing categories of Chinese cyber activity carry meaningful consequences for Washington's relationship with Beijing.

The United States must develop options ahead of time to enable policymakers to act flexibly yet decisively in a crisis. NSC staff should build a menu of pre-coordinated cross-domain consequences, such as structural sanctions on Ministry of State Security or PLA entities under an amended Executive Order 13694; secondary sanctions on entities that provide material support to Chinese operations; more restrictive export controls on U.S. advanced technologies; visa restrictions; additional tariffs on imports of Chinese goods; and coordinated allied sanction and trade measures. As Beijing demonstrated with its own rare-earth export regime, and as Washington has shown through its restrictions on semiconductors, the most useful tools of leverage are graduated, reversible, and impose minimal reciprocal costs.

In designing this framework, policymakers will need to determine whether to establish automatic triggers tied to defined categories of activity or to retain flexibility over which consequences to impose in which circumstances. Automatic triggers maximize deterrence value but constrain executive discretion and risk producing disproportionate responses. Flexible options preserve discretion but weaken the signaling effect that gives the framework its deterrent force. Policymakers will also need to decide how to communicate the framework to Beijing, including whether to revise U.S. declaratory policy to make consequences explicit or to suggest them through other channels. Whatever the choices, policymakers must be willing to impose consequences when relevant lines are crossed.

### *Pillar Three: Enhance Critical Infrastructure Resilience*

U.S. critical infrastructure must achieve a baseline level of security and resilience. These systems must be made easier and cheaper to defend, and the consequences of compromise should be minimal.

Vulnerabilities in the shared products and services on which critical infrastructure operators depend are the primary source of systemic cyber risk today. Enterprise software is developed under incentives that reward complex features and time to market over security. Networking hardware carries vulnerabilities for which fixes exist but go unapplied for years. Bad actors easily exploit foundational internet protocols for routing, naming, and identity. As a result, compromises of upstream providers translate directly into access to thousands of downstream customers, and individual outages can quickly cascade into systemic disruptions.

The concentration and shared dependency that creates this collective risk simultaneously presents opportunity. A security fix applied at the right point in the IT stack propagates automatically to every operator who depends on it; the characteristic that makes upstream compromise so devastating makes upstream remediation extraordinarily efficient. Furthermore, U.S. or allied companies hold commanding positions in key technology layers, including cloud computing, software, networking, semiconductors, and AI, which create viable pathways to implement systemic changes.

#### 3.1 Establish a Vendor Liability Regime

Congress should establish a federal civil liability regime for technology vendors. Liability should attach to identified negligent practices such as shipping products with weak default settings, failing to support multifactor authentication, failing to patch known exploited vulnerabilities, or failing to support products through their expected operational lifecycle. Congress should authorize CISA, in coordination with the National Institute of Standards and Technology (NIST), to update the list as best practices evolve.

The regime should apply to all vendors selling into U.S. critical infrastructure, regardless of country of origin. A regime that applies only to domestic vendors would advantage Chinese and other third-

country firms, undercutting domestic vendors without improving security outcomes. Addressing this issue may require new country-of-origin disclosure requirements for hardware and software, as well as additional liability for U.S.-based importers, resellers, or integrators of foreign products.

Ultimately, the details of a liability regime, and indeed whether a regime built on enumerated negligent practices is the right approach, will need to be worked out through the legislative process. Other approaches, such as a strict liability regime or a general standard of care paired with a safe-harbor framework, could also work. Congress will need to address related topics, including the treatment of open-source contributors and the structure of cyber insurance markets that price in residual risk.

### 3.2 Use AI to Drive Security at Scale

AI-driven vulnerability discovery is reshaping the cybersecurity landscape. General-purpose models developed by U.S. labs have demonstrated the ability to autonomously find software vulnerabilities and develop patches.<sup>32</sup> Multiple frontier labs have established controlled access programs to enable key technology providers to use these models to harden their software and, in some cases, have provided discounted access to less well-resourced players to harden open-source projects and publicly owned infrastructure. The AI Cyber Challenge of the Defense Advanced Research Projects Agency (DARPA) focused on developing open-source tools to find vulnerabilities autonomously in widely used software.<sup>33</sup>

In the near term, the federal government, frontier labs, and other private-sector partners should maximize this window of opportunity to harden software used in critical infrastructure. In July, the White House announced the new Gold Eagle initiative, bringing together federal agencies, critical infrastructure operators, and frontier labs to identify and patch vulnerabilities discovered by advanced AI models.<sup>34</sup> These same parties should also collaborate to assess where federal funding would support AI-enabled vulnerability research in OT firmware and widely deployed open-source projects that commercial efforts are unlikely to prioritize, and where public-private collaboration can facilitate managed patching across critical sectors. CISA and SRMAs should facilitate engagement between the AI-enabled vulnerability research ecosystem and operators in their sectors. In ICS applications where patching is difficult or impossible, CISA and SRMAs should coordinate the development of alternative

mitigations such as network segmentation. Although limiting adversary access to U.S. capabilities is important, controlled access programs, export controls, and counter-distillation measures should not be so restrictive as to prevent broad access by the defender community.

The longer-term objective is to shape the evolution of both general-purpose and specialized AI models and tools toward cybersecurity and defensive advantage. This will require sustained investments in areas such as high-fidelity digital twins of OT environments, where defenders can simulate attacks and stress-test defenses without disrupting live systems; a national repository of validated training datasets and baseline models through NIST and the national laboratories to reduce dependence on vendor-proprietary data; and credible evaluation frameworks for AI-enabled cybersecurity tools so that purchasing decisions are based on demonstrated performance. Continued federal investment in open-source AI cyber defense tooling, building on the DARPA model, should be part of this effort.

Decision-makers also need to address structural barriers to cooperation among AI labs on cyber defense. Adversaries are running campaigns across multiple models, and effective detection requires cross-lab sharing that current legal and competitive dynamics discourage.<sup>35</sup> The federal government should provide clear antitrust safe harbors for cooperation on cyber defense, including sharing information, detection signatures, and threat patterns derived from observing adversarial model use.

### 3.3 Establish Mandatory Cybersecurity Baselines

Voluntary approaches to critical infrastructure cybersecurity have failed to produce consistent outcomes necessary for ecosystem-wide resilience. Well-crafted standards give operators clear targets and a baseline level of resilience. Past attempts to institute baselines through executive action using existing authorities faced legal challenges and inconsistent implementation, leaving a patchwork in which some sectors face meaningful requirements while others face essentially none.<sup>36</sup> The executive branch cannot establish durable cybersecurity baselines for critical infrastructure without congressional authorization.

Congress should authorize federal agencies to set minimum, sector-specific cybersecurity baselines for critical infrastructure backed by meaningful enforcement. Requirements should be outcome-oriented,

specifying what operators must achieve rather than prescribing technical controls, and harmonized across sectors to reduce compliance burden while permitting sector-specific implementation where operational differences require. Wherever possible, these requirements should align with international standards to further minimize compliance burdens.

Many critical infrastructure operators, particularly in under-resourced sectors such as water and wastewater, education, and health care, do not have the financial or technical capacity to fully implement baselines. The federal government should pair requirements with targeted assistance, including accessible technical guidance, funding for cybersecurity investments at small and rural operators, and structured cost-recovery mechanisms coordinated with state and other regulators.

### 3.4 Harden Defense Critical Infrastructure

Some critical infrastructure networks are designated as essential to U.S. military operations by DoD through its Defense Critical Infrastructure (DCI) program and the Task Critical Asset and Defense Critical Asset tiers within it.<sup>37</sup> DoD has limited capacity to drive cybersecurity across these assets, however, because they operate outside the defense industrial base.<sup>38</sup> Many are the single utility, port, or fuel terminal serving a strategic location, with no substitute available. Many are owned by small public or rural operators that lack the financial or technical capacity to harden their networks on their own. These assets must be strengthened to a sufficient level of operational resilience.

DoD should use existing authority to update DCI program standards and require designated operators to regularly demonstrate two capabilities. The first should be mandatory manual operation capability sufficient to sustain core functions through adversary disruption, building on existing precedents such as North American Electric Reliability Corporation Critical Infrastructure Protection black-start requirements and DoE's cyber-informed engineering methodology.<sup>39</sup> Second, designated operators should be required to maintain the ability to quickly rebuild OT systems that are taken down.

Congress should appropriate sustained funds for DCI resilience, including federal cost-sharing on hardening investments for privately owned infrastructure. Costs for asset replacement or modernization

can quickly become substantial, and the program should treat cybersecurity investment at DCI-supporting infrastructure as a national defense expenditure. Even with funding and requirements in place, technical and operational resilience cannot be fully guaranteed. Joint operational plans should reflect this uncertainty rather than assume infrastructure will withstand sustained attack.

### 3.5 Mandate Internet Security Measures

Technical fixes for long-standing vulnerabilities in the internet's core routing, naming, and timing protocols have existed for years yet have not been consistently implemented.<sup>40</sup> The federal government should leverage its existing authorities to drive implementation of best practices across the internet ecosystem. The Federal Communications Commission should mandate resource-public-key-infrastructure route origin validation, filtering practices aligned with the recommendations of the Mutually Agreed Norms for Routing Security initiative, and encrypted DNS deployment by major ISPs and backbone operators.<sup>41</sup> CISA should issue binding operational directives requiring these measures across Federal Civilian Executive Branch networks and contractors; NSA should do the same for National Security Systems.

The United States must also actively participate in the organizations that are developing the rules for the next generation of the internet. China has invested heavily in the Internet Engineering Task Force, International Telecommunication Union, and other standards bodies to embed its technologies into global standards and shift internet governance toward a state-centric model.<sup>42</sup> U.S. participation has been inconsistent, uncoordinated, and under-resourced.<sup>43</sup> The federal government should adequately fund and staff sustained U.S. engagement in the standards bodies that shape the routing, naming, and security architectures of the global internet. Specifically, the federal government should reinvest in the State Department's Bureau of Cyberspace and Digital Policy and give it a mandate to manage a strategic increase of U.S. engagement in these bodies, in coordination with the private sector.

### *Pillar Four: Rebuild Government Capacity*

As it stands, the federal government cannot execute the strategy we describe. Part of the problem stems from broad budget and personnel cuts instituted since January 2025. Experts expect total spending on cybersecurity across major federal agencies to drop in fiscal year 2027 by 9.6 percent—to \$11.7 billion.<sup>44</sup> Today, technical billets sit empty across the federal cyber workforce, partnerships with the private sector have paused or contracted, and institutional knowledge has been lost.

Though the damage of the last two years has been severe, it compounds long-standing shortfalls in federal capacity. Restoring head count and appropriations to federal cyber offices is a necessary first step, but countering China's threat to critical infrastructure will require an executive branch that is not just larger and better resourced but also more effective in designing and executing cyber policy and strategy. Congress and the executive branch will need to work together to resolve long-standing structural challenges in how the government defines and executes its cyber priorities. Federal agencies need to improve and standardize the technical support they provide to sectors and deepen their ability to engage in true operational collaboration.

Restoring federal capacity will not prove as directly effective as disrupting Chinese campaigns or hardening critical infrastructure networks, but the other measures we recommend are unlikely to succeed without a capable executive to oversee their implementation. Moreover, sustained competition with China in the cyber domain will require continued policy leadership and innovation and the flexibility to adapt and respond to future challenges.

#### 4.1 Improve White House Coordination

The White House must be able to define strategic cyber priorities, align agency budgets, and drive implementation of complex policy initiatives. The Office of the National Cyber Director (ONCD) was created for that purpose, but it has not been able to establish its role within the interagency process. ONCD is operating without its full complement of staff, and turf battles with the NSC's cyber

directorate have left agencies and external partners unsure which office speaks for the White House on cyber policy.<sup>45</sup>

Congress should direct a review of ONCD to determine where the office has added value, where it has duplicated work done elsewhere, and whether its statutory authorities are sufficient to the coordination role Congress intended. The White House should ensure that ONCD is fully staffed to its statutory ceiling of seventy-five personnel, including technical experts, and it should issue a directive clearly defining ONCD's mandate within the interagency policy process.

## 4.2 Empower CISA

CISA is the national coordinator for critical infrastructure resilience and serves as the SRMA for eight of the sixteen designated critical sectors, but it has struggled to fully realize this broad mandate. Since January 2025, CISA has lost roughly one-third of its workforce through buyouts, budget cuts, and attrition. Organizationally, CISA has become cluttered with divisions, centers, and programs with overlapping responsibilities and unclear lines of authority. Key operational components have yet to fully mature, including the JCDC, which was designed to be CISA's primary operational touchpoint with the private sector, and the National Risk Management Center, tasked with cross-sector risk analysis.

CISA should rebuild its workforce, focusing on restoring technical capacity in cyber defense, incident response, and threat analysis. CISA, in coordination with Congress, should also assess opportunities to streamline its organizational structure to ensure it can perform cross-sector risk analysis, provide operational support to critical infrastructure operators, and establish effective partnership with other SRMAs.

Congress should assess whether CISA may also require regulatory authority to compel protective actions by critical infrastructure operators. When a critical vulnerability or adversary campaign is identified, CISA should have the ability to compel preventive actions by private operators, similar to its binding operational directives for federal civilian agencies. CISA has long resisted this role, worrying it would

compromise its ability to operate as a trusted partner, but other federal agencies house both collaborative and regulatory functions and still retain their ability to engage industry.

#### 4.3 Reform Sector-Specific Collaboration

The federal government must become a more consistently effective operational partner to the nonfederal organizations that operate most U.S. critical infrastructure. Some SRMAs lack the resources, technical staff, or authorities to engage in effective operational collaboration. Congress and the executive branch should reform the SRMA architecture to prioritize such collaboration. SRMAs should be resourced and authorized to recruit technical staff, facilitate regular classified briefings to their sectors, and establish operational connectivity to other federal partners to support crisis response.

CISA and FBI, as the nation's two lead organizations responsible for asset protection and threat response, respectively, should work with SRMAs, the intelligence community, and major operators to develop technical mechanisms to enable rapid, two-way threat information sharing. Years of investment in automated sharing have produced limited operational value because indicator quality is uneven and participation often imposes more cost than benefit on operators. SRMAs should be able to provide their sectors with actionable, machine-readable information to inform real-time defense.

Sector-specific coordinating bodies also vary in effectiveness, ranging from effective, CEO-led bodies to compliance forums dominated by trade associations and lawyers. The Alliance of National Councils for Homeland Operational Resilience—Critical Infrastructure, a new advisory body chartered by the Cybersecurity and Infrastructure Security Agency in June 2026, provides new opportunities to enhance sector-specific and cross-sector coordination on information sharing and collective defense. Participation in those organizations should be elevated to the CEO level across sectors, and the federal government should make clear that participation at this level is the expected standard for operators of nationally significant critical infrastructure.

#### 4.4 Consolidate the Government's Operational Interface

As the federal government engages the private sector for sharing information, coordinating defenses, disrupting adversaries, reporting incidents, and shaping policy and regulation, it does so through a complicated array of agencies, programs, and channels. Companies navigating a serious intrusion routinely face competing demands from agencies with different priorities and no single point of contact authorized to resolve conflicts. This friction slows response and discourages future engagement.

The federal government should consolidate its operational interface with the private sector so that companies have clear, fast, and predictable channels for each type of engagement. A unified incident-reporting platform should serve as the primary submission point for all federally required cyber incident reporting, with reports routed to all agencies with relevant equities. Operational engagement should run through a small number of designated technical interfaces aligned to sector and mission. The NSA Cybersecurity Collaboration Center, which serves as the technical interface between NSA and the defense industrial base, should be authorized and resourced to share information with stakeholders in other sectors.

The Enduring Security Framework, a public-private cross-sector cybersecurity working group cochaired by the NSA and CISA, should be granted its own convening authorities and broadened to include the most significant technology and critical infrastructure providers, including AI laboratories. Its working groups should be tasked against a prioritized list of the most consequential structural and architectural deficiencies in U.S. critical infrastructure, with a mandate to move from analysis to implementation.

#### Conclusion

Over the last decade, China has developed new cyber capabilities that threaten U.S. decision-making, restrict maneuvering room in a crisis, and give Beijing leverage across the bilateral relationship. Policymakers need to recognize that although this threat originates in the cyber domain, its harm

extends across the entire bilateral relationship and warrants a comprehensive, cross-domain response. Every year the United States delays action, Beijing's capacity to shape U.S. choices grows.

Meeting this challenge will require the active engagement of the private sector. The recommendations in this report would impose new burdens on American technology companies: liability for insecure products, mandatory information sharing, and baseline security requirements. But if implemented successfully, they will also produce a more resilient digital landscape where companies can innovate and prosper.

What is required now is coordinated and sustained action to close the cyber gap. The question is whether industry will treat this moment as an opportunity to lead or simply as a regulatory burden to manage.

## Appendix

The following table summarizes each recommendation in this report and identifies the executive branch agencies and congressional committees primarily responsible for implementation.

| <b>Table A1. Recommendations and Responsible Agencies</b>                                                                                                                 |                                                                |                            |                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|----------------------------|---------------------------------------------------------------------|
| The following table summarizes each recommendation in this report and identifies the executive branch agencies or other offices primarily responsible for implementation. |                                                                |                            |                                                                     |
| Number                                                                                                                                                                    | Recommendation                                                 | Lead agency/office         | Supporting agency/office                                            |
| <b>Pillar One: Build Shared Visibility Into Chinese Campaigns</b>                                                                                                         |                                                                |                            |                                                                     |
| 1.1                                                                                                                                                                       | Leverage commercial visibility into Chinese campaigns          | CISA; Congress             | FBI; DoD; intelligence community                                    |
| 1.2                                                                                                                                                                       | Deploy sensors in OT and ICS environments                      | CISA; Congress             | DoE; SRMAs; ISACs                                                   |
| 1.3                                                                                                                                                                       | Establish a national collective defense system                 | CISA (JCDC); Congress      | NSA; FBI; ISACs and ISAOs                                           |
| 1.4                                                                                                                                                                       | Establish a defensive shield to block foreign threats          | CISA; Congress             | Major ISPs; DNS operators                                           |
| <b>Pillar Two: Impose Costs on Chinese Operations</b>                                                                                                                     |                                                                |                            |                                                                     |
| 2.1                                                                                                                                                                       | Prioritize offensive cyber operations against the China threat | DoD (USCYBERCOM); Congress | NSA; CIA; FBI                                                       |
| 2.2                                                                                                                                                                       | Scale takedowns of Chinese infrastructure                      | DoJ/FBI; Congress          | CISA; NSA; private infrastructure operators                         |
| 2.3                                                                                                                                                                       | Create incentives to fracture the enabler ecosystem            | State Department; DoJ      | Treasury (OFAC); Commerce; intelligence community                   |
| 2.4                                                                                                                                                                       | Build a national deception capacity                            | CISA; Congress             | FBI; NSA; private infrastructure operators                          |
| 2.5                                                                                                                                                                       | Develop cross-domain response options                          | NSC                        | State Department; Treasury; Commerce; Congress; allies and partners |

| Pillar Three: Enhance Critical Infrastructure Resilience |                                                    |                                                   |                                                                                   |
|----------------------------------------------------------|----------------------------------------------------|---------------------------------------------------|-----------------------------------------------------------------------------------|
| 3.1                                                      | Establish a vendor liability regime                | Congress; CISA                                    | NIST; FTC; sector regulators; judiciary                                           |
| 3.2                                                      | Use AI to drive security at scale                  | CISA; NIST; Frontier AI labs                      | DOD; Treasury; SRMAs; DoE national labs; Congress                                 |
| 3.3                                                      | Establish mandatory cybersecurity baselines        | Congress; CISA                                    | SRMAs; Sector regulators; NIST                                                    |
| 3.4                                                      | Harden Defense Critical Infrastructure             | DoD; Congress                                     | CISA; SRMAs; critical infrastructure owners                                       |
| 3.5                                                      | Mandate internet security measures                 | FCC; State Department                             | Major ISPs; CISA; NSA                                                             |
| Pillar Four: Rebuild Government Capacity                 |                                                    |                                                   |                                                                                   |
| 4.1                                                      | Improve White House coordination                   | White House/ONCD; Congress                        | NSC; OMB                                                                          |
| 4.2                                                      | Empower CISA                                       | DHS/CISA; Congress                                | OMB; SRMAs; private sector partners                                               |
| 4.3                                                      | Reform sector-specific collaboration               | CISA; SRMAs; Congress                             | FBI; intelligence community; sector-specific and cross-sector coordination bodies |
| 4.4                                                      | Consolidate the government's operational interface | NSA (Collaboration Center); CISA (JCDC); Congress | FBI; DoJ; SRMAs                                                                   |
| cfr                                                      |                                                    |                                                   |                                                                                   |

## Advisory Committee

*China-Cyber Study Group*

Robert Bair

*Anthropic*

Derk Bernsen

*Defense Advanced Research Projects Agency*

Jessica Brandt

*Council on Foreign Relations*

Meredith Burkart

*Halcyon Tech*

Mark Montgomery

*Foundation for Defense of Democracy*

Andrew Scott

*Capital One*

Michael Sulmeyer

*Georgetown University*

Phil Venables

*Ballistic Ventures*

Brandon Wales

*CrowdStrike*

*This report reflects the judgments and recommendations of the authors. It does not necessarily represent the views of members of the advisory committee, whose involvement should in no way be interpreted as an endorsement of the report by either themselves or the organizations with which they are affiliated.*

*The mission of the Council on Foreign Relations is to inform U.S. engagement with the world. Founded in 1921, CFR is a nonpartisan, independent national membership organization, think tank, educator, and publisher, including of Foreign Affairs. It generates policy-relevant ideas and analysis, convenes experts and policymakers, and promotes informed public discussion—all to have impact on the most consequential issues facing the United States and the world.*

*The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.*

## Endnotes

1. Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: ODNI, 2026), <http://dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf>.
2. “Translation: Xi Jinping’s April 20 Speech at the National Cybersecurity and Informatization Work Conference,” DigiChina, Stanford University, April 30, 2018, <http://digichina.stanford.edu/work/translation-xi-jinpings-april-20-speech-at-the-national-cybersecurity-and-informatization-work-conference>.
3. Young Xu, “Deconstructing the Great Firewall of China,” ThousandEyes, March 8, 2016, <http://thousandeyes.com/blog/deconstructing-great-firewall-china>.
4. Cybersecurity and Infrastructure Security Agency, National Security Agency, FBI, et al., “People’s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection,” Joint Cybersecurity Advisory AA23–144A, May 24, 2023, <http://cisa.gov/news-events/cybersecurity-advisories/aa23-144a>.
5. CrowdStrike, “2026 Global Threat Report,” 2026, <http://go.crowdstrike.com/rs/281-OBQ-266/images/Crowdstrike-2026-Global-Threat-Report.pdf>.
6. Winnona DeSombre Bernsen, “Crash (exploit) and Burn: Securing the Offensive Cyber Supply Chain to Counter China in Cyberspace,” Atlantic Council, June 25, 2025, <http://atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn>.
7. Alex Wickham, “UK Spy Chief Warns China Is Closing Cyber Gap With the West,” Bloomberg, May 26, 2026, <http://bloomberg.com/news/articles/2026-05-26/uk-spy-chief-warns-china-is-closing-cyber-gap-with-west>.
8. Nikita Shah, “Why China Is Now a Peer Competitor to the United States in Cyberspace,” Center for Strategic and International Studies, May 15, 2026, <http://csis.org/analysis/why-china-now-peer-competitor-united-states-cyberspace>; Orange Cyberdefense, “The Hidden Network,” CERT Research, <http://research.cert.orangecyberdefense.com/hidden-network/report.html>.
9. U.S.-China Economic and Security Review Commission, “China’s Cyber Capabilities: Warfare Espionage, and Implications for the United States,” Chapter 3, Section 2 in *2022 Annual Report to Congress* (Washington, DC: U.S.-China Economic and Security Review Commission, November 2022), [http://uscc.gov/sites/default/files/2022-11/Chapter\\_3\\_Section\\_2--Chinas\\_Cyber\\_Capabilities.pdf](http://uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf).

10. Cybersecurity and Infrastructure Security Agency, National Security Agency, FBI, et al., “Countering Chinese State-Sponsored Actors’ Compromise of Networks Worldwide to Feed Global Espionage System,” Joint Cybersecurity Advisory AA25–239A, August 27, 2025, <http://cisa.gov/news-events/cybersecurity-advisories/aa25-239a>; “Experts Agree U.S. Communications Networks Remain Vulnerable Following Salt Typhoon Hack,” U.S. Senate Committee on Commerce, Science, and Transportation, December 2, 2025, <http://commerce.senate.gov/press/dem/release/experts-agree-u-s-communications-networks-remain-vulnerable-following-salt-typhoon-hack>; Greg Otto, “FBI: Threats from Salt Typhoon Are ‘Still Very Much Ongoing,’” CyberScoop, February 20, 2026, <http://cyberscoop.com/fbi-salt-typhoon-ongoing-threat-cybertalks-2026>.
11. Devlin Barrett, Jonathan Swan, and Maggie Haberman, “Chinese Hackers Are Said to Have Targeted Phones Used by Trump and Vance,” *New York Times*, October 25, 2024, <http://nytimes.com/2024/10/25/us/politics/trump-vance-hack.html>.
12. White House, Office of the Press Secretary, “Fact Sheet: President Xi Jinping’s State Visit to the United States,” September 25, 2015, <http://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.
13. Adam Segal, “The U.S.-China Cyber Espionage Deal One Year Later,” Council on Foreign Relations, September 28, 2016, <http://cfr.org/articles/us-china-cyber-espionage-deal-one-year-later>; Mara Hvistendahl, “The Decline in Chinese Cyberattacks,” *MIT Technology Review*, October 25, 2016, <http://technologyreview.com/2016/10/25/156465/the-decline-in-chinese-cyberattacks-the-story-behind-the-numbers>.
14. Michael Fischerkeller, Emily Goldman, and Richard Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (Oxford: Oxford University Press, 2022), <http://doi.org/10.1093/oso/9780197638255.001.0001>.
15. Julian Barnes, “U.S. Military Has Acted Against Ransomware Groups, General Acknowledges,” *New York Times*, December 5, 2021, <http://nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html>; “USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY,” National Security Archive, Cyber Vault, January 21, 2020, <http://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscycbercom-after-action-assessments-operation-glowing-symphony>.
16. White House, *President Trump’s Cyber Strategy for America* (March 2026), <http://whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf>.

17. Anthropic, “Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign,” November 13, 2025, <http://anthropic.com/news/disrupting-AI-espionage>.
18. Sam Schechner and Robert McMillan, “Chinese Hackers Used Anthropic AI to Automate Cyberattacks,” *Wall Street Journal*, November 13, 2025, <http://wsj.com/tech/ai/china-hackers-ai-cyberattacks-anthropic-41d7ce76>.
19. Emelia Probasco, Sam Bresnick, and Cole McFaul, “China’s Military AI Wish List: Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance, and Targeting (C5ISRT),” Center for Security and Emerging Technology, February 2026, <http://cset.georgetown.edu/publication/chinas-military-ai-wish-list>.
20. Filip Timotija, “Pentagon Reviewing Anthropic Partnership Over Terms of Use Dispute,” *The Hill*, February 16, 2026, <http://thehill.com/policy/defense/5740369-pentagon-anthropic-relationship-review>; Hadas Gold, “White House Lifts Export Control on Anthropic That Froze Its Most Advanced Models,” CNN, June 30, 2026, <http://cnn.com/2026/06/30/tech/anthropic-export-control-ban-lifted-white-house>.
21. Cybersecurity and Infrastructure Security Agency, “U.S. and International Partners Publish Cybersecurity Advisory on People’s Republic of China State-Sponsored Hacking of Critical Infrastructure,” February 27, 2024, <http://cisa.gov/news-events/news/us-and-international-partners-publish-cybersecurity-advisory-peoples-republic-china-state-sponsored>.
22. Joseph Menn, “FBI Advisory Warns of China Hacking Expansion,” August 27, 2025, <http://washingtonpost.com/technology/2025/08/27/fbi-advisory-china-hacking-expansion>.
23. Cybersecurity and Infrastructure Security Agency, “Edge Device Security,” <http://cisa.gov/topics/cybersecurity-best-practices/edge-device-security>; National Institute of Standards and Technology (NIST), *Guide to Operational Technology (OT) Security*, NIST Special Publication 800–82, Rev. 3 (2023), <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf>.
24. CrowdStrike, *2026 Global Threat Report*, <http://crowdstrike.com/en-us/global-threat-report>.
25. Eric Geller, “CISA’s Joint Cyber Defense Collaborative Takes Major Personnel Hit,” *Cybersecurity Dive*, July 30, 2025, <http://cybersecuritydive.com/news/cisa-joint-cyber-defense-collaborative-contract-lapse/756231>.
26. Cybersecurity and Infrastructure Security Agency, “CyberSentry Program,” <http://cisa.gov/resources-tools/programs/cybersentry-program>; U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, “Energy Sector Cybersecurity Preparedness,” <http://energy.gov/ceser/energy-sector-cybersecurity-preparedness>.

27. Cybersecurity and Infrastructure Security Agency, “Protective Domain Name System (DNS) Resolver,” <http://cisa.gov/resources-tools/services/protective-domain-name-system-dns-resolver>; National Security Agency, Cybersecurity Collaboration Center, “DIB Cybersecurity Services,” <http://nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services>.
28. National Cyber Security Centre, “Active Cyber Defence: Introduction,” <http://ncsc.gov.uk/section/active-cyber-defence/introduction>; State of Israel, *Israel National Cybersecurity Strategy 2025*, [http://gov.il/BlobFolder/news/cyber\\_strategy\\_2025/he/israel\\_national\\_cybersecurity\\_strategy\\_feb2025.pdf](http://gov.il/BlobFolder/news/cyber_strategy_2025/he/israel_national_cybersecurity_strategy_feb2025.pdf)
29. U.S. Department of Justice, “U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure,” January 31, 2024, <http://justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>.
30. U.S. Department of Justice, “Court-Authorized Operation Disrupts Worldwide Botnet Used by People’s Republic of China State-Sponsored Hackers,” September 18, 2024, <http://justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state>.
31. U.S. Department of State, “Rewards for Justice,” <http://state.gov/rewards-for-justice>.
32. Kent Walker, “A Summer of Security: Empowering Cyber Defenders With AI,” *The Keyword*, July 25, 2025, <http://blog.google/innovation-and-ai/technology/safety-security/cybersecurity-updates-summer-2025>; OpenAI, “Daybreak: Frontier AI for Cyber Defenders,” <http://openai.com/daybreak>; Anthropic, “Project Glasswing: An Initial Update,” May 22, 2026, <http://anthropic.com/research/glasswing-initial-update>.
33. Defense Advanced Research Projects Agency, “AI Cyber Challenge (AIxCC),” <http://aicyberchallenge.com>.
34. White House, “White House Launches Gold Eagle Initiative for Unprecedented Cybersecurity Vulnerability Coordination,” July 14, 2026, <http://whitehouse.gov/releases/2026/07/white-house-launches-gold-eagle-initiative-for-unprecedented-cybersecurity-vulnerability-coordination>.
35. Aaron Mak, “How Antitrust Law Could Weaken AI Security,” *Politico*, May 7, 2026, <http://politico.com/newsletters/digital-future-daily/2026/05/07/how-antitrust-law-could-weaken-ai-security-00910499>.
36. Government Accountability Office, *Cybersecurity Regulations: Industry Perspectives on the Impact, Progress, Challenges, and Opportunities of Harmonization*, July 30, 2025, <http://gao.gov/products/gao-25-108436>; Congressional Research Service, “Critical Infrastructure: Emerging Trends and Policy Considerations for Congress,” March 10, 2026, <http://congress.gov/crs-product/R48878>.

37. U.S. Department of Defense, *Mission Assurance (DoD Directive 3020.40)*, September 11, 2018, <http://esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf?ver=2018-09-11-131221-983>.
38. Annie Fixler, Mark Montgomery, and Rory Lane, “Military Mobility Depends on Secure Critical Infrastructure,” *CSC 2.0*, March 2025, <http://fdd.org/wp-content/uploads/2025/03/fdd-csc2.0-military-mobility-depends-on-secure-critical-infrastructure.pdf>; Government Accountability Office, *Civil Support: DoD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities During Cyber Incidents*, April 4, 2016, <http://gao.gov/products/gao-16-332>.
39. North American Electric Reliability Corporation, “NERC CIP Roadmap,” January 12, 2026, [http://nerc.com/globalassets/our-work/reports/special-reports/nerc\\_cip\\_roadmap\\_01122026.pdf](http://nerc.com/globalassets/our-work/reports/special-reports/nerc_cip_roadmap_01122026.pdf); U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, “Cyber-Informed Engineering,” <http://energy.gov/ceser/cyber-informed-engineering>.
40. The White House, *Roadmap to Enhancing Internet Routing Security*, 2024, <http://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf>; National Institute of Standards and Technology, *Secure Domain Name System (DNS) Deployment Guide*, NIST SP 800–81 Rev. 3 (March 2026), <http://csrc.nist.gov/pubs/sp/800/81/r3/final>; Cybersecurity and Infrastructure Security Agency, “Positioning, Navigation, and Timing,” <http://cisa.gov/topics/risk-management/positioning-navigation-and-timing>.
41. “Mutually Agreed Norms for Routing Security (MANRS),” <http://manrs.org>; National Security Agency, *Adopting Encrypted DNS in Enterprise Environments*, Cybersecurity Information Sheet, January 14, 2021, [http://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI\\_ADOPTING\\_ENCRYPTED\\_DNS\\_U\\_OO\\_102904\\_21.PDF](http://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF); Cybersecurity and Infrastructure Security Agency, *Encrypted DNS Implementation Guidance* (2024), [http://cisa.gov/sites/default/files/2024-05/Encrypted%20DNS%20Implementation%20Guidance\\_508c.pdf](http://cisa.gov/sites/default/files/2024-05/Encrypted%20DNS%20Implementation%20Guidance_508c.pdf).
42. Brett Schaefer and Danielle Pletka, “Countering China’s Growing Influence at the International Telecommunication Union,” *Heritage Foundation*, March 7, 2022, <http://heritage.org/global-politics/report/countering-chinas-growing-influence-the-international-telecommunication>; Mark Montgomery and Theo Lebryk, “China’s Dystopian ‘New IP’ Plan Shows Need for Renewed U.S. Commitment to Internet Governance,” *Just Security*, April 13, 2021, <http://justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance>.

43. Megan Stifel, "Maintaining U.S. Leadership on Internet Governance," Council on Foreign Relations, February 2017, <http://cfr.org/reports/maintaining-us-leadership-internet-governance>.
44. Sam Sabin, "Trump Hobbled Top Cyber Agency Just as AI Learned to Hack," Axios, May 26, 2026, <http://axios.com/2026/05/26/cisa-white-house-cybersecurity-ai>; Sara Friedman, "White House Fiscal 2027 Budget Proposes Cuts to Federal Agency Spending on Cybersecurity Needs," *Inside Security*, April 7, 2026, <http://insidecybersecurity.com/daily-news/white-house-fiscal-2027-budget-proposes-cuts-federal-agency-spending-cybersecurity-needs>.
45. Rebecca Klarr and Ines Kagubare, "Internal Clashes Reportedly Led to White House Cyber Adviser's Exit," *The Hill*, April 4, 2023, <http://thehill.com/newsletters/technology/3934489-internal-clashes-reportedly-led-to-white-house-cyber-advisers-exit>; Justin Doubleday, "Groups Urge Trump to Reinforce National Cyber Director Role," Federal News Network, December 13, 2024, <http://federalnewsnetwork.com/cybersecurity/2024/12/groups-urge-trump-to-reinforce-national-cyber-director-role>.

## Acknowledgments

We are grateful to the members of the advisory committee for their time and insight. Although the views expressed are our own, their feedback on early versions of the report not only expanded our understanding of critical infrastructure vulnerabilities, the history of U.S. cyber policy, and the development of Chinese cyber operations, but also strengthened our policy recommendations. We thank CFR President Mike Froman for his strong support of this project and Associate Vice President of Studies Stuart Reid for his review and incisive comments. Our special thanks to CFR Research Associates Zoë Moore, Benjamin Holtzman, and Aarya Vaidya for their research and exceptional administrative coordination, and to Senior Editorial Director Patricia Dorff and Senior Editor Cassandra Jensen for their editorial support and guidance. We thank the Hewlett Foundation for their generous financial support for this project.

## About the Authors

**Matthew Ferren** is a former international affairs fellow in national security, sponsored by Janine and J. Tomilson Hill, at the Council on Foreign Relations (CFR). He coauthored the *2023 National Cybersecurity Strategy* and the *2024 Report on the Cybersecurity Posture of the United States*.

**Adam Segal** is the Ira A. Lipman chair in emerging technologies and national security and director of CFR's Digital and Cyberspace Policy program. He was the project director for the CFR-sponsored Independent Task Force reports *Confronting Reality in Cyberspace, Innovation and National Security*, *Defending an Open, Global, Secure, and Resilient Internet*, and *Chinese Military Power*. His book *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* describes the increasingly contentious geopolitics of cyberspace.

**Rush Doshi** is the C.V. Starr senior fellow for Asia studies and director of the China Strategy Initiative at CFR. He is the author of *The Long Game: China's Grand Strategy to Displace American Order*. Doshi was also coeditor of *Global China: Assessing China's Growing Role in the World*.