U.S. House Committee on Homeland Security

Adam Meyers
Sr. Vice President, Counter Adversary Operations
CrowdStrike

"Unconstrained Actors: Assessing Global Cyber Threats to the Homeland"
January 22nd, 2025

Chairman Green, Ranking Member Thompson, members of the Committee, thank you for the opportunity to testify today. My name is Adam Meyers, and I serve as Sr. Vice President for Counter Adversary Operations at CrowdStrike. For over a decade, I've led the company's practice area on monitoring and disrupting cyber threats. The overwhelming majority of attention during that time, and in particular over recent months, has focused on the People's Republic China (PRC).[1] So I'll focus my remarks today on threats from that country and discuss other threats at a high-level.

As a leading U.S. cybersecurity company, CrowdStrike has a useful and often quite textured vantage point on malicious activities in cyberspace. Protecting organizations with our cybersecurity technology, threat intelligence, and incident response services, we confront a full range of cyber threats. We defend many components of the U.S. Federal government and serve as a commercial cybersecurity provider for major technology companies, 8 of the top 10 financial services firms, thousands of small- and medium-sized businesses, as well as all manner of critical infrastructure entities and many foreign companies. China-nexus adversaries target each of these sectors heavily, as do threat actors affiliated with other nations.

As I've noted in a recent testimony, we started CrowdStrike in large part due to the growing impact of unchecked cyber threats–frequently from China–and the inability of existing security tools to meet this challenge. In 2011, it wasn't uncommon to see Chinese campaigns spanning scores of victims, with a multi-year duration, using extremely basic tactics, techniques, and procedures (TTPs). At that time, cybersecurity was focused on preventing the most prevalent threats, rather than the most impactful ones. Moreover, it was considered impolite, or even counter to one's economic interests, to call out this activity directly. I'm proud of the work our team–and the cybersecurity community more broadly–has done over the intervening years to change this perception. Still, there's clearly more work to be done.

[1] This testimony draws in part from a previous one I delivered on "Big Hacks & Big Tech: China's Cybersecurity Threat," before the U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law on November 19th, 2024. https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/2024-11-19pm-testimony-meyers.pdf.

At CrowdStrike, we utilize a cryptonym-based naming convention to characterize adversaries. This has become a best practice, as it permits researchers the flexibility to update attribution, account for reorganizations, and manage multiple actors with the same institutional affiliation. We assign a cryptonym once we achieve a reasonably robust confidence level in our attribution, and designate China-based adversaries as "PANDAs."[2] At present, we track 64 distinct PANDA adversaries, 20 of which have been recently observed, as well as a large number of other "activity clusters" with likely ties to China, but lower attribution fidelity.

Key Threat: People's Republic of China

After over a decade of investing in programs to strengthen China's cybersecurity ecosystem, China's cyber capabilities have matured to achieve at least parity with those of world cyber powers. Chinese threat actors operate complex, sophisticated, meaningfully obfuscated, and often highly effective offensive cyber operations targeting every region and every industry vertical. Recent campaigns demonstrate the ability to compromise large, well-resourced, and well-defended enterprises operating as providers for the rest of the technology ecosystem. From an intelligence perspective, these examples highlight a growing emphasis within Chinese operations on "upstream" or "bulk" collection, which is notable for its efficiency, scale, and potential for impact. Other campaigns are suggestive of pre-positioning capabilities relevant for disruptive and destructive cyber attacks.

Over the past year, China-nexus intrusions increased 150 percent across all sectors on average compared to 2023. These increases were most significant in the financial services, media, manufacturing, and industrials and engineering sectors, which all experienced between 200- and 300-percent increases in observed China-nexus intrusions compared to previous years. Even among the top three sectors China-nexus adversaries most commonly target—government, technology, and telecommunications—intrusion activity from China increased 50 percent in 2024 compared to 2023. Suspected China-nexus cloud intrusions increased six percent in 2024 across multiple commercial cloud services providers. Another marker of maturation in general is the complexity of successfully exploited systems.[3]

Here is a brief overview of a few recent and notable campaigns:

---

[2] These names generally take the form of a community- or researcher-derived codeword with some significance, followed by an animal type determined by the actor's geography or motivation. This name scheme is designed to be somewhat more descriptive than others, and can simplify communication and information sharing with government and industry counterparts, as well as assist clients' threat modeling process. For more detail, see: "Global Threat Landscape," https://www.crowdstrike.com/adversaries/.

[3] China-nexus adversaries continue to increase their stealthiness and knowledge of the environments they are operating in, using novel techniques to move quickly, move laterally and escalate privileges, and remain undetected. Notably, a widely-reported 2023 breach of a major software provider demonstrated the ability to manipulate encryption systems to arbitrarily mint keys to grant the threat actors access to sensitive systems. See, "Review of the Summer 2023 Microsoft Exchange Online Intrusion," Cyber Safety Review Board, March 20, 2024. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

- Over the past year or so, **VANGUARD PANDA** (*Volt Typhoon*) drew significant attention from U.S. policymakers due to targeting critical infrastructure providers. Threat activity associated with this actor demonstrates the potential application for "preparation of the battlespace." That is, potential use of disruptive or destructive attacks preceding or coinciding with military hostilities. For initial access, the actor targeted ubiquitous unmanaged or perimeter (edge) devices and infrastructure.[4] These same edge devices that are integral to connecting networks to the internet provide a ripe attack surface for adversaries. Targeting these systems is fruitful because they are critical components for authentication and provide a pathway to compromise identities. These attacks are also relatively stealthy on account of reduced visibility from third-party security providers, minimal telemetry generated by system access and use, and limited forensic artifacts. Use of these techniques further limits the detection capabilities of defenders and the capacity to track adversary operations by researchers.
- At present, China-nexus adversaries heavily target telecommunications infrastructure likely in support of the intelligence collection goals of the PRC. **OPERATOR PANDA**[5] is one such adversary whose attacks have been widely reported. As noted above, this activity is consistent with tradecraft that we assess is designed to facilitate bulk collection and subsequently specific targeting. In some cases, the latter appears aimed at major U.S. political and national security officials.
- Other advanced adversaries such as **LIMINAL PANDA** also target the telecommunications sector and demonstrate extensive knowledge of its networks, including understanding interconnections between providers and the protocols that support mobile telecommunications.[6] Recently, this adversary compromised these networks by exploiting trust relationships between telecommunications organizations and poor security configurations, allowing them to create footholds to install multiple redundant routes of access across the affected organizations. The adversary ultimately emulated the global system for mobile communications (GSM) protocols to enable command-and-control (C2) and developed tooling to retrieve mobile subscriber information, call metadata and text messages, and facilitate data exfiltration. Actions on objectives indicated additional adversary aims of surveilling targeted individuals by gathering metadata about their cellular devices.

North Korea, Russia, Iran, and Beyond

As China's threat activity captures high-level attention, other threats continue to evolve. I'll mention a few high points here and can discuss at more length as appropriate.

---

[4] This is consistent with other China-nexus adversaries increasingly moving away from the use of low-sophistication methods for initial access like spear-phishing, weaponized USBs, and credential harvesting, instead favoring specific exploitation of vulnerabilities in edge devices like firewalls, gateways, or enterprise proxies to achieve initial access.

[5] This adversary's activity broadly aligns with previous China-nexus targeted intrusion activity tracked in industry reporting as *Salt Typhoon*.

[6] "Unveiling LIMINAL PANDA: A Closer Look at China's Cyber Threats to the Telecom Sector" CrowdStrike Blog, November 19, 2024. www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/.

- **North Korea.** Amid high-profile disruptive and destructive attacks in the mid-2010s, notably the Wannacry pseudoransomware attack and blended operation targeting Sony Pictures Entertainment, North Korea has engaged in significant financially-motivated threat activity since at least 2015. After 10 years of currency-generation campaigns, these operations have become a key lifeline to the regime while it is cut off from the international financial system due to sanctions. In addition to continuing to target banking and cryptocurrency targets, North Korea over the past few years has pivoted to campaigns placing malicious insiders in remote work positions. Beyond earning paychecks, these actors often attempt to steal intellectual property. In 2024, CrowdStrike Falcon OverWatch, our managed threat hunting service, responded to 304 incidents for a single prolific threat actor, FAMOUS CHOLLIMA, with nearly 40 percent of these representing insider threat operations.
- **Russia.** While Russia-nexus adversaries continued to focus on traditional Western targets and North Atlantic Treaty Organization (NATO) member states, the war in Ukraine continued to be the primary driver of these adversaries' 2024 operations, which were focused on intelligence collection against military, political, and diplomatic entities. A need for tactical intelligence also likely forced Russian adversaries to evolve their operations to keep pace with battlefield developments in Ukraine, as exemplified by adversaries associated with the GRU (a.k.a. GU, Main Directorate of the General Staff of the Armed Forces of the Russian Federation) heavily targeting mobile devices in Ukraine.
- **Iran.** In 2024, motivated by ongoing conflicts in the Middle East, Iran-nexus adversaries continued to extensively target Israeli entities. One threat actor, CHARMING KITTEN, collected traditional intelligence on regional policy experts, while other adversaries conducted destructive operations and information operations (IO), including targeting elections. Iran-nexus actors were also among the most notable groups over the past year leveraging generative AI support in the vulnerability landscape. Iran's government aims to use Large Language Models (LLMs) in vulnerability research and exploit development, as well as to enable vulnerability-patching systems for domestic networks.
- **Rest of the World**. While state-nexus threat activity is on the rise globally, CrowdStrike observed a concentration of activity in South Asia and the Middle East. Often, this threat activity is responsive to domestic politics and intra-regional conflict. However, many nation states increasingly leverage cyber capabilities more broadly, including by targeting U.S. entities, for intelligence collection and intellectual property theft.

Criminal and Hacktivist Threats

By volume, a meaningful share of threat activity targeting our customers comes from eCrime actors that seek to monetize malicious cyber activity. I'll share a few observations about that activity, as well as politically-motivated "hacktivist" actors, which continue to proliferate.

- **eCrime** actors continued to represent a meaningful majority of cyber threat activity by volume in 2024. The number of publicly named victims and CrowdStrike Intelligence's

direct observations of adversarial activity demonstrate that "Big Game Hunting" ransomware actors (i.e., those that target enterprises) remain the most significant eCrime threat to organizations across all geographical regions and industries. Over the past year, these actors continued a previously-observed trend of increasingly leveraging dedicated leak sites to publicly expose data in order to extort victims. However, if there's a positive news story anywhere in the cyber domain in 2024, it's that coordinated law enforcement operations like that which targeted BITWISE SPIDER (LockBit) in mid-February and Operation Endgame[7] in May sharply decreased the volume of key indicators we monitor like spam and bot activity, and ultimately forced adversaries to search for other initial-access methods. (I'll return to this theme in the *Recommendations* section, below.)

- **Terrorist organizations** are increasingly developing and maturing their offensive cyber operational capabilities. In 2024, CrowdStrike Intelligence attributed (that is, graduated from a cluster of linked activity to a formally named adversary) three terrorist-related adversaries: one affiliated with Hamas, one with the Houthi movement in Yemen, and one with Lebanese Hezbollah. More broadly within the hacktivist space, we observed a potential emerging trend where a number of hacktivists were observed engaging in financially-motivated eCrime in addition to threat activity furthering traditional social, political, or nationalist ideologies.

Recommendations

I'd like to conclude with a few recommendations for various government entities as well as enterprises and their defenders. Our respective responsibilities differ, but across the board, our shared goal must be to raise the cost for the adversary to infiltrate our networks and reduce the impact if they do. This means we need to harden our defenses and degrade the ability of the adversary to wage successful, undetected attacks.

To this point, I've mainly focused on the threat environment and the policy landscape for confronting those threats. But I'd be remiss if I didn't at least briefly highlight some of the operational capabilities that all enterprises–whether private or public sector–can leverage to actually defend themselves. From my experience, the highest-leverage approaches are:

- Taking increasing care to defend **identity** across the enterprise. Compromised identities are at the core of most of the threat activity CrowdStrike has observed and responded to over the past several years. Better identity security enables a radical reduction in threats. Identity Threat Detection and Response (IDTR) tools are an important, intelligence-informed layer of the broader identity picture.
- Maintaining **visibility** across increasingly complex, distributed, and federated networks. Today, that requires instrumenting and monitoring traditional endpoints like laptops and desktops, network infrastructure, cloud environments, mobile and IOT devices, and

[7] "Operation Endgame: Coordinated Worldwide Law Enforcement Action Against Network of Cybercriminals," Federal Bureau of Investigation, May 30, 2024. https://www.fbi.gov/news/press-releases/operation-endgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals.

increasingly, Software-as-a-Service (SaaS) applications. Such monitoring generates valuable security telemetry, designed to alert defenders to threats across each of these vectors. Endpoint Detection and Response (EDR) tools are essential to this end.

- Developing an **integrated** picture of IT extended environments, particularly in the face of increasing cross-domain threats (i.e., those targeting different platforms and systems). Use of technologies like Next-Generation Security Information and Event Management (NextGen SIEM) tools can help make this duty more straightforward for organizations of all sizes.

Executive Branch. The federal government can enhance national security by doing cybersecurity well, adopting best-in-class technologies, and disrupting adversary infrastructure. As the federal government takes on initiatives to modernize and create efficiencies during this period of transition–as well as review and deprecate legacy programs and systems–there's a significant opportunity to move the needle in each of these areas.

While key U.S. federal departments and agencies have come a long way over the past number of years on defense, there's still progress to be made. The U.S. government itself faces among the most severe threat environments of any organization globally. Federal organizations must lead by example by ensuring federal departments and agencies have the best tools, best training, and most informed concepts of operations for defense available. This will require appropriately resourcing and empowering Federal CIOs and CISOs. Helpfully, findings from successfully defending federal agencies can support the development of best practices of value to other sectors, like academia, commercial enterprises, and nonprofits.[8]

Several key departments can also do more to proactively meet and defeat cyber threats. Government missions and responsibilities change over time, catalyzed by evolving opportunities, constraints, and conditions. Based on current competencies and authorities, and my observations from facilitating collaboration widely over a long period, I'll outline a few suggested focus areas. For its part, DHS, including CISA, can double down on promoting federal cybersecurity so agencies are coordinated and operationally aligned to defeat threats. Threat actors are adept at exploiting gaps and seams, so a unified approach is essential. In recent years, the federal government has deployed 920,000 endpoint detection and response (EDR) sensors, which has helped.[9] The task now is to layer additional mission capabilities into this infrastructure to improve vulnerability management, IT hygiene, and to enable better and more responsive managed threat hunting. CISA can also refocus on critical infrastructure cybersecurity, particularly in light of continued, consequential attacks from actors like VANGUARD PANDA and OPERATOR PANDA.

---

[8] For specific recommendations on improving federal cybersecurity, *see Rob Sheldon, Testimony on "Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs"* U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection (September 19, 2023). https://www.crowdstrike.com/wp-content/uploads/2023/11/9.19-CHS-Federal-Cyber-Testimony.pdf.

[9] "Securing Federal Networks: Evolving to an Enterprise Approach," Cybersecurity and Infrastructure Security Agency, January 13, 2025. https://www.cisa.gov/news-events/news/securing-federal-networks-evolving-enterprise-approach.

The FBI tends to lead on performing threat actor infrastructure takedowns and coordinated law enforcement actions. Efforts along these lines do take place and can be successful, such as with Operation Endgame (cited above). Still, from my vantage, over the past decade the threat environment has worsened more rapidly than our capacity to execute such operations has increased. It's now worth asking: in collaboration with international partners, what might we do to increase the tempo of disruptions by 5x? Or by 10x? It may take that scale to durably impact threat actors' operations sufficiently to raise their cost of doing business and offer meaningful relief to victims. CISA can do more to promote this mission area by providing textured, real-time insights from stakeholders, including major IT and cybersecurity providers and critical infrastructure entities, about the most pressing threats. This can inform prioritization.

The National Security Agency, Cybercommand, and other elements of the U.S. defense and intelligence enterprise have complementary roles in disrupting threat actors and their infrastructure. A full discussion is beyond the scope of this testimony but I will highlight the importance of ongoing efforts to secure the Defense Industrial Base.

Legislative Branch. For Congress' part, it's appropriate to perform oversight to ensure federal agencies are actively pursuing the objectives outlined above as well as ensuring resource alignment and accountability. Further, to the extent that some of the defense I outlined above appear out of reach for the average small business in your state, it's appropriate to engage in a more meaningful conversation than we as a community have had to date on the use of tax credits, rebates, or other incentives to make best-in-class cybersecurity tools and training more accessible.

Thank you again for the opportunity to testify today, and I look forward to your questions.

###

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Committee on Homeland Security

Unconstrained Actors

Assessing Global Cyber Threats to the Homeland

RADM (RET.) MARK MONTGOMERY

Senior Director and Senior Fellow
Center on Cyber and Technology Innovation
Foundation for Defense of Democracies

Washington, DC
January 22, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

INTRODUCTION

Chairman Green, Ranking Member Thompson, and distinguished members of the committee, thank you for inviting me here to testify today.

Every president since the tragic attacks of 9/11 has stated that "defense of the homeland" is the nation's number one national security mission. In his first term as president, Donald Trump approved a National Security Strategy that stated his first responsibility was "to protect the American people, the homeland, and the American way of life."[1] As he takes office again eight years later, the homeland has never been less secure, and America's greatest vulnerability is not a physical attack from non-state actors and terrorists, although that risk still exists. Rather, the greatest vulnerability is the threat of cyberattacks and long-range missile strikes by China and Russia — risks that undermine historical assumptions that the Atlantic and Pacific Oceans will protect America from foreign aggression.

I am confident the Armed Services Committee is looking hard into the missile defense issues, but House oversight of the protection of our national critical infrastructure from cyberattack starts here in the Committee on Homeland Security.

THREAT

The cyber threat is the greatest daily threat to the safety and security of American citizens and to the American way of life and the Chinese Communist Party (CCP) is America's most capable and opportunistic cyber adversary.[2]

Revelations over the past year have exposed the true depth of CCP cyber penetrations into U.S. critical infrastructure. These attacks should remove any doubt about either America's vulnerability or Beijing's intention to unseat the United States as the preeminent global power.

China's Volt Typhoon penetration sought to enable its hackers to lie in wait, ready to disrupt and destroy U.S. systems at the time of Beijing's choosing during a crisis.[3] This campaign compromised numerous critical infrastructures, including ports, energy systems, and water utilities.[4] As a military planner, this is what I called "operational preparation of the battlefield." Senior U.S. intelligence officials have warned that the CCP intends to activate these capabilities

---

[1] The White House, "National Security Strategy of the United States of America," December 2017. (https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf)
[2] Cyberspace Solarium Commission, "Final Report," March 2020. (https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report)
[3] "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says," *Federal Bureau of Investigation*, April 18, 2024. (https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says)
[4] "The CCP Cyber Threat to the American Homeland and National Security," *U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party*, January 31, 2024. (https://selectcommitteeontheccp.house.gov/about/events/hearing-ccp-cyber-threat-american-homeland-and-national-security)
[5] Sarah Krouse, Robert McMillan, and Dustin Volz, "China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack," *The Wall Street Journal*, September 26, 2024. (https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835)

later during a crisis or contingency to disrupt key military logistics movements and to cause societal panic by disrupting electricity and water for the average American.

The revelations about this systematic compromise of U.S. critical infrastructure were followed later in 2024 by reports of yet another unprecedented hack by the CCP.[5] Salt Typhoon — a different advanced persistent threat actor operated by the CCP's Ministry of State Security[6] — conducted extensive cyber espionage in the United States and other Western allies. This campaign accessed the systems of nine U.S. telecommunications systems and internet service providers, including those used to support U.S. law enforcement and intelligence agencies in the conduct of court-authorized wiretaps.[7] This extensive theft of data included audio recordings of telephone calls made by high-ranking U.S. government officials.

These CCP penetrations are not a new thing. Over the past few years, there have been numerous high-profile cyber espionage campaigns conducted by the CCP against the United States, penetrating U.S. government email systems and stealing the data that comprised many companies' intellectual property.

Meanwhile, not to be forgotten, Russia, Iran, North Korea and criminal actors all had an equally successful year in 2024, penetrating U.S. networks, conducting espionage, extorting ransoms, and stealing sensitive data.[8] Russia's intelligence and military services have successfully conducted complex espionage attacks against the United States, such as SolarWinds,[9] but also work closely with state-affiliated or state-abetted criminal organizations to conduct aggressive ransomware and other cybercriminal attacks.[10] North Korea is often referred to as a cyber-criminal gang masquerading as a nation-state and has specialized in ransomware and cryptocurrency theft.[11] Iran historically fixed its cyber sights on the Iranian diaspora in the West

[5] Sarah Krouse, Robert McMillan, and Dustin Volz, "China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack," *The Wall Street Journal*, September 26, 2024. (https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835)
[6] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise," January 17, 2025. (https://home.treasury.gov/news/press-releases/jy2792); Greg Otto, "Malware linked to Salt Typhoon used to hack telcos around the world," *CyberScoop*, November 25, 2024. (https://cyberscoop.com/salt-typhoon-us-telecom-hack-earth-estries-trend-micro-report)
[7] Martin Matishak, "US adds 9th telecom company to list of known Salt Typhoon targets," *The Record*, December 27, 2024. (https://therecord.media/nine-us-companies-hacked-salt-typhoon-china-espionage)
[8] "The 2024 Year in Review: Cybersecurity, AI, and Privacy Developments," *Hinckley Allen*, January 9, 2025. (https://www.jdsupra.com/legalnews/the-2024-year-in-review-cybersecurity-8353611)
[9] U.S. Department of the Treasury, Press Release, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," April 15, 2021. (https://home.treasury.gov/news/press-releases/jy0127)
[10] Lily Hay Newman, "Russia's Sway Over Criminal Ransomware Gangs Is Coming Into Focus," *WIRED*, November 10, 2022. (https://www.wired.com/story/russia-ransomware-gang-connections); C. Todd Lopez, "In Cyber, Differentiating Between State Actors, Criminals Is a Blur," *DOD News*, May 14, 2021. (https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur)
[11] "The Attack on America's Future: Cyber-Enabled Economic Warfare," Eds. Samantha Ravich and Annie Fixler, *Foundation for Defense of Democracies*, October 28, 2022. (https://www.fdd.org/analysis/2022/10/28/the-attack-on-americas-future-cyber-enabled-economic-warfare)

and on Israel, but it expanded its target set to include U.S. critical infrastructure over the past two years.[12]

Beyond these nation state threats lies an even more aggressive cybercriminal enterprise. The FBI received reports of $12.5 billion in cybercrime losses in the United States in 2023, an increase of nearly 20 percent over 2022. While we know that unreported losses are much higher, the annual increase in reported crime is an accurate reflection of the growing impact of criminal activity.[13]

CONSEQUENCES

The purpose of the CCP's cyberattacks is not just to sow chaos or intimidate civilians. Chinese leaders understand that America will struggle to rapidly mobilize military forces if the rail, aviation, and port systems that move military equipment, personnel, and supplies to the battlefield are degraded or inoperable. Indeed, the success of Chinese aggression in the Taiwan Strait or Russian aggression in the Baltics, for example, could depend to a significant degree on the speed with which the United States is able to send additional military forces forward from the homeland. Last year, the U.S. intelligence community expressly warned that the CCP would "consider aggressive cyber operations against U.S. critical infrastructure and military assets" not only to deter America from taking military action in response to Chinese aggression but also specifically to "interfere with the deployment of U.S. forces."[14] If adversaries can delay the mobilization and deployment of American forces from the United States, that could make it much more difficult to defeat the aggression in time.

Addressing these domestic vulnerabilities is easier said than done because the government does not control the infrastructure on which military mobilization depends. The U.S. military primarily relies on 18 commercial seaports, about 70 civilian airports, and 40,000 miles of rail lines to move troops and equipment from fort to port and overseas. These strategic airfields, seaports, and railroads are almost wholly owned and operated by the private sector and maintained with insufficient levels of cyber resilience. For decades, many of these infrastructures have prioritized safety and physical security, adding internet-connected sensors and remote-access systems to allow real-time, cost-efficient monitoring and operations. This digitalization, however, has opened pathways for America's adversaries to penetrate and preposition malicious capabilities across the homeland.

---

[12] National Security Agency, Press Release, "Iranian Cyber Actors Access Critical Infrastructure Networks," October 16, 2024. (https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3935330/iranian-cyber-actors-access-critical-infrastructure-networks); Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities," Revised December 18, 2024. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a)

[13] Federal Bureau of Investigation, Press Release, "FBI Releases Internet Crime Report," April 4, 2024. (https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report); Federal Bureau of Investigation, Press Release, "FBI Releases Internet Crime Report," April 4, 2024. (https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report)

[14] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf)

The energy, financial services, and manufacturing industries that drive economic productivity are also privately owned and equally vulnerable to cyberattack. The lifeline systems that Americans rely on for daily life — water, food, and healthcare — are increasingly targeted by unscrupulous criminals out for a quick payday at the expense of the American people.

While the private sector owns the infrastructure and needs to better understand that cybersecurity is essential for core business functions, the U.S. government has too often been a poor partner for industry.[15] For more than a decade, the federal government has preached the importance of public-private partnerships to share cyber threat information and mitigate cyber risks. And yet, these public-private partnerships to support the resilience of America's critical infrastructures are inconsistent, and the sector risk management agencies (SRMAs) responsible for this collaboration are under-resourced.[16]

SOLUTIONS

The 119th Congress will not be the first Congress to face this situation. As a young Naval officer, I worked at the National Security Council from 1998 to 2001 when we first tried to tackle this problem. We developed a National Infrastructure Assurance Plan in 2000, and it identified many of the same challenges I have highlighted above and some of the solutions I am listing below. Both the Clinton and Bush administrations, as well as the Congress, began to take up some of the recommendations, but all the momentum was lost in the wake of 9/11 when responding to the physical threat of terrorists became jobs one, two, and three.

More recently, Congress — led by former Reps. John Katko and Jim Langevin from this committee, as well as Rep. Mike Gallagher and Senators Angus King and Ben Sasse — sought to highlight this issue, and they worked on legislation that created the Cyberspace Solarium Commission. That commission, of which I was executive director, made a series of 80 recommendations, 50 of them legislative in nature. Congress enacted nearly 80 percent of these recommendations, but some of the most important ones — the harder ones to implement — have been left unaddressed.[17] And of course, as threats and conditions evolve, new recommendations have emerged as well.

The core issue is to restore deterrence in cyberspace, making it too hard or too painful for an adversary to disrupt or exploit our networks and systems there. To do this requires both deterrence by denial — improving our defensive efforts — and deterrence by punishment — improving our ability to impose costs on an adversary.

---

[15] Mary Brooks, Annie Fixler, and RADM (Ret.) Mark Montgomery, "Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure," *Cyberspace Solarium Commission 2.0*, June 7, 2023. (https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure)

[16] RADM (Ret.) Mark Montgomery and Jiwon Ma, "We must invest in defending our critical infrastructures," *Washington Examiner*, May 23, 2024. (https://www.washingtonexaminer.com/opinion/3014980/we-must-invest-in-defending-our-critical-infrastructures)

[17] Jiwon Ma and RADM (Ret.) Mark Montgomery, "2024 Annual Report on Implementation," *Cyberspace Solarium Commission 2.0*, September 19, 2024. (https://cybersolarium.org/annual-assessment/2024-annual-report-on-implementation)

Improve Our Defense

Secure the Critical Infrastructures that Support Military Mobility: The vulnerabilities in U.S. aviation, rail, and maritime port infrastructure directly impacts America's national security and economic productivity. As was mentioned earlier, the U.S. military primarily relies on 18 commercial seaports, about 70 civilian airports, and 40,000 miles of rail lines to move troops and equipment overseas. These assets are largely owned and operated by the private sector and are routinely assessed to have insufficient levels of cyber resilience. The SRMAs responsible for managing cyber risks to these subsectors — the U.S. Coast Guard, Transportation Security Administration, and Federal Aviation Administration — need authorizations and appropriations to fully execute their responsibilities. The private sector operators of these systems will need technical and financial assistance to combat the aggressive nature of the CCP cyberattacks and to ensure availability of essential services in a time of crisis. Congress will have to work across multiple jurisdictional issues to ensure that these efforts are synchronized for success.

Prioritize Assets: The United States cannot protect everything, everywhere, all at once. Within critical infrastructure, there are assets and entities that are more critical to U.S. national security, economic prosperity, and public health and safety. Last April, the Biden administration rightfully tasked the Cybersecurity and Infrastructure Security Agency with working with the other sector risk management agencies to identify these systemically important entities (SIEs). The administration failed, however, to outline the benefits and burdens for companies identified as SIEs. These companies need priority access to intelligence, information, and incident response support. In return, the American people should expect them to practice a higher level of cybersecurity, which is assessed and validated by a third party or even the government. Congress should detail the benefits and burdens of SIEs in law.

Resource Sector Risk Management Agencies for the Mission: Congress established SRMAs as the federal agencies responsible for collaborating with and supporting key critical infrastructure sectors. Collaboration between the government and critical infrastructure owners and operators will not improve if SRMAs and/or federal agencies are not sufficiently focused on this mission or resourced to undertake it. Many of these SRMAs have failed to cultivate the necessary expertise within the agency and have not invested appropriately in their staffing. One or two full-time equivalent workers are not sufficient to help share information, assess risk, and provide guidance to thousands of companies struggling with a changing cyber threat environment. Some SRMAs are barely resourced enough to maintain a website with cyber hygiene resources. Yet not all sectors need the same amount of support. Not all SRMAs need the same budgets. But all SRMAs should have sufficient resources to meet the needs of their sector. As the annual budget season begins, Congress should demand that agencies answer tough questions about their repeated failures to invest appropriate resources into helping secure critical infrastructure.

Restart Continuity of the Economy (COTE) Planning: A core component of deterrence is our adversaries' understanding that America can quickly recover — and strike back — if an adversary launches significant cyberattacks against us. The federal government needs a plan for how it will work with the private sector to restore critical economic functions rapidly. This goes beyond disaster planning for lifesaving and life-safety services. What assets do we need to

prioritize to restart financial flows and restore normal business operations? Congress wisely understood the importance of this complex issue and tasked the administration in the FY2021 National Defense Authorization Act with developing COTE plans. The Biden administration, however, largely failed to respond to the congressional tasking. The effort brushed aside gaps in current federal incident response capabilities and failed to grapple with the ways the private sector must participate in the development and implementation of the plan.[18] Congress should work with the Trump administration to restart the planning process in earnest, leveraging the original legislative mandate which requires updates to the COTE plan every three years.

Harmonize Cybersecurity Regulations: Critical infrastructure owners and operators are regulated by independent regulators at the federal, state, and local level. Many of these regulators have begun imposing cybersecurity regulations, leading to a patchwork of inconsistent or redundant regulations. Private industry has repeatedly warned that duplicative regulations strain already tight cybersecurity budgets.[19] When companies demonstrate to one set of regulators that they comply with one set of cybersecurity requirements, the companies should not then have to demonstrate the same facts again to a second regulatory body. Last Congress, Sens. Peters and Lankford introduced legislation to harmonize cybersecurity regulations across the federal government.[20] Restarting efforts like this in the 119th Congress should be a priority.

Utilize the National Guard to Defend our Critical Assets. The National Guard is the asset most likely to garner the authorities, capability, and capacity to help defend our domestic networks. As such, Congress needs to define the Guard's cybersecurity tasking to do this. The National Guard's unique position bridging the military and civilian sectors, as well as federal and state government authorities, makes it ideally suited to respond to domestic cyber threats. The 54 Guard entities have the local presence and capabilities that position them well to serve as a rapid response force for cyber incidents at both the state and federal levels. Over the years, the Guard has taken on more cybersecurity responsibilities and has built more cyber capacity. The Congress should work with the administration to determine the Guard's long-term role in the cyber protection of critical infrastructures and identify the necessary new authorities (few, I suspect) and resources (likely many) to do this.

Recruit and Develop an Effective Government Cyber Workforce. We need to hire, onboard, and develop cyber talent for the federal, state, and local governments. Back in 2000, I was tasked with helping create the CyberCorps: Scholarship for Service program, which was modeled after ROTC programs: we pay for your tuition at an approved college's cybersecurity program, and you commit to a few years of federal service. This program has survived for 25 years and now produces 450 graduates a year for governmental service. This program remains necessary but needs a partner program that focuses on more technical employees who hail from vocational

[18] Mark Harvey and RADM (Ret.) Mark Montgomery, "After the Attack: A Playbook for Continuity of the Economy Planning and Implementation," *Foundation for Defense of Democracies*, September 13, 2023. (https://www.fdd.org/analysis/2023/09/13/after-the-attack)
[19] Office of the National Cyber Director, "Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information," June 2024. (https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf)
[20] David DiMolfetta, "Senate panel advances cyber regulatory harmonization bill," *NextGov*, July 31, 2024. (https://www.nextgov.com/cybersecurity/2024/07/senate-panel-advances-cyber-regulatory-harmonization-bill/398478)

schools and community colleges where they accrue specific skills and certifications. The Cyber PIVOTT Act from the 118th Congress will answer this exact challenge. Additionally, the federal government needs to do a better job onboarding and initially guiding federal cybersecurity workers. To that end, Sens. Mike Rounds and Jon Ossoff introduced the Federal Cyber Workforce Training Act, and Reps. Ro Khanna and Pat Fallon worked on a similar provision last Congress. When taken together, these pieces of legislation will improve the recruiting, onboarding, and initial training of federal cyber workers and should be pursued gain in the 119th Congress.

Improve Our Offense

Enhance our Cost Imposition Capability. Over the past 10 years, the CCP has increased the size of its operational cyber forces severalfold while the United States has remained static in its force generation capability. Despite congressional attention and persistent efforts by U.S. Cyber Command, the U.S. military services have been unable to raise their readiness for a number of years. In addition, each service is inconsistent and sometimes ineffective in its recruiting, training, maintaining, and retaining of cyber warriors. Additionally, the size of each service's contribution to the Cyber Mission Force has not changed appreciably since the original agreements between the services and Cyber Command a decade ago despite significant changes in the cyber threat. As a result, the United States is not optimized for conflict with a Chinese adversary — which first created its own military cyber component almost a decade ago.[21] We see the results of Beijing's investment in its cyber forces in Volt Typhoon and other attacks. The Congress needs to work with the Trump administration to fundamentally change how we generate the cyber forces which give us the ability to impose costs on our adversaries.

CONCLUSION

In the past, U.S. presidents and Congress had the luxury of thinking about how to handle the threat from adversary states "over there" in their backyard. Things are different today as the 119th Congress takes the reins. You will be looking at a variety of security challenges, but none is more serious than the cyber threats to the homeland. To make America secure again, you will have to make the investments in cybersecurity and critical infrastructure defense that America has postponed for far too long.

On behalf of the Foundation for Defense of Democracies, thank you for inviting me to testify.

[21] Matt Bruzzese and Peter W. Singer, "Farewell to China's Strategic Support Force. Let's meet its replacements," *Defense One*, April 28, 2024. (https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143); Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review*, Spring 2018. (https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf)

Written Testimony of Kemba Walden

United States House Committee on Homeland Security
Hearing on "Unconstrained Actors: Assessing Global Cyber Threats to the Homeland"
January 22, 2025

Chairman Green, Ranking Member Thompson, distinguished members of the Subcommittee, my name is Kemba Walden, and I am the President of Paladin Global Institute (Paladin), a think tank committed to ensuring that secure critical infrastructure and the safety of people online remain core to sustainable technological innovation. I also serve as a co-chair of Aspen Institute's U.S. Cybersecurity Group, which published cybersecurity policy recommendations for the new Administration, some of which are reproduced below, based on the collective experience and expertise that membership gained over decades of experience in the public and private sectors.

Prior to Paladin, I served as the acting National Cyber Director and the first Principal Deputy National Cyber Director in the Office of the National Cyber Director in the Executive Office of the President. Before that, I was an Assistant General Counsel in Microsoft's Digital Crimes Unit (DCU), where I led the Ransomware Analysis and Disruption Program. I also spent a decade in government service at the U.S. Department of Homeland Security (DHS) in several attorney roles, specifically as the DHS lead for "Team Telecom," the lead attorney for the DHS representative to the Committee on Foreign Investment in the United States (CFIUS) and then as a cybersecurity attorney for the Cybersecurity and Infrastructure Security Agency (CISA), and its predecessor.

Over the course of my career, I've witnessed the evolution of global cyber threats, new approaches to exploiting vulnerabilities in technology, and our responses to them. There are three types of cyber threats – nation state actors, criminals, and insider threats. And there are two evolving types of vulnerabilities - the pace of technological advancement, and the status quo of business processes. The impact of these threats and the creativity and sophistication with which malicious are exploiting vulnerabilities is considerable.

The world is in a state of flux. The risks are too high to continue to take a tactical approach to responding to these threats individually. Faced with this strategic context, we must continue to pursue a more resilient and defensible infrastructure that is aligned with our values. A sustainable and successful effort against these threats will require a whole-of-government strategy executed in close partnership with the private sector, our allies, and international partners.

Over time, we've matured our governance and developed strategy, but there's much more to do. In this testimony, I first describe three types of global threats and two pernicious vulnerabilities—and second, I offer governance, skilling, and technological solutions to mitigate the resulting risks.

In this testimony, I will leverage the expertise gained through the work of Paladin Global Institute, its insight into various markets, and my experience through Aspen Digital and previous roles, to provide an overview of the threat landscape and provide recommendations I believe this subcommittee may find relevant as it continues to consider responses to these global cyber threats. Paladin Global Institute leverages its global reach and deep bench of cutting-edge thought leaders and policy experts to protect global critical infrastructure. Paladin encourages both (1) operational opportunities to mitigate cyber threats and vulnerabilities and (2) policy solutions for sustainable cybersecurity and cyber safety improvements.

A. The Evolving Landscape of Global Cyber Threats and Vulnerabilities

1. Nation-State Actors

As the world bears witness to the transition to a new Administration and a new Congress, our adversaries are considering exploiting vulnerabilities in the seams created by the transfer of power. It is in these transitions where pernicious threats thrive, and vulnerabilities loom largest. To advance their own geopolitical standing in the world and to impact the balance of alliances, nation state threat actors aim to strike when the United States is at its most vulnerable. These threat actors use diverse methods to achieve their geopolitical aims, but they share common goals. They each need for the United States to appear weak and off-balance, and they've learned that there's opportunity during times of transition.

These threats are coalescing around common goals. This month, Russia signed a treaty with Iran to expand economic and security ties between the two countries. Last year, North Korea also signed an agreement with Russia to provide military assistance in times of war. In 2022, China and Russia announced a formal partnership announcing that there are "no limits" to areas of cooperation between the two countries. These reported alliances inform the dynamic nature of global cyber threats.

Russia

Russia uses cyber operations as a foreign policy lever to shape other countries' decisions, focusing on cyber operations to gain advantage in the Ukrainian war and the region, but continuing to target critical infrastructure in the United States. When the Biden Administration was transitioning into office, it did so in the wake of the Russian state-sponsored breach of the SolarWinds Orion platform. This supply chain attack was novel in its approach, and unprecedented in its reach. Russian-backed cybercriminals then to breached Colonial Pipeline and held it for ransom. The world then watched the subsequent run on gasoline across the East Coast of America and learned that cyber has power in the real world. Russia's Federal Security Service has long-standing ties to national cyber criminals and indigenous hacktivist

communities. Because of their relationship with the government, the government tacitly permits criminals to operate, shielding them from U.S. law enforcement.

The People's Republic of China (PRC)
As noted in The Office of the Director of National Intelligence's 2024 Annual Threat Assessment, "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks." As the People's Republic of China (PRC) seeks annexation of Taiwan, with U.S. Adm. John Aquilino, Head of U.S. Indo-Pacific Command, noting "all indications" point to the Chinese military being ready for a potential invasion of Taiwan by 2027, the PRC has moved to prepare the battlespace. Long gone is a China simply focused on IP theft; we've now witnessed China snooping on telecommunications networks (i.e., Salt Typhoon) and prepositioning in U.S. critical infrastructure to enable disruption operations in preparation for a future military conflict with the U.S (i.e. Volt Typhoon).

The most recent revelations about China's massive cyberattacks on U.S. critical infrastructure and telecommunications networks demonstrate the increased sophistication of PRC threat actors, and the expansion from espionage to potential disruption or destruction activities. Although the PRC threat actors used to be known for "smash and grab" cyber intrusion, they've moved to a new era of stealth cyber intrusion, with the PRC exploiting legitimate privileges in private sector systems not only for espionage, but more importantly to hold our critical infrastructure at risk. Through an operation, named Volt Typhoon, we discovered that the PRC were "living off the land" in our infrastructure to evade our detection technologies. Over time, the PRC gained sophisticated knowledge not only of our technology but of the governance structure through which we secure that technology, forming creative opportunities for exploiting new vulnerabilities.

One additional known PRC penetration strategy is through PRC investment in U.S. critical infrastructure. Working often through creative investment vehicles, the PRC took a strategic approach to eventually holding our infrastructure at risk while the United States took a tactical approach to blocking transactions that raised national security concerns. As your Committee found in an investigation, this includes investment in the maritime industry, with two-PRC state-owned enterprises controlling portions of five U.S. ports. Notably, the PRC is outpacing most national investments in emerging technologies. According to some reports, the global investment in quantum technology is over $40 billion, with the PRC driving approximately $15 billion in investments whereas the U.S. is investing just under $5 billion

As early as 2012, the House Committee on Intelligence warned that "the United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies" and further recommended that "Committees of

jurisdiction in the U.S. Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure." In response, at the direction of Congress, the Federal Communications Commission established the Supply Chain Reimbursement Program to reimburse small providers of advanced communications services for expenses related to the removal and replacement of communication equipment and services provided by Huawei or ZTE. More work remains to be done to remove Chinese equipment from our critical infrastructure, including TP-Link consumer routers in the U.S. which have been used to launch cyber-attacks via a Chinese hacking entity that maintains thousands of compromised TP-Link routers. The fact that TP-Link is dumping routers in the US market below a profitable point has enabled them to move from 8% of the market to 60% in only a few short years. The PRC is playing the long game for an operational and strategic advantage.

Iran

Iran seeks dominance in the Middle East and conducts influence operation in the U.S. to include targeting U.S. elections. Just this summer Iran's Revolutionary Guard Corps-affiliated cyber actors targeted the Trump campaign, in efforts to erode confidence in the U.S. electoral process ahead of the November presidential election. In addition, we have seen Iran-based cyber actors enabling ransomware attacks and using brute force to compromise U.S. health care and other critical infrastructure providers.

Democratic People's Republic of Korea (DPRK, a.k.a. North Korea)

The Democratic People's Republic of Korea (DPRK) seeks the survival of the dynasty and to "reunify" the Korean peninsula under their terms and vision. Cyber operations are a main source of funding for the government which get around U.S. and international financial sanctions. In the earliest days of the Biden Administration, as blockchain technology was maturing and the virtual currency system built upon that technology were gaining in popularity, the DPRK found opportunities to exploit them for financial gain. Initially, the DPRK used ransomware to obtain virtual currency, but they later learned that exploiting vulnerabilities in blockchain technology and stealing virtual currency from cryptocurrency exchanges is far less expensive. We have also seen an uptick in DPRK targeting of critical infrastructure to steal technical information and IP to further its nuclear ambitions.

2. Cybercriminals and Fraudsters

The proliferation of cybercrime presents an escalating threat to our national and economic security. As reported by the FBI, criminal activities ranging from business email compromise, investment scams, ransomware, and fraud resulted in potential losses of over $12 billion in 2023. The General Accountability Office estimates that cyber fraud costs the U.S. federal government between $223 billion and $521 billion every year. Organized criminal groups have developed sophisticated ransomware operations impacting the operations and availability of critical

infrastructure, including healthcare facilities, and government institutions. Of particular concern are the emerging trends of criminal networks recruiting and exploiting minors for cyber operations, creating both a security and societal challenge, and the proliferation of ransomware as a service, allowing less sophisticated cyber criminals to launch attacks at a lower cost. An insidious through line across many of these nation-states and cyber criminals is the abuse of network access and privilege, with threat actors stealing credentials through phishing attacks, social engineering, and malware.

Ransomware has evolved into a highly lucrative business model, with threat actors using advanced intelligence collection to shape ransom demands. Once criminal actors break into a network, they may access and study their target's financial documents and insurance policies, and research the penalties associated with data breach laws, to better inform their eventual ransom demand and negotiating position. Leveraging this significant intelligence gathered on victim companies, the criminal actors then launch their ransomware attacks, identifying what they regard as an "optimal" ransom amount. These criminal actors extort money from their victims, not only to unlock systems but also to prevent public disclosure, making significant money from data theft and double extortion, and deploying thousands of instances of malware across thousands of victims.

As cybercrime has evolved to more enterprise-like operations involving multiple players, countering these efforts requires a multi-stakeholder and global approach. The private sector and the U.S. government have engaged in and experimented with technical and legal models, globally, to disrupt and dismantle cybercrime infrastructure. Efforts to date illustrate that a collaborative multi-stakeholder approach – sharing actionable information and leveraging the combined capabilities of the private sector and the government – yields the best opportunity to disrupt cybercrime quickly and at scale.

Paladin's direct experience with technology companies engaging in public-private partnerships has shown how potent collaboration can be. One technology company's facilitation of many hundreds of FBI victim notifications had an impact far wider than just protecting the notified victims. In one engagement, the company intercepted an attack against an IT provider with over 600 large financial institution customers. The threat actor was planning to sell access to a ransomware affiliate who would then attempt to encrypt the IT Provider's customer networks, creating a catastrophic impact on not just the victim's business, but its many customers. Public-private partnerships, when scaled up as in this case, can disrupt the criminal supply chain, thereby making it more difficult for ransomware affiliates to successfully find and attack victims.

The cybercrime ecosystem is dynamic and massive, but the Federal government has done incredible work to hold these malicious actors accountable. The National Cyber Investigative Joint Task Force, law enforcement agencies, U.S. Cyber Command, the National Security

Agency, and other elements of the intelligence community have led multiple initiatives to increase the speed and scale of disruption operations, coordinating joint, sequenced disruption campaigns with international partners. Sustained efforts, and investments, in these programs will continue to defend the Nation and our critical infrastructure from ransomware threats.

3. Insider Threats

The increasing globalization of the job market, rise of remote work, and need for highly-specialized skilled workers provides global adversaries—specifically the DPRK and the PRC—an opportunity to creatively target U.S. companies' sensitive intellectual property (IP), high-tech research and development (R&D), and financial assets. Information Technology (IT) workers often have privileged access to systems. So, while today they may just be a source of hard currency (and occasional R&D), they could use their positions of trust to conduct more conventional cyber operations.

Since at least 2022, information technology (IT) workers from the DPRK have been fraudulently obtaining remote employment at unwitting companies in the United States, including at Fortune 500 companies across a variety of industries. DPRK threat actors use U.S.-based job search sites to seek employment with U.S. companies and use stolen U.S. citizens identities to gain employment. This scheme often requires the assistance of other U.S. individuals as facilitators to help the DPRK workers appear to be in the U.S. and move money and IP out of the U.S. These works, some of whom live in China and Russia, provide a critical revenue stream that helps fund DPRK economic and security priorities and helps the DPRK gain access to sensitive IP and R&D. These fraudulent employees put U.S. companies at risk of violating U.S. and international sanctions and put IP and sensitive data at risk.

Similarly, Chinese intelligence services abuse U.S. student and work visas to gain access to critical technology at U.S. companies and universities that require highly technical and skilled workers to fill critical technology roles. For those U.S.-trained Chinese nationals who otherwise cannot lawfully stay in the United States upon completion of their studies, the PRC benefits from the talent and skills and knowledge of those students when they return. Intellectual property theft from U.S.-employed or trained Chinese nationals poses a significant risk to the private sector and academia, particularly amongst the defense sector and emerging dual-use civil-military technologies, such as Artificial Intelligence (AI). In fact, approximately 60% of all FBI trade secret theft cases involve a nexus to the PRC. For example:

- In 2018, Chinese state intelligence actors used a U.S.-based job search site to target and clandestinely recruit a former US Intelligence Community employee.
- In 2019, a U.S.-based Chinese national pleaded guilty to stealing over $1 billion in petroleum research and development from 2017 to 2018.
- In 2020, People's Liberation Army Lieutenant Yangqing Ye falsely posed as a student to enter the US on a J-1 visa. While posing as a student, Ye conducted biomedical research

at Boston University, assessed US military websites, and exfiltrated sensitive documents and information back to China.
- From 2022 to 2024, US-based Chinese national employee exfiltrated sensitive company proprietary AI technology and research to two PRC-based startups.

4. Technological Acceleration

The rapid pace of technological advancement, while offering tremendous opportunities, also presents significant security challenges. As innovations in fields like AI, quantum computing, and biotechnology emerge at an unprecedented rate, they bring both exciting possibilities and potential vulnerabilities. It is in the seams where innovative technologies are integrated into legacy IT systems, that our adversaries find exploitable opportunities.

As stated in the 2024 Report on the Cybersecurity Posture of the United States and 2024 Annual Threat Assessment, these technological advancements can enhance our capabilities in various sectors, from healthcare to transportation, but they also create new attack vectors for malicious actors. The interconnectedness of our digital infrastructure means that a single vulnerability can have far-reaching consequences, making it crucial to stay ahead of potential threats.

We must shift from reactive to proactive security postures to address emerging threats from quantum computing, AI, and other transformative technologies. This paradigm shift requires a fundamental change in how we approach security, moving away from simply responding to threats as they occur to anticipating and mitigating risks before they materialize. For instance, the development of quantum-resistant cryptography is essential to protect sensitive data from future quantum computing attacks.

Similarly, leveraging artificial intelligence and machine learning for threat detection and response can help identify and neutralize sophisticated cyber threats more efficiently. Proactive security measures also involve continuous monitoring, threat intelligence sharing, and regular security assessments to identify and address potential vulnerabilities before they can be exploited.

This requires forward-thinking policies and adaptive security frameworks and long-term investments in technology. The U.S. government and private sector need to develop comprehensive strategies that not only address current security challenges but also anticipate future threats. These policies should be flexible enough to evolve with the rapidly changing technological landscape. Adaptive security frameworks should incorporate principles of resilience, allowing systems to detect, respond to, and recover from security incidents quickly.

Capital investments in cutting-edge security technologies and innovation hubs focused on cybersecurity research and development are crucial components of this approach. Additionally,

streamlined procurement processes can ensure that organizations can quickly adopt and implement the latest security solutions. By fostering collaboration between the public and private sectors, as well as academia, we can create a robust ecosystem of innovation and security that is better equipped to face the challenges of technological acceleration.

5. Status Quo Business Processes

Supply chain attacks. Cyber threat actors' exploitation of critical vendors has highlighted the need for robust cyber supply chain risk management and vendor vetting. From the SolarWinds Orion platform breach in 2020 to Okta in 2023, the concentration of risk in and across supply chains demands constant attention. Third party risk management is a critical part of supply chain security, and I was encouraged to see that the National Institute of Standards and Technology (NIST) added cyber supply chain risk management across several publications in the last four years, including the Cybersecurity Framework 2.0.

Investments, Mergers & Acquisition. Cybersecurity challenges are commutative and can transfer during mergers and acquisitions. The United States' historical openness to foreign investment has also been exploited by competitors. The National Counterintelligence and Security Center (NCSC) has issued guidance warning start-ups that foreign threat actors could invest in their companies to "harm U.S. economic and national security interests." The FBI is reportedly investigating Hone Capital, which launched in 2015 with an initial investment of $115 million from a Chinese private equity group and has invested in over 350 U.S. tech startups. The investment has allegedly resulted in the transferring of trade secrets and intellectual property back to Beijing.

It is imperative to invest capital in technologies that adhere to U.S. law, conform to U.S. sanctions, and are not subject to the jurisdiction of adversarial nations before they go to markets. These trusted capital principles promote security, trust, safety, and national security *before* products go to market. When the company is secure by design and intent, the digital ecosystem it then joins is, too.

This complex and multi-actor threat demands of us sustaining investments in innovative, intrepid, and industry-led solutions.

B. Policy Recommendations

We must strengthen national cybersecurity by prioritizing security across all lines of efforts by clarifying roles and responsibilities of the private sector and government, upskilling our collective workforce, and embracing technological innovation that will enhance the resilience of

our infrastructure against cyber attacks. These strategic investments will yield greater returns in our security.

1. Policy Solutions to Clarify Roles and Responsibilities

Continue Building Mechanisms to Measure Progress. Government efficiency depends on good data and clear-eyed analysis. We cannot understand what works without data. We need a repository of data in this area to know what cybersecurity regulations and programs to keep and what to cut.

Clarify Lawful Proactive Solutions for Industry and Improve the Cybersecurity and Information Sharing Act of 2015 5 U.S.C. §§1501-1510. The current state of U.S. infrastructure vulnerability is unacceptable. Power grids, transportation systems, water supplies, and communication networks are all in jeopardy. You can send a clear message: the United States will defend itself against cyber aggression with the same resolve as it defends against physical threats. Everything from defensive measures to offensive operations should be on the table. Crooks, spies and terrorists should be hunted jointly with key private sector actors. Efforts to "defend forward" must be continued in conjunction with providing resources and assistance to critical, often overlooked entities such as small businesses and rural communities. Further, we must leverage the U.S.'s unique combination of innovation and capital investment to support and incentivize in areas of the world aligned with U.S. interests.

Industry cannot defend the infrastructure the Nation relies upon without the assistance of the U.S. government and its allies. We cannot expect industry alone to defeat nation-state actors. The Cybersecurity Information Sharing Act of 2015 was a good start to encouraging better collaboration between the private sector and government. Congress authorized certain protections to industry if they shared cyber threat indicators and defensive measures within industry and with the government for cybersecurity purposes. As the law is up for renewal, Congress should consider more precision in defining defensive measures (5 U.S.C. §650) so that the lines between proactive defense and "hacking back" are clearer. Most importantly, this Committee must take action to reauthorize CISA 2015 before it lapses in September to ensure we do not see hard won progress lost to Congressional inaction.

Prioritize Cybersecurity Regulatory Alignment and Streamlining. Regulatory harmonization is another key issue for the Committee to consider. Under my leadership at ONCD - and in alignment with the National Cybersecurity Strategy Implementation Plan - we put out an extensive request for information to the private sector to understand their challenges with overlapping regulatory regimes. What we heard was startling. Businesses of all sizes and from 11 of the 16 critical infrastructure sectors reported that the compliance burden was hampering their cybersecurity programs. One industry group reported that CISOs were spending 30 to 50 percent

of their time focused on compliance. This is not only a drain on our economy - it actually leaves us less secure, by keeping cyber operators filling out paperwork instead of defending systems.

Last Congress, Senator Peters, Senator Lankford, and Congressman Higgins introduced legislation to help bring coherence to the multitude of Federal regulatory approaches. The bill would have empowered the National Cyber Director to convene all of the relevant parties, including independent regulators, to develop a set of cross-sector minimum requirements that would have reciprocity baked in. A business that operates in multiple sectors - or that is in the supply chain of many regulated entities - would only need to show they met the baseline once. I am very confident this approach will both meaningfully improve our cybersecurity posture and reduce compliance costs, and I hope Congress will continue last year's momentum and move swiftly to enact this legislation. In this post-Chevron era, the incoming Administration's work with Congressional leadership will be critical.

Of course, cybersecurity is a global challenge, and the regulatory landscape is changing swiftly internationally as well. Late last year, dozens of multinational chief information security officers sent a letter to senior leaders from the Organization for Economic Co-operation and Development (OECD) countries urging them to add regulatory harmonization to the OECD's digital agenda. This builds on work former DHS Secretary Mayorkas did earlier in 2024, in partnership with the European Commission, to catalog overlapping incident reporting regimes. I urge this Committee to champion international regulatory harmonization work, including through venues like the OECD, to ensure a level playing field across the markets of our allies and partners - and to achieve our shared interest in protecting our critical infrastructure from adversary nations and cyber criminals.

Support and Instantiate the Cyber Safety Review Board (CSRB). The Cyber Safety Review Board has played a critical role in fostering transparency and accountability and driving improvements across federal agencies and critical infrastructure providers. This Committee should consider how to codify and strengthen the CSRB's role in providing a mechanism to learn lessons from past incidents and strengthen our nation's cyber defenses. Steps to strengthen the CSRB include making a full-time, independent, non-partisan board, with a full-time technical staff and administrative subpoena power. Independence will enhance the credibility of CSRB's investigations and advice.

2. Policy Solutions for Investing in a Skilled Workforce to combat cyber threats

Expand support for the Federal Cyber Scholarship-for-Service Program. 5 U.S.C § 7442 and the National Center of Academic Excellence program in Cybersecurity. The integration of emerging technologies into legacy systems, the maintenance of those systems, and the security of technology requires a well-skilled workforce in the private and public sectors. Over the last

several years, Congress has proffered positive legislation to improve our workforce. As succinctly described in the National Cyber Workforce and Education Strategy, Federal programs in cyber workforce and education reinforced the importance of sustained Federal investments by establishing a foundation for cyber workforce and education program development to provide a pipeline of qualified cyber talent. These legislative efforts include the National Center of Academic Excellence program in Cybersecurity led by the National Security Agency (NSA); the CyberCorps®: Scholarship for Service (SFS) program, led by the National Science Foundation (NSF) in coordination with the Office of Personnel Management and the Department of Homeland Security; the Department of Defense Cyber Service Academy; the Cybersecurity Education and Training Assistance Program led by the Cybersecurity and Infrastructure Security Agency; and the National Initiative for Cybersecurity Education led by National Institute of Standards and Technology.

Congress has an opportunity now to improve and expand upon these programs. It was necessary to bolt on cybersecurity to existing programs in the past, but it is now time to ensure that these programs are impactful and remain sustainable. To remain sustainable, Congress should expand the current programs in connection with the cyber workforce to (1) expressly authorize and appropriate CISA to carry out the responsibilities of DHS where appropriate under existing law, (2) provide resources to increase the number of internships and apprenticeships available to qualifying students from high-schools, two-year community colleges, or four-year universities, and (3) provide incentives to federal and non-federal entities for jobs placement to soft targets like our water and energy systems.

3. Policy Solutions to Better Integrate Technological Solutions for Mitigating Cyber Risks

Eliminate "Tech-Debt" - Technical debt, resulting from legacy IT and unsupported technologies, creates risk to operations, cybersecurity, and resilience, and creates inefficiencies and wasteful spending. The U.S. government and critical infrastructure providers must focus on eliminating technical debt by identifying existing technical debt and then modernizing IT infrastructure, including moving to the cloud and deprecating legacy IT systems.

Build Cyber Resilience and Response Capabilities. The choice between defense and offense is not binary. A game-winning interception steals the advantage from the offense and puts the team on the scoreboard. That's an offensive defense, and a principle our cyber resilience must consider. Continued investments in automated recovery, real-time threat detection, and security operations center (SOC) modernization will further advance the ball here.

Strengthen Critical Infrastructure as part of our National Defense. We need to correct foundational weaknesses in our Nation's critical infrastructure and defense systems, focusing on (1) securing supply chains, (2) protecting sensitive data, and (3) ensuring resilience against

unauthorized access and emerging vulnerabilities. A legislative agenda focused on implementing secure-by-design principles, upgrading supply chain standards, and fortifying critical digital and physical systems will fortify our critical infrastructure against nation-state threats.

Promote the Use of Artificial Intelligence (AI) to Transform Cyber Defense. We have already seen the benefit of AI to cyber defenders, including using AI to more quickly identify threats and new vulnerabilities, and scale cyber talent. The federal government should build on this success to accelerate the development and deployment of AI and explore ways to improve the cybersecurity of critical infrastructure and small and medium businesses using AI. The federal government can achieve this acceleration through (i) funding of public-private pilots on the use of AI to enhance cybersecurity in critical infrastructure sectors, (ii) funding for large-scale, labeled datasets to make progress on cyber defense research, and (iii) prioritizing research and development on human-AI interaction methods to assist with cyber analysis and incident response.

Advance Threat Detection and Intelligence. The need for advanced threat detection and intelligence capabilities to counter both known and emerging threats is certain. A combined congressional and administrative agenda could focus on integrating AI, advanced analytics, and threat intelligence to enhance situational awareness and preempt adversarial actions in cyberspace and the information domain. Constant vigilance—like a digital See Something, Say Something program—will enable the foresight needed to defend and defeat malicious cyber actors. Further, to enable identification of threat activity, CISA's capability to hunt for and identify threats across Federal Civilian Executive Branch agencies under 44 U.S.C. 3553(b)(7) must be strengthened. This includes developing the technical capability to gain timely access to required data from Federal Civilian Executive Branch (FCEB) agency endpoint detection and response (EDR) solutions and from FCEB agency security operation centers.

Enhance Identity and Access Security. Distinguishing between our digital presences is - knowing who's who, and that you are you - is of paramount importance for cyber security. Compromises of identity and authentication are a leading attack vector that our adversaries exploit year after year; weak identity infrastructure also provides adversaries with the quickest and easiest way to monetize stolen data, given that many of the identity solutions we use online are built around the premise that "knowing several things about you" means "someone is you." Solving this will require that America addresses the gap between the paper and plastic credentials - such as driver's licenses, birth certificates, and passports - that work in the physical world and the lack of any digital counterpart that can be used to prove who you are in the online world. This is an area where government must play a bigger role – in that government is the only authoritative issuer of identity. Likewise, knowledge-based systems for identity proofing are vulnerable, so too are our knowledge-based systems such as passwords for authenticating. We need to continue to drive the adoption of more modern, robust authentication solutions such as FIDO passkeys and security

keys that can stop phishing attacks cold. Identity and access management (IAM) remains a pillar of zero-trust architectures – and encouraging both government and private sector organizations to accelerate their adoption of a unified identity security program can streamline efforts to prevent unauthorized access, phishing, and email-based attacks.

C. Conclusion

The global cyber threat landscape requires a coordinated, proactive approach combining legislative action, technological innovation, and operational collaboration. By addressing these challenges through the framework I've outlined, we can better protect our national security interests while fostering innovation and economic growth.

Statement of

Brandon Wales
Vice President, Cybersecurity Strategy, SentinelOne

"Unconstrained Actors: Assessing Global Cyber Threats to the Homeland"

Before the
Committee on Homeland Security
United States House of Representatives

January 22, 2025

Chairman Green, Ranking Member Thompson, and members of the Committee, thank you for the opportunity to testify today on global cyber threats, a subject that I have worked as the Executive Director of the Cybersecurity and Infrastructure Security Agency (CISA) and now as Vice President of Cybersecurity Strategy as SentinelOne.

Introduction

The past few years of publicly-acknowledged intrusions by China, Russia, Iran, North Korea and cyber criminal organizations make clear that the U.S. is facing increasingly sophisticated adversaries in ongoing cyber warfare. The intensity of the threat is at an all-time high, driven by a combination of increasing geopolitical tension and the rapid pace of technological change. Defenders in the government and the private sector are learning from each breach and adapting to offender tactics. However, threat actors are learning and innovating as well. Maintaining a strategic edge and building national cyber resilience in the face of this onslaught remains a critical challenge and will require a collaborative whole of government and whole of industry response.

Russia

Russia's security services are an acute and malign cyber threat, willing to take increasingly aggressive cyber and sabotage operations to undermine western resolve in support of Ukraine. They maintain exceptionally skilled hacking teams that operate globally in support of Russian national interests, leveraging supply-chain attacks and access to sensitive national critical infrastructure to hold western security interests at credible risk.

Russian security services are conducting brutal sabotage campaigns across Europe in support of their illegal war and other geopolitical goals. Intelligence collection through cyber espionage plays a role in selecting targets for disruption. In addition to conflict-related targets, Russia's security services remain keen intelligence collectors against the US government. Political intelligence collection on personnel, the Department of Defense, and other US government

elements are a high priority. They remain very skilled at combining cyber and psychological operations to interfere in elections, inflame social divisions, and undermine democratic systems across the world, and have baked these operations into their doctrine for warfare against the West.

Beyond disruption, these groups engage in economic espionage, stealing sensitive data from critical sectors to bolster Russia's strategic interests. Ransomware gangs with tacit support from the state wreak havoc on U.S. businesses and institutions. The combined effect is deniable disruption and hybrid warfare that throws the security balance off kilter while imposing growing costs on our society.

Russia takes a mercenary approach to its foreign policy and cyber operations. According to public reporting from the Associated Press, Russian security services are improving their ties with the security services of the UAE.[1] Across Central Asia and Africa, Russia and the Emirates find common cause in stirring the pot in unstable countries to control gold mines and other precious resources. Their combined activities in Libya and Sudan make clear their goal to extract precious metals that help Russia blunt the impact of western sanctions.

Iran

Iran continues to dedicate its most capable teams to attacks against Israel and Israeli targets while also actively monitoring its own dissidents internally and abroad, in some cases to target them for assassination.[2] Iranian attacks against Unitronics PLCs in 2023 demonstrated the intent of the Iranian regime to target Israeli companies even outside of Israel and their willingness to target industrial control systems operating critical infrastructure.[3]

In the lead-up to the 2024 U.S. presidential election, the Islamic Revolutionary Guard Corps (IRGC) orchestrated a sophisticated "hack-and-leak" operation targeting President Donald Trump's re-election campaign. Employing spear-phishing techniques, IRGC cyber operatives infiltrated campaign email accounts, exfiltrating sensitive documents, including a 271-page vetting report on then vice-presidential candidate J.D. Vance. These stolen materials were subsequently disseminated to media outlets and individuals associated with rival political campaigns, aiming to undermine President Trump's candidacy and sow discord within the U.S. electoral process. The IRGC's efforts were, however, effectively neutralized by the broad unwillingness to publicize the stolen material.

North Korea

---

[1] https://apnews.com/article/intelligence-leak-russia-uae-pentagon-9941a3bb88b48d4dbb5218649ea67325

[2] https://www.reuters.com/world/middle-east/us-uk-taking-action-against-network-that-targeted-iranian-dissidents-us-treasury-2024-01-29/

[3] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

Multiple federal indictments demonstrate how the North Koreans are trying to get their cyber operators hired into American companies so they can wreak havoc from the inside–looting companies to pay for their rapidly advancing nuclear weapons program.[4]

Late in 2024, research by SentinelLabs showed how a web of shell companies based in China were serving as fronts for DPRK remote IT workers seeking jobs at US firms.[5] These companies were registered in China as legitimate businesses with local government through individuals in China, though it is unclear the extent to which the PRC knew of and supported these operations. Our SentinelLabs researchers tracked these registrations back to Shenyang Province in China. Reporting by CNN a decade earlier identified DPRK Military Bureau 121 operating a hotel as a front for hacking operations in the same province.[6]

Unfortunately, DPRK's IT worker scam is still in full-swing. America's front line of defense is the HR department of enterprises big and small, many of which are not technically capable enough to identify discrepancies that may indicate an issue. North Korea's effective use of mules and laptop farms create issues in detecting worker scams before these "new employees" are hired into a company.

The DPRK is also unique in that their security services are expected to turn a profit, and they do so to the tune of several billion dollars a year. These days, most of their ill-gotten gains are generated via the theft of cryptocurrencies, and many observers estimate that the North Korean government is, collectively, the largest thief of cryptocurrencies in the world. These highly fungible digital assets are then used to fund their nuclear program and evade other sanctions placed on the regime.

Cyber Criminals

Cyber criminals continue to make use of a robust ecosystem of infrastructure providers, money launderers, and tool developers to attack businesses through ransom of systems, the blackmail of leaking data, and the sale of stolen data. Ultimately, the cyber criminal ecosystem relies on three core factors: (1) a vulnerable and misconfigured install base here in the U.S. and elsewhere; (2) a cryptocurrency ecosystem outside the oversight of the traditional fiat economy by which criminals can monetize those vulnerabilities and misconfigures to extract wealth from the west; and (3) a safe harbor in Russia and its sphere of influence from which the criminals can conduct their operations without fear of consequence.

---

[4] https://www.justice.gov/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information
https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and

[5] https://www.sentinelone.com/labs/dprk-it-workers-a-network-of-active-front-companies-and-their-links-to-china/

[6] https://www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/index.html

The US and allied governments have conducted effective joint operations to reduce the trust between actors, seize criminal infrastructure, and disrupt criminal networks. Still, many criminal actors persist and profit from poor cybersecurity practices in the public and private sectors. Our research and reporting will show in 2024 that the groups Akira, BlackBasta, and Play topped the metrics for frequency and profitability of their attacks. Cybersecurity companies, such as SentinelOne, are on the front line of stopping such attacks and we continue to work alongside our law enforcement partners in disrupting these operations.

China

But one threat actor, the People's Republic of China, stands out among the rest for its persistence, breadth of operations, and capabilities.

In our public conscience, the words "OPM hack, Google, Experian, Microsoft, Marriott" are anchors in our minds of China's large-scale data theft campaigns against the US. Many now more than a decade old, we can look back on China's hacking teams and see the lack of expertise and professionalism in their old trade craft. They were noisy, easy to track, and effective.

Things have changed, though. China's hacking teams have grown significantly in size and capability over the last decade.

After Xi Jinping came into power in 2013, he quickly established the Leading Small Group on Cybersecurity and Internet Management.[7] Within a year, he would transform that Leading Small Group into one of a handful of standing committees of the Chinese Communist Party Central Committee. It was a significant step for China and signaled Xi's personal interest in the issue.

Shortly thereafter in 2015, China revamped its cybersecurity degree requirements for universities, using the U.S.'s own National Initiative for Cybersecurity Education as a model to replicate.

In 2016, after hearing about a project in Wuhan to establish a National Cybersecurity Talent and Innovation Base, with its own National Cybersecurity School, the CCP Central Committee on Cybersecurity and Informatization deputized it as a national project. The school graduates around 2000 students each year that are trained in offensive and defensive cybersecurity techniques.

A year later, in 2017, China began certifying some schools as World-Class Cybersecurity Schools–a designation again meant to copy from the US system. This time, the inspiration was the joint DHS-NSA Centers for Academic Excellence in Cyber Operations.

The following year in 2018, China outright banned its best vulnerability researchers from traveling abroad for 0day competitions, where they burned vulnerabilities for cash. Instead,

[7] https://www.cfr.org/blog/chinas-new-small-leading-group-cybersecurity-and-internet-management

these vulnerabilities–which China's policy community consider a "national resource"–were forced to remain in the country and surrendered to the security services at competitions like Tianfu Cup.

By 2021, China decided to do something no other government had done–they mandated the collection of software vulnerabilities, a key tool in hacking operations, be reported to the government within 48 hours of discovery by companies "doing business in China."
It should come as no surprise that we see China's hacking teams repeatedly accessing critical infrastructure, corporate trade secrets, and sensitive national security systems.

As a result of these efforts, over the past decade, China has evolved from being one of the noisiest attackers–acting without regard for being caught, while still stealing massive amounts of data–to some of the best and most stealthy hackers on the planet.

In recent years, the People's Liberation Army has tasked a group of its hackers to target American critical infrastructure and develop persistent access to those systems.

This persistent access is all too easy to procure. It will only ever take a few people, with normal laptops and the knowledge of how their targets are vulnerable, to gain and retain persistent access. Deterring this behavior may not be possible.

It is also important to note the sheer scale of Chinese malicious cyber activity is unparalleled anywhere on the globe. Each intrusion is a warning, but the vast size and pace are the true concerns.

China's view that the U.S. military is superior to the People's Liberation Army drives them to pursue asymmetric tools to weaken the U.S., including cyber attacks against our critical infrastructure. The PLA believes cyber, information operations, and anti-satellite weapons are key to winning any military conflict including preventing the United States from intervening on behalf of Taiwan. So while we may be able to deter China from using these capabilities, we are not likely to deter China from preparing for conflict by prepositioning in our critical infrastructure.

Network Complexity

As adversaries grow more sophisticated, our networks have become increasingly complex. The adoption of cloud computing and expansion of remote workforces have further burdened already overextended defenders. In pursuit of constant availability, businesses have pushed technologists to deploy and maintain more tools with less downtime, resulting in poor hygiene. Additionally, the rapid emergence of AI is creating vast new data repositories which carry forward these same challenges.

As a result, our networks evolved into a patchwork of interdependent services and providers, frequently built on legacy technologies predating many current defenders and defenses. These outdated foundations, central to many businesses, have become easy prey for malicious actors.

Over the past decade, a surge in zero-day vulnerabilities targeting these systems has given adversaries a significant advantage. Tools and systems previously considered best-practice for security have quickly been turned against us.

Once-trusted solutions, such as VPN appliances, have become prime targets. Originally intended to protect remote workforces, these devices now represent a significant attack surface due to vulnerabilities and misconfigurations that go undetected or remain unpatched. As adversaries evolve their tactics, widely adopted security measures can be weaponized against any organization slow to adapt.

Vendors responding to market forces have been pushed to deliver new features, to maintain a competitive edge, at the expense of comprehensive testing and secure coding practices. As a result, old classes of vulnerabilities continue to be delivered to customers, providing an avenue for threat actors to gain a foothold. This relentless pressure to innovate often backfires, putting their customers and our infrastructure at even greater risk.

Addressing these gaps calls for a collective effort by businesses, vendors, and both the public and private sectors. There is no single, foolproof solution. As defenders strengthen their controls, attackers will evolve their methods. Emerging technologies like generative AI lower the bar for malicious actors while simultaneously providing defenders with advanced tools to detect and thwart these threats.

Driving meaningful change across the industry demands unified initiatives, such as CISA's Secure By Design, the Known Exploited Vulnerabilities catalog, Zero Trust architectures, and the NIST Cybersecurity Framework. Yet these efforts alone are insufficient. We must empower our defenders with the training and resources to counter modern threats, ensuring they possess the skills necessary to match, and surpass, those of our adversaries.

Policy Recommendations

There are steps that the government and industry must take to weaken our adversaries, bolster U.S. cyber defenses and enhance our resilience.

First, the gravity of this moment - the continually compounding risk posed by an exploding set of cyber threat actors, highlighted by the preparation for war by the Chinese Communist Party - requires serious, straightforward conversation amongst policy makers, elected officials, business leaders, and the American public. We must call our adversaries' activities what they are - preparation for war. Accordingly, we must call them by their names, plainly, and without fanciful marketing terms that only benefit cybersecurity vendor marketing teams and the adversary themselves, by mythologizing and obfuscating. Foreign government hackers positioned to take hospitals offline and turn off the water supply don't deserve flashy codenames, they deserve disdain and confrontation. No more typhoons or blizzards. Instead, we must speak to the American people about the provocations of the Chinese military and the

Russian security services. In no other theatre of conflict do we willingly throw a veil over our adversaries and their malign activities. It must end now.

Second, to ensure that industry retains its ability to share cyber threat information without fear of liability, Congress should reauthorize the Cybersecurity Information Sharing Act of 2015, which expires later this year. This Act is an important tool to facilitate the flow of critical cyber intelligence between industry and government, and letting it expire would be a huge step back. At the same time, the executive branch, led by CISA, should continue to look for ways to enhance public-private operational collaboration. While CISA's Joint Cyber Defense Collaborative is a great tool, there is more that needs to be done to ensure these efforts can achieve the scale and consistency to match the intensity of today's threats.

Third, we need a whole-of-nation effort to engage and encourage our critical infrastructure to improve their security and enhance their systemic resilience. We are never going to stop every cyber attack so our infrastructure needs to be capable of operating in a degraded state and getting back up and running quickly. The Federal Government should be supporting our infrastructure with information, guidance, technical assistance and, in some cases, with funding. That is why Congress should reauthorize and fund the State and Local Cybersecurity Grant Program, so that our resource constrained State and local government agencies can build and sustain minimum cybersecurity capabilities.

Fourth, the federal government should actively promote competition and avoid monoculture in our technology ecosystem, starting with federal networks. Not only will this spur more innovation, but it will help create more robust systems that minimize opportunities for broad systemic failure and disruption. In part, this can be done by maintaining the momentum in recent years of investing in and centralizing cybersecurity capabilities in CISA. The establishment of CISA in 2018, a key cybersecurity win of the first Trump Administration, combined with authorities granted by Congress in 2021 (e.g., persistent threat hunting on federal networks, administrative subpoena, Joint Cyber Planning Office, etc.) and 2022 (Cyber Incident Reporting for Critical Infrastructure Act) have steadily advanced the nation's cybersecurity capabilities. As we all recognize, however, in the modern digital economy, defenses must keep pace with the threats. Therefore, we must continually adapt and improve our defensive posture, including how we are organized, how we are resourced, how we interact across stakeholder groups, and how we respond. In that spirit, we believe elements of last week's Executive Order on cybersecurity and artificial intelligence continue much-needed forward progress on defending federal networks, such as the accelerating persistent threat hunting and strengthening the security of internet routing. I encourage the Administration and Congress alike to carefully evaluate the positive advances of the prior Administration's cybersecurity executive actions and retain those that put Federal networks and the private sector alike into the best possible position to defend against constantly evolving cyber threats.

Fifth, the U.S. government should continue to foster our global edge in innovation in emerging and next generation technologies such as Artificial Intelligence (AI), particularly in the cybersecurity space and quantum computing. Today, AI is being more quickly integrated into

cybersecurity tools, such as SentinelOne's PurpleAI, than our adversaries are able to integrate AI into their cyber weapons. In cybersecurity, speed kills, and AI-powered tools give defenders the ability to identify, investigate, and mitigate threats faster than ever before. If we want that to persist, we will need to ensure that the U.S. and its allies continue to lead the growth and development of AI, and that attempts to address potential AI risks don't create barriers to broader AI adoption. The PRC's enormous investments in quantum-related research and development threatens U.S. leadership as we look ahead to the emergence of quantum computing with the potential to revolutionize fields, from medicine to material science to AI, while putting much of today's encryption at risk. Congress and the executive branch must work together to ensure that not only does the U.S. win the race for supremacy in quantum computing, but that American businesses and government agencies are ready to upgrade systems to post-quantum cryptographic standards now that the National Institute of Standards and Technology (NIST) has released its first set of quantum resistant algorithms.

Sixth, the U.S. government should aggressively pursue and counter adversary activity wherever it originates from. The takedown of LockBit in early 2024 is an excellent case study. In February of last year, Operation Cronos demonstrated to LockBit affiliates and would-be victims that the group cannot be trusted to delete data after ransoms are paid–this hit a key component of the attacker-victim relationship, trust.[8] More recently, the operation against the Chinese actor, Twill Typhoon, by the DOJ and the FBI demonstrates the opportunities to disrupt nation state cyber threats.

Seventh, our alliances provide tremendous value in cyber space. Takedown after takedown of ransomware operators and criminal groups make clear the value of intelligence sharing and operational coordination across allied nations. More importantly, when attempting to address the intrusions by nation state actors, such as China and Russia, intelligence sharing agreements between like-minded nations, information sharing on adversary tactics, unified messaging and joint action are all critical in preparing for, stopping and countering adversary action.

Conclusion

Our nation continues to face unprecedented risks in cyberspace and our success in addressing this challenge is dependent on how effectively the government, industry and allies work together. No one organization or company can do this on their own. We need the unique expertise, skills and authorities resident across these communities, and time is not on our side. I applaud the Committee for making this subject its first hearing of the 119th Congress, and I look forward to working with the Committee in the months ahead.

[8] https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/