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)