TESTIMONY OF Mr. Zachary Tudor

Associate Laboratory Director, IDAHO NATIONAL LABORATORY

before the

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON ENERGY

concerning

"Securing America's Energy Infrastructure:
Addressing Cyber and Physical Threats to the Grid"

December 2, 2025

Chairman Latta, ranking member Castor, and members of the committee, thank you for the opportunity to testify on a topic critical to our nation's security. My name is Zach Tudor, and I am the associate laboratory director for National and Homeland Security at the Idaho National Laboratory (INL). I am a cybersecurity expert by education and trade, and I have spent most of my professional and military careers focused primarily on operational technology (OT) cybersecurity and the protection of United States (U.S.) critical infrastructure. The directorate I lead consists of nearly 900 scientists, engineers, cyber researchers, analysts, and staff dedicated to safeguarding the United States from the most consequential foreign and domestic threats, including cybersecurity threats that aim to disrupt our nation's energy supply, clean water, telecommunications, and other critical functions. We are among the best in the world at understanding threats to critical infrastructure and, more importantly, developing solutions that protect our nation's critical functions from attacks.

INL, managed by Battelle Energy Alliance, LLC, is one of 17 U.S. Department of Energy (DOE) national laboratories. Located in Idaho Falls, Idaho, INL employs more than 6,100 researchers and support staff with a common vision: to change the world's energy future and secure our nation's critical infrastructure. The national security mission I lead focuses on protecting the

nation's critical infrastructure, preventing the proliferation of weapons of mass destruction, and providing direct support to America's warfighters. Our decades of nuclear innovation—52 reactors built and tested, with next-generation demonstrations underway—forged INL's distinctive approach to securing critical systems distinctive for a deep understanding of OT and of the cybersecurity and engineering needed to secure systems and provide critical function assurance. INL's 890-square mile Site provides unique infrastructure to test threats and mitigations to our critical systems at scale.

Lay of the Land: Cyber Threats to U.S. Critical Infrastructure

The United States faces an unprecedented wave of cyber threats directed at our critical infrastructure. The 2025 Annual Threat Assessment of the U.S. Intelligence Community underscores this reality: Adversarial states are conducting aggressive campaigns to pre-position themselves within U.S. networks, with the goal of breaking our resolve and limiting our response options at a time of their choosing. Among these adversarial states, China, Russia, Iran, and North Korea stand out as key actors with distinct capabilities and motivations.

China is the most persistent and capable threat, embedding itself into OT networks across sectors. According to recent analysis from the Foundation for Defense of Democracies, China has significantly escalated its cyber-enabled economic warfare operations, targeting the U.S. through intellectual property theft, critical infrastructure intrusions, and mass collection of personally identifiable information.[1] Beijing's strategy aims to control global information and communications technology infrastructure, leveraging technology to manipulate vast amounts of

[1] Ravish, S., M. Montgomery. 2022. "China's Accelerating CEEW Campaign." Foundation for Defense of Democracies, CEEW Campaign. Last modified October 28, 2022. https://www.fdd.org/analysis/2022/10/28/chinas-accelerating-ceew-campaign/

data and disrupt essential services. This ambition is further supported by aggressive industrial policies and extensive legal frameworks that merge commercial ventures with intelligence collection, allowing China to access information from firms under its jurisdiction and blurring the lines between economic activity and espionage.[2] This multifaceted cyber and technological offensive poses a severe threat, underscoring China's intent to undermine U.S. economic stability and national security without direct military confrontation. As such, it is imperative for the United States to bolster its defenses and regulatory mechanisms against these insidious attacks.

Similarly, Russia seeks disruptive capabilities, demonstrated by its attacks against Ukraine's energy infrastructure, supply-chain assaults, and constant probing of U.S. industry and infrastructure. Iran has shown willingness to cause disruption for political leverage, particularly against water and oil resources. North Korea remains financially motivated but opportunistic, with capabilities extending into energy and telecommunication targets.

Although the United States is not the only nation in the crosshairs of these advanced, persistent cyber actors, the unique makeup of our critical infrastructures and key resources makes us particularly vulnerable. Our interdependent systems and heavy reliance on technology amplify the potential impact these threat actors pose. The modern-day risk environment in the United States is extensive and evolving because our critical infrastructures include:

---

[2] Burnham, J., J. Yang. 2025. "Protecting Our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control." Foundation for Defense of Democracies, Public Comment. October 6, 2025. https://www.fdd.org/analysis/2025/10/06/protecting-our-communications-networks-by-promoting-transparency-regarding-foreign-adversary-control-2/

- **Interconnected Systems –** Energy, telecommunications, transportation, and water systems are deeply interdependent. A disruption in one sector often cascades across others, worsening the potential damage and complicating response efforts.
- **Unique U.S. Exposure –** Unlike other nations, the U.S. operates vast, digitized, and largely privately owned infrastructure. The sheer size and intricacy of our critical infrastructure systems and networks create significant challenges in implementing unified security measures across all sectors, increasing the potential for gaps in protection.
- **Aging Infrastructure –** Much of the critical infrastructure in the U.S. is aging, with many systems operating well past their intended life cycle. Consequently, many of these systems remain vulnerable to cyberattacks.
- **Lag in Security Upgrades –** The long lifecycle of industrial control systems, often operating for 30–40 years, ensures simplicity and efficiency. However, this results in a lag in adopting modern security technologies and standards. Consequently, these systems are more vulnerable to advanced cyberattacks, leaving critical infrastructure exposed to evolving threats.
- **Attractive Targets –** Infrastructure assets are both symbolic and practical targets. Disruption in these areas can have a significant impact on human health and safety, economic stability, and national security, making them highly attractive to adversarial actors.

Given that foreign adversaries are likely to continue their persistent use of cyberattacks against our critical infrastructure, it is essential for policymakers to understand their methods and distinct motivations.

Key State Actors

The cybersecurity landscape is dominated by several key state actors, each with unique capabilities and objectives. China, Russia, Iran, and North Korea are routinely identified as the primary adversaries targeting U.S. critical infrastructure. Their actions range from espionage and intelligence gathering to disruptive attacks and financial extortion, posing significant risks to national security, economic stability, and human health and safety.

China – The People's Republic of China (PRC) pursues long-term, stealthy cyber operations to collect intelligence, pre-position access, and prepare options for disruptive effects in the event of a crisis. The PRC favors a strategy denoted by asymmetrical actions, including winning without fighting, or achieving strategic objectives by undermining an adversary's confidence and capabilities without engaging in direct conflict. This approach is a key aspect of irregular warfare, defined as a form of warfare in which states and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities.[3]

In recent years, the U.S. has been the victim of this strategic approach as hacking campaigns[4] like Salt, Volt, and Flax Typhoon demonstrate how state-sponsored entities are infiltrating our digital ecosystems to steal sensitive data and embed themselves in our communications, industrial, and defense networks. Prominent organizations, including Microsoft,[5] Tenable,[6] and

---

[3] Theohary, C. A. 2024. "Defense Primer: What Is Irregular Warfare?" Congressional Research Service, Product Number IF12565. November 29, 2024. https://www.congress.gov/crs-product/IF12565

[4] Singleton, C., et al. 2025. "Countering Threats Posed by the Chinese Communist Party to U.S. National Security." Foundation for Defense of Democracies, Congressional Testimony. March 5, 2025. https://www.fdd.org/wp-content/uploads/2025/03/03-05-25-Singleton-Written-Testimony-Final-1.pdf

[5] Microsoft Threat Intelligence. 2023. "Volt Typhoon Targets U.S. Critical Infrastructure with Living-Off-The-Land Techniques." Microsoft, Research. Last modified May 24, 2023. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[6] Caveza, S. 2025. "Salt Typhoon: An Analysis of Vulnerabilities Exploited by this State-Sponsored Actor." Tenable, Blog, Cyber Exposure Alerts. Last modified January 23, 2025. https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor

Dragos,[7] along with government agencies, such as the Cybersecurity and Infrastructure Security Agency,[8] the Federal Bureau of Investigation,[9] and the National Security Agency,[10] have confirmed that these campaigns remain active and continue to target critical infrastructure and key resources across the United States. Through these campaigns, the Chinese Communist Party is setting the conditions[11] to execute destructive cyberattacks against the United States should there be a regional conflict in the Pacific over Taiwan. These efforts are part of China's broader strategy to weaken our infrastructure and undermine our willingness to engage in a prolonged conflict.

Most concerningly, China's aim is to conduct espionage and pre-position themselves on the IT networks of U.S. critical infrastructure while remaining undetected for as long as possible, providing them with a rapid capability to disrupt or destroy our critical infrastructure at the time and place of their choosing. These sophisticated campaigns have knowingly impacted critical infrastructure sectors, including energy, communications, manufacturing, utilities, transportation, construction, maritime, government, information technology, and education.

---

[7] Hanrahan, J. 2024. "VOLTZITE Espionage Operations Targeting U.S. Critical Systems." Dragos Safeguarding Civilization, Intelligence Brief. Last modified February 2024. https://hub.dragos.com/hubfs/116-Datasheets/Dragos_SB_IntelVOLTZITE_Feb24_FINAL_r4.pdf?hsLang=en

[8] CISA. 2024. "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure." News & Events, Cybersecurity Advisory. Last modified February 7, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[9] Leatherman, B. 2025. "FBI Announces Joint Cybersecurity Advisory Related to Salt Typhoon." U.S. Federal Bureau of Investigation. Video, August 27, 2025. https://www.fbi.gov/video-repository/salttyphoon082725.mp4/view

[10] National Security Agency/Central Security Service. 2025. "NSA and Others Provide Guidance to Counter China State-Sponsored Actors Targeting Critical Infrastructure Organizations." Press Release, August 27, 2025. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/

[11] Harper, J. 2025. "Air Force Cyber Leader Warns Threats Like Volt Typhoon Could Enable China to Wage 'Total War' Against US." DefenseScoop. Last modified September 23, 2025. https://defensescoop.com/2025/09/23/volt-typhoon-china-us-air-force-cyber-defensive-operations/

Russia – Russia continues to pose a credible threat to the U.S. across the cyber domain despite the current constraints they face from the war in Ukraine. Russian state-sponsored cyber actors routinely engage in espionage, pre-positioning access, campaigns that compromise supply chains, and sabotage. The Russian cyber threat is multifaceted, blending state-sponsored actors like military and intelligence services with hacktivist groups, and more traditional criminal organizations.[12]

From ransomware attacks that extort millions of dollars to major supply-chain attacks for covert intelligence gathering, the Kremlin's cyber strategy integrates technical and psychological operations within its concept of information confrontation[13] to achieve strategic objectives, often below the threshold of armed conflict, sometimes referred to as irregular warfare. They combine offensive measures like infrastructure attacks with defensive efforts such as "digital sovereignty," leveraging state actors, proxies, and false flags to exploit open systems and obscure attribution.[14] Furthermore, a recent Atlantic Council report thoroughly examined Russia's intensifying bilateral ties with China, Iran, and North Korea. The report conveys the particularly close relationship between Russia and China, particularly related to critical military capabilities including artificial intelligence, quantum computing, and space technology.[15]

---

[12] Sherman, J. 2022. "Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior." Atlantic Council, Cyber Statecraft Initiative, Issue Brief, September 2022. https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Untangling-the-Russian-Web-Spies-Proxies-and-Spectrums-of-Russian-Cyber-Behavior-1.pdf

[13] Voo, J., Singh, V. V. 2025. "Russia's Information Confrontation Ecosystem." IISS, Charting Cyberspace. Last modified June 26, 2025. https://www.iiss.org/charting-cyberspace/2025/06/russias-information-confrontation-ecosystem/

[14] Hakala, J., J. Melnychuk. 2021. "Russia's Strategy in Cyberspace." 978-9934-564-90-1, NATO Strategic Communications Centre of Excellence.

[15] Stent, A. 2025. "THE CRINK: Inside the New Bloc Supporting Russia's War Against Ukraine." Atlantic Council, Eurasia Center. https://www.atlanticcouncil.org/wp-content/uploads/2025/10/the-crink-inside-the-new-bloc-supporting-russias-war-against-ukraine.pdf

In the last decade, Russia has emerged as a major source of cyberattacks against global critical infrastructure, both through state-sponsored operations and cybercriminal groups operating from Russian territory. Notable attacks include the 2015 BlackEnergy and 2016 Industroyer campaigns against Ukrainian power companies, the 2017 NotPetya attack that began in Ukraine and spread globally causing billions in damages, the Triton malware attack on a Saudi Aramco petrochemical plant, the 2020 SolarWinds supply-chain compromise, and the 2021 Colonial Pipeline ransomware attack by the Russia-based DarkSide group. Many of these attacks initiated in information technology (IT) networks and then propagated to OT systems through their interconnections.

With the war in Ukraine, Russian cyber activity has only increased with the FBI warning that a Russian cyber-espionage group has targeting a known vulnerability in CISCO equipment to go after telecommunications, higher education, and manufacturing sectors across North America, Asia, Africa, and Europe. In 2024, Russian-linked hacking groups carried out a cyberattack against a Texas water treatment facility that caused a tank to overflow. The incident led national security agencies to issue a stark warning to the more than 170,000 private U.S. water and wastewater treatment facilities to shore up their cyber defenses. Two months ago, European leaders were briefed on two cyberattacks that targeted water systems in Norway and Poland, both linked to Russian hackers.

Iran – According to the Institute for National Security Studies, Iran's cyber capabilities can disrupt, sabotage, and destroy civil and commercial targets, critical national infrastructure, and military capabilities.[16] Their cyber espionage and information operations have grown over time

[16] Freilich, C. 2024. "The Iranian Cyber Threat." The Institute for National Security Studies. Accessed November 20, 2025. https://www.inss.org.il/publication/iranian-cyber/

and represent a significant threat, particularly to the United States, Israel, and Saudia Arabia. They have steadily improved their cyber warfare capabilities, with espionage, sabotage, and revenge as core motivations. Experts characterize Iran's cyber ambitions as asymmetrical, clandestine, and focused on plausible deniability, mixing state-sponsored actions with sympathetic hacktivist organizations that together complement the well-understood proxy and shadow operations the Islamic Republic has favored for decades.[17]

Regarding specific critical infrastructure threats, Iran has in recent years actively targeted U.S. water, energy, manufacturing, and healthcare organizations after finding success executing similar campaigns against Israel in response to the Israel-Hamas conflict.[18] In 2023, a water authority near Pittsburgh, Pennsylvania, was breached by state-sponsored Iranian hackers and forced to shut down parts of their IT and OT networks. Though the water supply remained safely available to customers, the hackers managed to shut down a pump on a supply line that provided drinking water from the plant to local communities.[19] Reports of similar compromises affecting Unitronics Vision Series programmable logic controllers were reported by companies operating energy, food, beverage manufacturing, and healthcare equipment in several states.

In 2024, an international contingent of national security organizations issued an updated advisory to warn critical infrastructure equipment owners and operators of continued malicious cyber

---

[17] Daragahi, B. 2023. "Iran is Using its Cyber Capabilities to Kidnap its Foes in the Real World." Atlantic Council, IranSource. Last modified May 24, 2023. https://www.atlanticcouncil.org/blogs/iransource/iran-cyber-warfare-kidnappings/

[18] CISA. 2025. "Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest." Accessed November 20, 2025. https://www.ic3.gov/CSA/2025/250630.pdf

[19] Counter Threat Unit Research Team. 2023. "Iranian Cyber Av3ngers Compromise Unitronics Systems." Last modified December 7, 2023. https://www.secureworks.com/blog/iranian-cyber-av3ngers-compromise-unitronics-systems

activity by Iranian-affiliated cyber actors.[20] This joint advisory was informed by recent FBI investigations and included new information on likely tactics, techniques, and procedures the Islamic Republic could use against U.S. critical infrastructure. This year, several U.S. national security organizations published an updated factsheet detailing increased cyber threats and risks against U.S. critical infrastructure by Iranian state-sponsored or affiliated threat actors.[21] Of particular concern, the agencies noted that defense industrial base companies with relationships in or with Israeli research and defense firms were at greater risk.

North Korea – North Korea has emerged as a persistent player in the cyber domain, leveraging its capabilities to conduct espionage, theft, and disruptive attacks against its perceived enemies. While their tactics often lack the scale of more sophisticated adversaries like China and Russia, they frequently deploy harassment and nuisance strategies designed to sow confusion, frustration, and financial loss. The regime's state-sponsored hackers often target financial institutions, critical infrastructure, and government agencies.

North Korea is known for aggressive cyber operations, including the 2014 Sony Pictures hack and the 2017 WannaCry ransomware attack.[22] These attacks demonstrate their capability for cyber warfare and use of cybercriminal activities to fund their regime. In 2024, global companies lost $1.34 billion[23] to North Korean cyberattacks. Earlier this year, North Korean hackers stole

---

[20] CISA. 2024. "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities." Last modified December 18, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

[21] CISA. 2025. "Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest." Accessed November 20, 2025. https://www.ic3.gov/CSA/2025/250630.pdf

[22] U.S. Department of Justice. 2018. "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." Archives, Press Release, September 6, 2018. https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

[23] Chainalysis Team. 2024. "$2.2 Billion Stolen from Crypto Platforms in 2024, but Hacked Volumes Stagnate Toward Year-End as DPRK Slows Activity Post-July." Chainalysis. Last modified December 19, 2024. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/

$1.5 billion in cryptocurrency through the ByBit exchange.[24] Beyond financial theft, the North Korean regime has been linked to various cyber intrusions aimed at gathering intelligence on military capabilities and critical infrastructure in adversarial nations, particularly the U.S. and South Korea.

Cybersecurity firms like Mandiant[25] and CrowdStrike[26] have reported on North Korean cyber tactics, revealing a focus on stealth and deception designed to evade detection. As geopolitical tensions continue, North Korea is expected to further employ its cyber capabilities to conduct disruptive operations and espionage, posing an ongoing threat to U.S. and allied national security.

Sector-Specific Threats

Conducting a cyberattack against the specialized computer systems controlling critical infrastructure is difficult. Such attacks usually require significant resources and months or years of preparation. However, our adversaries have learned that they can degrade or destroy critical infrastructure by targeting the easier-to-compromise IT networks that support these systems. Because IT and OT systems are intertwined across every critical infrastructure sector, this approach provides adversaries with widespread opportunities for disruption.[27] Adversaries have recognized these vulnerabilities, and they are adapting their strategies accordingly. Cyber threats

---

[24] CSIS. 2025. "The ByBit Heist and the Future of U.S. Crypto Regulation." Last modified March 18, 2025. https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation

[25] Fraser, N., et al. 2018. "APT38: Details on New North Korean Regime-Backed Threat Group." Google Cloud, Threat Intelligence. https://cloud.google.com/blog/topics/threat-intelligence/apt38-details-on-new-north-korean-regime-backed-threat-group

[26] Kapko, M. 2025. "CrowdStrike Investigated 320 North Korean IT Worker Cases in the Past Year." Cyberscoop. Last modified August 4, 2025. https://cyberscoop.com/crowdstrike-north-korean-operatives/

[27] Brumfield, C. 2025. "Foreign Hackers Breached a US Nuclear Weapons Plant via SharePoint Flaws." CSO, News Analysis. Last modified October 20, 2025. https://www.csoonline.com/article/4074962/foreign-hackers-breached-a-us-nuclear-weapons-plant-via-sharepoint-flaws.html

are a function of both adversary capability and intent. Not only are adversary capabilities becoming stronger and more sophisticated each year, but we are also seeing changes in their intent to use those capabilities against critical infrastructure. While the nation has developed better resilience, we have not kept pace with this growing threat, leaving us more vulnerable than ever before.

Electric Power Grid

The U.S. electric grid is indispensable. It is the foundation for healthcare, communications, national defense, and societal functioning, but also a prime target. Russian cyber operations against Ukraine's grid in 2015 and 2016 proved that remote power disruption is viable. More recently, the emergence of the Industroyer2 malware in 2022 confirmed our adversaries continued tool development for grid attacks.[28] In 2023, analysts disclosed that China's Volt Typhoon group had infiltrated U.S. utility networks with the intent of long-term positioning for disruption. The previously mentioned 2025 Annual Threat Assessment of the U.S. Intelligence Community warns Russia and China are advancing capabilities that could disable segments of the U.S. grid during a major crisis. The emergence of artificial intelligence (AI) has shown promise in both the ability to enhance grid operations and defend the grid from cyberattacks, but it also introduces risks and conditions that could be exploited by adversarial cyber actors.[29]

Oil and Natural Gas

The 2021 Colonial Pipeline ransomware attack showed how crippling an energy infrastructure

---

[28] Tidy, J. 2022. "Ukrainian Power Grid 'Lucky' To Withstand Russian Cyber-Attack." BBC. Last modified April 12, 2022. https://www.bbc.com/news/technology-61085480

[29] Industrial Cyber. 2025. "INL's TAIGR Initiative Confronts AI Hallucinations, Cyberattacks, Other Risks Threatening Power Grid Stability." Last modified August 13, 2025. https://industrialcyber.co/utilities-energy-power-water-waste/inls-taigr-initiative-confronts-ai-hallucinations-cyberattacks-other-risks-threatening-power-grid-stability/

intrusion can be. Fuel shortages, panic buying, and emergency action by government all followed. State actors continue probing the oil and gas domain. Russian -and Iranian-linked groups have scanned pipeline control systems, while Cybersecurity Infrastructure Security Agency (CISA) and private firms report attempts to access programmable logic controllers (PLC) in energy facilities. Iran's focus on utilities and U.S. infrastructure includes efforts to compromise PLCs and remote automation systems.[30] Russia's historical interest in mapping pipeline networks in Europe raises concern about similar probing in North America.[31] Aging infrastructure, fragmented ownership, and reliance on just-in-time logistics amplify the risk: Disruption or loss of control could cascade through transportation, manufacturing, and nation-wide fuel markets.

Telecommunications

Telecommunications networks are the nervous system linking other critical sectors. China's embedding of hardware vulnerabilities in routers and switches continues to pose deep structural risk.[32] Meanwhile, Russian and Iranian groups target satellite networks and undersea cables, essential conduits for military and civilian communications. For instance, packet routing disruptions and satellite degradations have been observed during Russia's offensive in Ukraine, affecting users across Europe.[33] In September, the U.S. Secret Service dismantled a network of electronic devices located throughout the New York tristate area that were capable of disabling

---

[30] Greenberg, A. 2025. "CyberAv3ngers: The Iranian Saboteurs Hacking Water and Gas Systems Worldwide." Wired, Security. Last modified April 14, 2025. https://www.wired.com/story/cyberav3ngers-iran-hacking-water-and-gas-industrial-systems/

[31] Jones, S. 2025. "Russia's Shadow War Against the West." Center for Strategic and International Studies. Last modified March 18, 2025. https://www.csis.org/analysis/russias-shadow-war-against-west

[32] CISA. 2025. "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System." Last modified September 3, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

[33] CSIS. 2022. "Russia Threatens to Target Commercial Satellites." Last modified November 10, 2022. https://www.csis.org/analysis/russia-threatens-target-commercial-satellites

cell phone towers, enabling denial of services attacks, and facilitating anonymous, encrypted communication.[34] As next-generation communication systems, software-defined networking, and edge computing proliferate, infrastructure operators and contractors become higher-value targets. Disruptions to telecom could magnify breakdowns across energy, water, and emergency response.

Water Systems

Water utilities are comparatively under-resourced for cybersecurity, with many lacking full-time cyber personnel or real-time monitoring systems.[35] In 2023, Iranian-aligned hackers forced a Pennsylvania water utility to cease operations in portions of its system. The U.S. Environmental Protection Agency has warned that over 70% of surveyed U.S. water systems fail to meet basic cybersecurity best practices.[36] Even brief disruptions in pumping or treatment can compromise public health, making water infrastructure a vulnerable and high-stakes domain.

The Role of the National Laboratories and Idaho National Laboratory

DOE's national laboratories play a critical role in addressing the national security challenges facing our nation. As Federally Funded Research and Development Centers, the labs conduct cutting-edge research and development in the national interest, addressing the nation's long-term needs with expertise and capabilities that private industry and academia cannot, will not, or

---

[34] U.S. Secret Service. 2025. "U.S. Secret Service Dismantles Imminent Telecommunications Threat In New York Tristate Area." Last modified September 23, 2025. https://www.secretservice.gov/newsroom/releases/2025/09/us-secret-service-dismantles-imminent-telecommunications-threat-new-york

[35] Industrial Cyber. 2025. "FDD Experts Warn EPA Cyber Grants are a 'Drop in the Bucket' as Attacks Escalate, Call for Expanded Support." Last modified August 26, 2025. https://industrialcyber.co/utilities-energy-power-water-waste/fdd-experts-warn-epa-cyber-grants-are-a-drop-in-the-bucket-as-attacks-escalate-call-for-expanded-support/

[36] EPA. 2024. "EPA Outlines Enforcement Measures to Help Prevent Cybersecurity Attacks and Protect the Nation's Drinking Water." Last modified May 20, 2024. https://www.epa.gov/newsreleases/epa-outlines-enforcement-measures-help-prevent-cybersecurity-attacks-and-protect

should not perform. Our operations are governed by federal statutes and guidelines to ensure objectivity, facilitate technology transfer, and encourage collaboration with external partners.

The INL national security mission is primarily focused on securing our nation's 16 critical infrastructure sectors through strategic efforts that protect and ensure the functionality of industrial control systems and OT. Since the late 1990s, INL has been a seminal leader in securing industrial control systems, OT, and critical infrastructure from cyber and physical threats. Our expertise is widely recognized and referenced in industry publications, academic journals, government reports, and congressional testimony. Our leaders frequently provide advice and counsel, perform technical engagements, conduct product evaluations, lead comprehensive training, and speak at leading conferences, forums, and events. In short, we have been at the forefront of defending critical infrastructure from cyber and physical threats for more than two decades, building the expertise, facilities, capabilities, curriculum, and test and evaluation ranges to support key federal agencies, including the DOE, Department of Homeland Security, the War Department, and the Intelligence Community.

Examples of our contributions include these:

- **Supply-Chain Security:** This involves the protection of vast networks of manufacturers, software vendors, and logistics providers that function in near-constant coordination. These networks are only as strong as their weakest link. A single compromised supplier, outdated component, or misconfigured cloud service can ripple through hundreds of companies at once, halting production, exposing sensitive data, or corrupting critical systems. Foreign adversaries know this and often use supply-chain compromise as a weapon intentionally disrupting supply chains. In fact, recent analysis suggests adversaries are increasingly exploiting trusted relationships within the supply chain.

Instead of direct breaches, they compromise the connections between vendors and clients, software platforms and users, administrators and networks, and developers and use the supply chain as a vehicle to compromise unsuspecting victims. As seen in the recent F5 hack, foreign adversaries are embedding themselves through stolen credentials, hijacked update channels, or vendor compromise to gain persistent access that bypasses traditional defenses.[37] This stealthy approach provides extended presence with reduced detection risk, lowers operational costs, and undermines fundamental assumptions in cyber defense frameworks.[38] Ensuring the integrity and security of the supply chain is essential to mitigating risks and protecting the infrastructure that supports the nation's critical systems. At INL, we lead multiple national efforts to improve supply-chain security for industrial control systems and OT. All these programs start with the ideas of prioritizing and addressing risk based on impact through a comprehensive understanding of critical-function delivery. Pioneered by INL researchers, critical function assurance is an approach to prioritizing and addressing risk based on impact and is rooted in a holistic understanding of how critical functions are delivered.[39] It provides rapid focus to what matters most and illuminates elements and areas of risk that otherwise are often overlooked. Supply-chain security is often overlooked but essential to critical infrastructure security. Programmatic efforts supporting Critical Function Assurance (CFA) are these:

---

[37] CISA. 2025. "ED 26-01: Mitigate Vulnerabilities in F5 Devices." Last modified October 15, 2025. https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices

[38] Booz Allen. 2025. "Breaking Through: How to Predict, Prevent, and Prevail over the PRC Cyber Threat."

[39] Gellner, J. R., et al. 2023. "CRITICAL FUNCTION ASSURANCE: Understanding Critical Function and Critical Function Delivery is Foundational for Meaningful ICS Security Improvement and Policy Efforts." INL/MIS-23-75497-Revision-0, Idaho National Laboratory.

- **Cyber-Informed Engineering (CIE):** Integrating cybersecurity considerations into the engineering design process, CIE aims to mitigate potential threats, including those within the supply chain. By incorporating cybersecurity measures from the earliest stages of system development, CIE ensures that industrial control systems and their supply chains are inherently more secure and resilient against cyberattacks. Through support from DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), INL leads in implementing the national strategy by developing engineering tools, standards, and educational resources that prioritize cybersecurity in infrastructure design and operation.
- **Consequence-driven Cyber-informed Engineering (CCE):** Hands-on, scenario-based engagements incorporated into CCE are designed to strengthen system resilience, including in-depth analysis of supply-chain processes. This approach emphasizes understanding the potential consequences of cyber threats across a company's entire operation and develops strategies to protect critical functions, thereby enhancing the overall security posture of industrial control systems. Multiple federal agencies, including DOE and the Department of War (DoW), support and fund CCE engagements.
- **Cyber Testing for Resilient Industrial Control Systems (CyTRICS):** A DOE CESER program, CyTRICS is led by INL and supported by six national laboratories. Focused on identifying and remediating vulnerabilities within energy supply chains, CyTRICS conducts rigorous testing and evaluation of hardware and software components used in the energy sector. By leveraging the expertise of multiple national laboratories, CyTRICS aims to enhance the security and

resilience of industrial control systems and their supply chains, ensuring the reliability of the nation's energy infrastructure and safeguarding it against potential cyber threats.

- **Infrastructure Testing:** INL conducts comprehensive infrastructure testing to identify and mitigate cyber and physical vulnerabilities in industrial control systems, power grid equipment, communication networks, and other critical components. The test range sits within INL's 890-square mile site and is equipped with utility-scale electric grid test beds, secure radio-frequency environments for wireless communications, and a national security test range for testing against physical threats. It also includes an uncrewed aerial systems airfield for Unmanned Aerial Systems (UAS) and counter-UAS testing and integration. These facilities support federal and industrial collaborators, including the DOE, DoW, National Nuclear Security Administration, and the Department of Homeland Security.
- **Workforce Development:** INL addresses the critical need for a skilled workforce in the national security sector through hands-on training, education, and professional development. Collaborating with academic institutions, industry partners, and government agencies, we develop curricula and training programs focused on cybersecurity, physical security, advanced engineering, and OT. Practical experience opportunities are provided through internships, fellowships, and cooperative education programs. We collaborate with states and universities to strengthen cybersecurity across critical infrastructure sectors. Partnerships with institutions such as the University of Texas San Antonio, the University of South Florida, and the University of Utah, as well as non-government organizations like Cyber Florida and the FORGE Institute, help

develop technical solutions and cybersecurity talent. The laboratory also partners with the U.S. Department of Homeland Security's CISA and DOE CESER to offer training courses for securing industrial control systems. Training programs like ICS 300/301, Accelerate, CyberStrike, and the Fundamentals of Industrial Control Systems provide immersive training for industry professionals. Specialized training, such as Nuclear Cybersecurity, addresses unique security challenges for advanced reactor technology, while large-scale exercises like Liberty Eclipse prepare private utilities for coordinated defense of energy systems. The Operational Technology Defender Fellowship further develops OT cybersecurity leaders across various energy sectors.

- **Countering Irregular Warfare:** Foreign adversaries pose complex and ongoing threats to the nation's critical functions, using cyber access and advanced capabilities to weaken the U.S. without direct confrontation. To counter these threats, INL established the Special Activities Office (SAO) to provide technical support for defending against irregular warfare. Irregular warfare uses asymmetric and indirect tactics to erode a nation's power and will. The SAO leverages INL's expertise in cybersecurity, wireless communications, materials science, and UAS/counter-UAS to develop technology, training, and specialized services that mitigate these threats. Collaborating with government, industry partners, and other national laboratories, the SAO deploys advanced technologies to support irregular warfare deterrence.

Conclusion

America's adversaries are not waiting. They are already embedded in our systems, mapping our infrastructure, and preparing to disrupt critical operations at a time of their choosing. The threat is no longer hypothetical. Cyberattacks on energy infrastructure are a daily reality and a growing

strategic weapon. Congress has a vital role to play in ensuring that policy, funding, and oversight match the scale of the challenge. Going forward, the most pressing need is increased research and capability development in two critical areas: (1) resilience, so critical services can continue to be delivered even during a cyberattack, and (2) deterrence, so adversaries know there will be consequences to any attack they conduct. We must do the following:

- Accelerate public-private partnerships to secure infrastructure.
- Provide resources to state and local governments in alignment with Executive Order 14239.
- Promote the State and Local Cybersecurity Grant Program to support regional cybersecurity efforts. The recent House passage of the PILLAR Act is a positive development.
- Establish an interagency task force coordinating the federal response to Chinese state-sponsored cyber threats, including Volt Typhoon.
- Continue and expand partnerships with the national laboratories to advance OT security, with emphasis on resilience and deterrence capabilities.
- Increase international coordination to deter adversarial actions.

At INL, we have been tracking cyber threats for decades, historically, those threats centered on espionage and financial theft. Today's threats aim to disrupt and destroy critical infrastructure. We are more concerned than ever before, and you should be too. We face a defining test of resilience and critical function assurance. If we act decisively, we can safeguard the systems that power America's economy and protect our way of life.

Thank you, and I look forward to your questions.