Operational Technology Cybersecurity Coalition

U.S. House of Representatives

Committee on Homeland Security

Subcommittee on Cybersecurity and Infrastructure Protection

Fully Operational: Stuxnet 15 Years Later and the Evolution of Cyber Threats to Critical Infrastructure

Written Testimony of Tatyana Bolton

Executive Director

Operational Technology Cybersecurity Coalition

July 22, 2025

Chairman Garbarino, Ranking Member Swalwell, and members of the subcommittee; on behalf of the Operational Technology Cybersecurity Coalition, thank you for the opportunity to share our perspective on the threat Iran poses to operational technology and critical infrastructure, as well as the broader state of critical infrastructure security in the United States. I commend the subcommittee for prioritizing critical infrastructure security and holding this hearing to discuss the heightened threat landscape.

My name is Tatyana Bolton, and I am the Executive Director of the OTCC, where I lead a group of cybersecurity organizations, critical infrastructure owners and operators, and thought leaders. Representing the entire OT lifecycle and with decades of experience protecting our nation's critical infrastructure assets, we believe that the strongest, most effective approach to securing our collective defense is one that is open, vendor-neutral, and allows for diverse solutions. I look forward to discussing our perspective on Iranian cyber threats and the state of critical infrastructure resilience in the United States.

What Has Changed

Stuxnet, discovered in 2010, marked a pivotal moment in cyber operations by demonstrating that digital tools could indeed cause real-world physical destruction. This sophisticated cyberattack targeted Iran's nuclear enrichment program, manipulating industrial control systems (ICS) to subtly alter centrifuge rotation speeds while feeding back normal data, ultimately destroying nearly 1,000 centrifuges and setting back Iran's nuclear program by years.

Since Stuxnet, the cyber landscape has undergone significant transformation. The nature of the threats we face has evolved. While Stuxnet utilized physical USB drives, today's cyber actors increasingly employ phishing, social engineering, and credential theft as primary vectors of attack. Furthermore, they are progressively striking more significant entities, as evidenced by the Volt Typhoon attack, which should prompt serious reflection on the priority given to and methods used for securing critical infrastructure. They stay on networks longer, sometimes going unnoticed for several years, putting our most sensitive networks at risk.

Adversaries have expanded their cyber operations. Iranian actors specifically have targeted critical infrastructure entities, focused on water and energy sectors, performed defacements, data exfiltration, and ransomware attacks. They have also developed strong relationships with cyber criminal groups and increased their use of information operations. Other actors are targeting critical infrastructure to establish persistent access and pre-positioning capabilities for use during future geopolitical contingencies.

Concurrently, the spectrum of threat actors has become increasingly sophisticated, now encompassing organized criminal enterprises, cyber mercenary groups, ransom for hire organizations, terrorist organizations, and state-sponsored proxies. Regrettably, the U.S. government has encountered considerable challenges in effectively keeping pace with this accelerating evolution of the cyber threat landscape.

These attacks are happening on OT networks—the hardware and software that monitors and controls physical devices—machines like vents, pumps, and SCADA systems. And critically, **Operational Technology (OT) is distinct from Information Technology (IT)**, and their respective security requirements differ. While IT security protects networks that run business systems, OT security protects physical systems and must prioritize safety, reliability, and physical process continuity. These systems can be older, built to last decades, and many were never designed to be connected to the internet. Most importantly, when policymakers craft rules and requirements about cybersecurity, they must address both IT and OT use cases.

Despite the elevated risks associated with attacks on OT systems, this area of cybersecurity remains significantly underfunded and underprioritized. Even the Department of Defense (DoD) has yet to complete the fundamental step of identifying and inventorying its OT assets. **Congress must urgently answer the question of who has accepted these critical risks, as a debilitating cyberattack on our critical infrastructure would demand clear accountability**.

As you examine these issues, there are three considerations that I urge you to take into account:

Critical Infrastructure Security is a Matter of National Security

Critical infrastructure security is not merely an economic or operational concern; it is a **foundational element of U.S. national security**. An attack against critical infrastructure can lead to **severe consequences, potentially impacting national and economic security, public health and safety, and societal trust**. Recent incidents vividly illustrate this escalating danger:

- In May 2021, the Colonial Pipeline Company suffered a ransomware attack that halted pipeline operations, disrupting fuel supplies across the East Coast. While this attack did not touch OT systems, OT systems were shut down to prevent the risk of further damage. It is the first time that the public woke up to the danger a cyber attack could pose.
- In February of the same year, a hacker gained remote access to the Oldsmar, Florida water treatment plant and attempted to dangerously increase sodium hydroxide levels, an attack prevented only by an alert operator.
- In 2013, an Iranian national employed by a company contracted by Iran's Revolutionary Guard Corps accessed the SCADA systems of the Bowman Dam in Rye, New York, gaining insight into its operational status and water controls.[1]
- Most concerning were the Chinese state-sponsored Volt Typhoon attacks, discovered last year, targeting U.S. critical infrastructure sectors, pre-positioning a major adversary for long-term disruption during potential geopolitical conflicts.

Indeed, Iranian state-sponsored groups like **MuddyWater, APT33, OilRig, CyberAv3ngers, FoxKitten, and Homeland Justice** have also actively targeted U.S.

[1] "Manhattan U.S. Attorney Announces Charges Against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities," March 24, 2016, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.

critical infrastructure, particularly in the transportation and manufacturing sectors, with Nozomi Networks Labs observing a **133% increase in their activity** in May and June alone.[2]

Despite these breaches, the United States does not sufficiently prioritize OT and critical infrastructure security. This problem is both a cultural and structural issue, and we need to address both in order to ensure the security of U.S. critical infrastructure.

Whole of Nation Effort

We need to begin addressing critical infrastructure security through a whole of nation approach. Just as we would not expect an individual district, such as Cameron Parish, Louisiana to defend themselves against missile strikes from a nation state actor, we should not expect them to respond to cyberattacks on their own. Of America's 3,144 counties, about 1500 of them can be classified as rural.[3] These counties and municipalities do not have the resources or capacity to ensure resilience themselves, yet are often targets of cyber actors because they are the weakest link in our chain.

As we've seen play out again and again, cyber actors practice on smaller entities and then move to bigger targets. And, not only do we see our adversaries moving from small entities to larger targets like hospitals and casinos, but also globally as our adversaries practice their techniques on our allies and partners before they attack U.S. entities. And these attacks on small, unprotected entities can have significant costs to the entire nation. A 2023 report by the U.S. Water Alliance concluded that a one-day disruption in water service at a national level would amount to a daily loss of $43.5 billion in sales and $22.5 billion in GDP. An eight-day national disruption would total a 1% loss in annual GDP.[4]

Public Private Partnerships are Essential

Addressing the pervasive and existential threat of modern cybersecurity demands robust public and private sector partnerships. This threat impacts the foundational OT underpinning critical infrastructure across all sectors, from energy, water, and transportation to manufacturing, healthcare, and financial services. The intricate interconnectedness of these systems means a successful cyberattack in one area can trigger devastating cascading effects.

Since a significant majority of this vital critical infrastructure is privately owned and operated, bridging the inherent divide between private entities (with their specialized expertise and operational control) and the government (with its responsibility for national security and policy) is paramount. True resilience requires deep, trust-based collaboration where information, best practices, and threat intelligence flow seamlessly.

[2] Nozomi Networks, "Threat Actor Activity Related to the Iran Conflict," July 9, 2025, https://www.nozominetworks.com/blog/threat-actor-activity-related-to-the-iran-conflict.

[3] "Rural and Underserved Counties List | Consumer Financial Protection Bureau," Consumer Financial Protection Bureau, January 23, 2025, https://www.consumerfinance.gov/compliance/compliance-resources/mortgage-resources/rural-and-underserved-counties-list/.

[4] Value of Water Campaign, "The Economic Benefits of Investing in Water Infrastructure," n.d., https://uswateralliance.org/wp-content/uploads/2023/09/Economic-Impact-of-Investing-in-Water-Infrastructure_VOW_FINAL_pages_0.pdf.

To foster this essential synergy, it is critical to re-establish and strengthen effective public-private coordination mechanisms. We must bring back mechanisms like the **Critical Infrastructure Partnership Advisory Council (CIPAC)**, which provided a vital forum for government and industry collaboration on security issues. Organizations like the **Operational Technology Cybersecurity Coalition (OTCC)** also play a crucial role in bringing together stakeholders to provide broad perspectives and engage with policymakers.

By prioritizing and investing in these collaborative frameworks, we can ensure our nation is optimally prepared for today's rapidly evolving and increasingly sophisticated cyber threats across all critical infrastructure domains.

Recommendations

These issues are not insurmountable. To prevent adversaries from infiltrating our critical infrastructure and protect our national defense, the OTCC has the following recommendations

Raise Awareness. The U.S. government must prioritize operational technology cybersecurity to prepare critical infrastructure against growing threats. Congress must work with industry to ensure critical infrastructure entities are aware of the threats they face, to ensure cyber policy always takes OT into account. Our government has acknowledged that U.S. infrastructure is at risk; however, it has not taken sufficient steps to address the growing vulnerabilities or prioritized response and resilience in the wake of attacks like Volt and Salt Typhoon. While securing IT is important, it is the OT systems that, if attacked: turn off our lights; bring hospitals to a standstill; and disrupt essential services. Congress must be a partner in bringing light to this unresolved issue.

Reauthorize CISA 2015. On May 19, 2025, our coalition submitted a letter to Congress urging the reauthorization of the Cybersecurity and Information Sharing Act of 2015 (CISA 2015), which will expire on September 30, 2025.[5] This legislation is crucial to information sharing and strengthening U.S. collective defense.

Private sector cybersecurity teams, particularly those protecting critical infrastructure often targeted by foreign adversaries, rely on information sharing from other organizations to strengthen their defenses. If the legal protections established by the Act were to lapse, this flow of information would be disrupted. These communication channels are crucial for enhancing national threat awareness and enabling rapid responses to cyber incidents, protecting national security.

Improve Resourcing. Ultimately, a significant barrier to our national security is a lack of resources for OT cybersecurity. From addressing the growing tech debt, hiring cybersecurity experts, to procuring and building updated and secure systems, OT owners and operators do not have the funding necessary to fund the necessary security transformation.

[5] Operational Technology Cybersecurity Coalition, "Letter to Congress Re: CISA 2015 Reauthorization," May 19, 2025, https://www.otcybercoalition.org/post/letter-to-congress-re-cisa-2015-reauthorization. Letter to Congress re: CISA 2015 Reauthorization

Funding such as the State and Local Cybersecurity Grant Program (SLCGP) allows entities without the resources to utilize grant funding to move away from Chinese routers, hire cybersecurity staff, or replace outdated servers from the 2000's. Our coalition supports the reauthorization of this program and believes that it can help organizations take steps like creating an asset inventory; implementing multifactor authentication; introducing continuous monitoring and detection; ensuring secure remote access processes; and implementing network segmentation. OT environments are the heart of our physical infrastructure, and increasingly, the battlefield of modern conflict.

Asset Investories Agencies should prioritize creating OT asset inventories, which provide visibility into their OT network. Before an organization can protect their systems, it is essential to know what technologies are being used. The OTCC is working with the Department of Defense and CISA to encourage agencies to complete an OT asset inventory.

Supply Chain Security. Entities should also be aware of their supply chain risk. Today, critical infrastructure operators and private companies face significant vulnerabilities as they expose OT systems to the internet and bring on new contractors and vendors.[6] This risk increases when purchasers do not have the capability to identify vulnerabilities of third-party software. Like IT security, OT security requires expert technical assessments to ensure that the right solutions are implemented to mitigate weaknesses.

SRMA Maturity. OTCC is also in the process of publishing a Sector Risk Management Agency (SRMA) Maturity Model, which will allow the Office of the National Cybersecurity Director to annually grade the maturity of each sector. These assessments will give SRMA's direction depending on their current maturity and provide a clear roadmap to resilience.

We also advocate for measures like multifactor authentication, segmentation, and security by design, seeking to increase the cybersecurity baseline. Together, these recommendations are a roadmap to ensure the United States retains its OT, and national, security.

Conclusion

The threat posed by Iran and other adversaries to our operational technology and critical infrastructure is indeed real and growing. With the implementation of the right policies, allocation of sufficient resources, and cultivation of robust partnerships, we can collectively build a more resilient and secure nation. Thank you again for the opportunity to testify. I look forward to your questions.

[6] "Defending Against Software Supply Chain Attacks," Cybersecurity & Infrastructure Security Agency (CISA), n.d., https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks.

Appendix I

ALLIANCE FOR DIGITAL INNOVATION

American Bankers Association

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

bpi
BANK POLICY INSTITUTE

Business Software Alliance

EEI
Edison Electric INSTITUTE

ICBA

ITI

NRECA
America's Electric Cooperatives

Operational Technology Cybersecurity Coalition

sifma

March 21, 2025

Via Electronic Mail

The Honorable John Thune Majority Leader U.S. Senate Washington, DC 20510	The Honorable Charles Schumer Minority Leader U.S. Senate Washington, DC 20510
The Honorable Mike Johnson Speaker U.S. House of Representatives Washington, D.C. 20515	The Honorable Hakeem Jeffries Minority Leader U.S. House of Representatives Washington, D.C. 201515

Dear Majority Leader Thune, Minority Leader Schumer, Speaker Johnson, and Minority Leader Jeffries:

As the 119th Congress begins, we urge Congress to extend the September 30, 2025 expiration date for the *Cybersecurity Information Sharing Act*. This bipartisan legislation passed in the wake of the 2015 OPM breach and sought to "encourage public and private sector entities to share cyber threat information, removing legal barriers and the threat of unnecessary litigation."[1] This voluntary information sharing framework has been instrumental in strengthening our collective defense against cybersecurity threats that continue to grow in sophistication and severity.

Recent events underscore the imperative of continuing to support both private-public information sharing and collaboration as well as providing the legal clarity that companies currently count on to share cyber threat information with other companies and across sectors. Nation-state hackers have launched numerous attacks on U.S. critical infrastructure[2] including our communications systems—

[1] Consolidated Appropriations Act, Pub. L. No. 114-113, Div. N, Title I—Cybersecurity Information Sharing Act, 129 Stat. 2935 (2015), 6 U.S.C. § 1501; S. Rep. No. 114–32, at 2 (2015).

[2] Dustin Volz et al., *How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons*, Wall St. J. (Jan. 4, 2025), https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95; Office of the Dir. of Nat. Intelligence, *SolarWinds Orion Software Supply Chain Attack* (Aug. 19, 2021),

signaling they are positioning for bigger, more disruptive attacks. Federal agencies have similarly been targeted—most recently the Treasury Department in the BeyondTrust breach,[3] but also during the SolarWinds incident where nine agencies were compromised.[4]

In the decade since its enactment, the law has meaningfully improved the capacity and speed with which we can respond to large-scale cyber incidents while establishing clear expectations for privacy and confidentiality. This includes building the structures used by private sector cyber defenders to inform government partners of ongoing cyber threats from malicious actors. Equally as important, the law's antitrust exemption and associated protections have also facilitated broader cyber information sharing between private companies. Private sector cyber defenders, including those from critical infrastructure entities regularly targeted by foreign threat actors, depend on threat indicator sharing from other companies to strengthen their defenses and protect their customers' data. A lapse in the legal framework provided in the Act could limit this sharing. These communication channels are essential for enhancing overall awareness of national security threats and quickly responding to incidents. Given that value, these statutory provisions have been incorporated by reference to other significant cyber laws like the *Cyber Incident Reporting for Critical Infrastructure Act*—making their reauthorization all the more critical.[5]

The aforementioned attacks demonstrate the urgent need for increased collaboration and information sharing. The expiration of these protections risks creating a chilling effect on this critical information exchange—leaving us all more vulnerable to nation-state attacks and cybercriminals moving forward. Thank you for your leadership on this important issue and we are committed to working with you to preserve these key national security authorities.

Sincerely,

Alliance for Digital Innovation
American Bankers Association
American Public Power Association
Bank Policy Institute
Business Software Alliance
Edison Electric Institute
Independent Community Bankers of America
Information Technology Industry Council
Institute of International Bankers
National Rural Electric Cooperative Association
Operational Technology Cybersecurity Coalition
Securities Industry and Financial Markets Association

https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf.

[3] Arielle Waldman, *CISA: BeyondTrust breach affected Treasury Department only*, TECHTARGET (Jan. 7, 2025), https://www.techtarget.com/searchsecurity/news/366617777/CISA-BeyondTrust-breach-impacted-Treasury-Department-only.

[4] Office of the Dir. Of Nat. Intelligence, *SolarWinds Orion Software Supply Chain Attack* (Aug. 19, 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/SolarWinds%20Orion%20Software%20Supply%20Chain%20Attack.pdf

[5] *See* 6 U.S.C. § 681e.