MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Tuesday, July 22, 2025

10:00 a.m. EDT in 310 Cannon House Office Building

Subcommittee on Cybersecurity and Infrastructure Protection

Hearing

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

WITNESSES

Ms. Kim Zetter
Author and Journalist
Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon

Mr. Robert M. Lee
Chief Executive Officer and Co-Founder
Dragos Inc.

Ms. Tatyana Bolton
Executive Director
The Operational Technology Cyber Coalition

Dr. Nathaniel Gleason
Program Leader
Lawrence Livermore National Laboratory

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION
ONE HUNDRED AND NINETEENTH CONGRESS

---

22 JULY 2025

Kim Zetter

Chairman Garbarino, Ranking Member Swalwell and distinguished members of the Subcommittee, thank you for giving me an opportunity to testify before you today on the subject of Stuxnet and threats to critical infrastructure. My name is Kim Zetter, and I'm a journalist, author and adjunct professor at Georgetown University. I've been writing about cybersecurity and national security for two decades as a staff writer for *Wired* magazine and as a freelancer for the *New York Times*, Politico, the *Washington Post* and others. I wrote what is considered to be the seminal work on Stuxnet — *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapo*n. Recently, I have also begun to teach graduate students about nation-state cyber operations — the threat actors behind them, the technical capabilities they use to pull off these often very sophisticated operations, and the vulnerabilities in critical infrastructure and other systems that make the operations possible. Many of my students currently hold positions in the federal government or military, and others plan to work in government when they complete their degrees. My goal is to provide them with a solid foundation of knowledge — both technical and contextual — that will serve them in the policy and decision making positions they currently hold or may hold one day.

Today, I've been asked to talk about the digital weapon known as Stuxnet, which was designed to sabotage Iran's nuclear program and was discovered in 2010, three years after it was unleashed. I've been asked specifically to describe how Stuxnet conducted its sabotage, the impact it had on Iran's nuclear systems, the implications for other critical infrastructure here in the US and whether these systems are any more secure against similar attacks today than they were at the time Stuxnet was unleashed.

Fifteen years ago this month, Stuxnet was discovered on systems in Iran but its impact has not diminished and is still felt in the security community today.

Stuxnet was discovered after it spread out of control and far beyond the facility at which it was aimed. Although Stuxnet spread to millions of machines — the exact number is unknown — it only unleashed its destructive payload on the specific systems it was designed to target: systems at Iran's underground uranium enrichment plant at Natanz. It didn't sabotage other systems because Stuxnet was a highly sophisticated, carefully crafted, precision weapon that was designed to avoid collateral damage. Attacks against critical infrastructure, however, don't need to be precision-targeted or sophisticated to cause disruption or damage. They just need systems that are vulnerable. This is worth noting given the recent warnings from government about the potential for Iran to launch retaliatory cyberattacks against US critical infrastructure, following the recent US bombing of Iranian targets, including the Natanz facility that Stuxnet hit more than a decade ago. Iran doesn't have the skills to pull off a Stuxnet-like attack, but it doesn't need them to cause disruption and damage to US critical infrastructure.

Although a lot has been done since the discovery of Stuxnet to try to secure critical infrastructure in the US, many of the issues that made these systems vulnerable to attack in 2010 make them still vulnerable today.

In 2009 here in Washington DC, a metro train plowed into the back of another metro train that was stopped at a station during the afternoon rush hour. Sensors on the track should have indicated to any incoming train that another train was stopped at the station. Sensors on the front of the incoming train should also have detected the presence of the train at the station and alerted the driver or automatically slowed the incoming train. But the sensors failed to work and the driver noticed the stopped train too late and had trouble stopping the train manually. The collision killed nine people and injured 80 others. This incident, as far as anyone knows, wasn't the result of a cyberattack.

But this month CISA issued a critical security alert about a decade-old high-severity flaw in the braking system used by trains that hackers could exploit to cause a train to abruptly stop or derail. An attack like this could potentially result in the kind of outcome that occurred in 2009 of worse. The flaw exists in the protocol that devices located in the head and end of trains use to communicate with each other over radio to, among other things, engage the brakes and stop the train. The protocol employs a weak authentication, however, which means an attacker can also communicate with one of these devices as if they were a legitimate train device. They could send brake commands directly to a device, causing a train to halt or the brakes to fail.

The Association of American Railroads said it's developing more secure protocols and systems to replace the current devices and communication protocols. But the flaw was discovered by researcher Neil Smith back in 2012 and the AAR has ignored it since then, saying it was theoretical and without a real-world example to prove the flaw could be exploited in this way, it left the flawed system in place. Neil notified ICS-CERT years ago about the problem and together they tried unsuccessfully to convince the AAR to address it. But it was only after Smith and CISA recently threatened to go public with information about the flaw that the AAR announced it would be replacing the bad protocol. This won't happen, however, before 2027 at the earliest. The flaw can't be exploited over the internet — an attacker would need proximity to a train to communicate with it over radio frequency. But here's how Smith recently described it: "You could remotely take control over a Train's brake controller from a very long distance away, using hardware that costs sub $500. You could induce brake failure leading to derailments or you could shutdown the entire national railway system."

In my testimony today I'll focus first on explaining how Stuxnet operated so you can understand the level of expertise and sophistication that went into its unique design. Then I'll talk about the implications — how some of the tactics Stuxnet employed have been used by other threat actors since 2010, but also how the full capabilities demonstrated and hinted at by Stuxnet have not been realized yet in subsequent attacks. What I mean is that Stuxnet opened the door to a vast array of possibilities when it comes to attacking critical infrastructure, but threat actors have so far refrained from deploying the most impactful and dangerous of these, though they no doubt possess the capability to use them.

The World's First Digital Weapon

Stuxnet was a first-of-its-kind attack in that it was the first *known* example of malicious code designed to leap from the digital realm to the physical realm to cause physical impact not on the computers it infected, but on the equipment and processes controlled by those computers. Unlike other malicious programs in the past that undermined the computer systems they infected, Stuxnet was targeting the industrial equipment those computers controlled — centrifuges — in order to have a kinetic impact on them and sabotage the enrichment of Iran's uranium. The same tactic and techniques can be used in other critical infrastructure environments to temporarily disrupt services that the public, government and military rely on daily; to permanently damage equipment; and, in some cases, to even cause loss of life — either directly by creating conditions that, for example, cause trains to collide, or indirectly by preventing patients from being treated at a hospital that doesn't have electricity.

Stuxnet was discovered the same year Operation Aurora was uncovered. Aurora was an espionage campaign, attributed to China, conducted against Google and dozens of other targets for intelligence-gathering purposes. Until Stuxnet was discovered, the only attacks we'd seen in the wild were either cases of cybercrime or espionage. When Stuxnet was first discovered, researchers believed it, too, was an espionage operation. This is because embedded in Stuxnet's code were instructions for it to search for the presence of Siemens Step 7 control software any time it infected a new system. The Siemens software is used to control and monitor all kinds of manufacturing and industrial processes, so researchers believed the attack was likely coming from China and was aimed at stealing the blueprints or configuration data for industrial plants so that China could emulate their designs. After reverse-engineering the code, however, researchers discovered that it was actually designed for sabotage.

This is significant, because attacks against critical infrastructure can be almost indistinguishable from espionage operations in their initial stages of infection. Both kinds of operations can use the same *types* of tools, or even *identical* tools, to gain initial access to a system, conduct reconnaissance to study the system or network, and move laterally within the network to find the systems that contain the data an attacker seeks or that control the processes they want to affect. What's more, intrusions done initially for intelligence-collection purposes can morph into a disruptive or destructive operation simply by introducing malicious code or commands aimed at that purpose — meaning that an attacker may initially intend only to steal data from a system but then change course to damage or disrupt it as well, or to hand off access to the system to another actor who has the intention to disrupt or destroy. It can be difficult to discern the end goal of an intrusion until it's too late to stop it. I say this because a lot has been written recently about the Salt Typhoon and Volt Typhoon ongoing breaches of telecoms and critical infrastructure and attributed to China. These compromises don't appear now to be aimed at disruption or damage but could morph into such operations if China were to decide to use their presence in these systems for that purpose.

Returning now to Stuxnet and the Siemens software it sought, if Stuxnet found the presence of the Siemens Step 7 software on a system it infected, as well as evidence that the system was connected to a Siemens programmable logic controller — PLCs are essentially standalone computing devices that are used to control and monitor industrial equipment and processes — Stuxnet would then deposit its destructive payload on the PLC. But it did this only if it found a specific model and number of Siemens PLCs connected to the infected system as well as a specific model and number of other equipment Stuxnet was targeting. This was the precision part of Stuxnet that was aimed at ensuring that Stuxnet would not unleash its payload on any system except the intended target.

The Payload

Two known versions of Stuxnet were unleashed at separate times. The payloads in both of them operated similarly, though they impacted different parts of the centrifuges at Natanz. The first version of Stuxnet targeted the valves on the centrifuges, and the second version targeted the speed at which the centrifuges would spin.

With the first version of Stuxnet, once its payload was deposited on a Siemens PLC, Stuxnet would first sit on the device silently for 30 days and record the normal operation of the centrifuges as the PLC collected that data and sent it to engineers at monitoring stations. The PLCs collected data about the temperature of the centrifuges the speed at which they were spinning; the pressure inside the centrifuges; and the state of the valves that managed the flow of gas into and out of the centrifuges, noting if they were open or closed.

At the end of the 30 days, the sabotage began. Stuxnet began to close the exit valves on some of the centrifuges to prevent gas from exiting the devices. Gas would continue to pour into the centrifuges, but could not get out. In some cases the valves it closed had already been chosen by the attackers and were hardcoded into Stuxnet. But Stuxnet also randomly chose some valves on the fly to avoid consistency. Natanz engineers might notice some of the valves malfunctioning and closing, but not be able to isolate the cause or see a pattern.

Stuxnet would close the valves for a period of two hours or until the pressure inside the affected centrifuges rose five times what was normal. During this time the valves were closed, Stuxnet took the data that it had recorded during the first 30 days, and fed it to monitoring stations so that engineers would not see what was occurring. To the engineers, the valves would have appeared to be open, and the pressure inside the centrifuges would have appeared to be normal. During this time, Stuxnet also disabled the safety system on the cascade — a cascade is a configuration of multiple centrifuges connected by a series of pipes. Safety systems on industrial control systems are designed to detect when a system or process is entering into an unsafe or abnormal condition. When the safety system senses this is occurring, it initiates an automatic shutdown of the affected components to alert operators and control the problem. Because Stuxnet disabled this system during its sabotage, however, the affected centrifuges did not shut down. At the end of the two-hour sabotage period, the centrifuges returned to their normal operation for another 30 days, when the same sabotage sequence would occur again.

There are two potential impacts from closing exit valves. By increasing the pressure of the gas inside the spinning centrifuges, the uranium gas would have begun to solidify and either slow down the spinning rotors or cause them to malfunction, potentially damaging the centrifuges and spoiling the gas.

The second version of Stuxnet operated in a similar manner. But this version was designed to alter the speed at which the centrifuges were spinning. When this version infected a PLC, it would sit on the device for 26 days recording the normal operation of the centrifuges and store that information. Then when the sabotage began, Stuxnet would increase the frequency controlling the centrifuges from 1,064 Hz to 1,400 Hz for fifteen minutes, then restore the centrifuges to the normal frequency. Stuxnet would then wait 13 days and cause the centrifuges to slow to 2 Hz for 50 minutes then restore the original frequency. During the sabotage, Stuxnet fed the recorded data to the monitoring stations so engineers would not see the change in frequency.

By increasing the frequency to 1,400 Hz, the attackers were pushing the centrifuges to the highest frequency they could withstand. The centrifuges Iran used were first-generation devices that had material defects, and the increased frequency would have caused them to deteriorate over time or spin out of control. By also slowing down the centrifuges to 2 Hz for 50 minutes, the attackers would have undermined the enrichment process itself. For enrichment, centrifuges have to spin at a high and uniform speed for uninterrupted lengths of time to separate the isotopes needed for nuclear fission from the rest of the material in the gas. By slowing down the centrifuges, any separated isotopes would have come back together with other particles in the gas, effectively undoing the enrichment. At the end of each enrichment cycle, Iran would have had less enriched gas than it expected to produce, and that gas would have been enriched to a lower level than Iran expected.

The engineers understood they were having problems with the centrifuges, but couldn’t determine the cause. This is because Stuxnet thwarted attempts to investigate. If the engineers tried to examine the code blocks on the PLCs to see if they had been corrupted in some way, Stuxnet intercepted the code blocks before they were displayed on the engineering station and scrubbed any malicious code from them so the engineers would see no change to them. If the engineers decided to wipe the existing code blocks from the PLC and load new ones, Stuxnet intercepted the fresh code blocks and injected its malicious code into them as well. In this way, Stuxnet remained undetected for three years.

The cyclical pattern to the sabotage, and the fact that only some centrifuges were impacted during each round of sabotage, tells us that the attackers were not looking to cause one-time catastrophic damage to the centrifuges and the enrichment process — this would clearly have been suspicious — but instead intended to cause only incremental impact over time that could not be easily detected. The aim was to slow the enrichment process in order to buy time for diplomacy to work and get Iran to the negotiating table over its nuclear program.

Stuxnet is believed to have first infected systems at Natanz in late 2007, and it remained undetected until 2010 when the attackers got reckless and added too many spreading capabilities to the second version of Stuxnet. These caused it to proliferate wildly out of control — which led to its discovery. But, again, because Stuxnet was a precision weapon, it didn't cause damage to other systems it infected.

I've provided all of these details about Stuxnet to demonstrate the high level of sophistication and expertise that went into this operation. Stuxnet required the attackers to have knowledge not only of the Siemens software and computer systems controlling the centrifuges, but also knowledge about the material and parts that formed the centrifuges and about the uranium gas and enrichment process in order to understand how their manipulation of the centrifuges would impact both. The attackers used model centrifuges and cascades made from the same material and design as the centrifuges in Iran, and built a makeshift cascade to test the impact the Stuxnet attack would have on the centrifuges and the enrichment process.

But as previously noted, other attacks on critical infrastructure would not need to have the same level of sophistication to cause considerable disruption or damage. The systems at Natanz were also air-gapped from the internet — meaning they were not directly connected to the internet. This made it difficult for the attackers to reach them. They needed an insider to physically and surreptitiously deliver the code for them. But many critical infrastructure systems are directly connected to the internet and have insufficient protections to prevent attackers from accessing them remotely.

In 2013 I wrote about a researcher who used an automated scanner to find systems connected to the internet that were using port 5900 (the port on a computer that is used for VNC and TeamViewer remote-management software). He found 30,000 connected systems that required no authentication to access them. This included two hydroelectric plants in New York, a generator at a Los Angeles foundry, a system for monitoring and controlling ventilation for underground miners in Romania, and the refrigeration system for a food service company in Pennsylvania that provided lunches to schools and other facilities. That was 2013. Surely, you'd think, this wouldn't still be the case years later. But in 2021, a water treatment facility in Oldsmar, Florida was hacked through its TeamViewer remote-management software over the internet. All of the computers at Oldsmar were connected to the internet without a firewall to protect them and limit who could access them, and all of them apparently shared the same password for the remote-management software.

Implications and Impact

One of the most significant impacts of Stuxnet was the awareness it brought to vulnerabilities in critical infrastructure that few had noticed before. The security community, largely focused before Stuxnet on IT networks — the systems used to run the business side of a company or industrial operation — had its eyes opened to a vast sector it had previously ignored: industrial control systems and the OT (operational technology) networks where they are deployed. Control systems consist not only of programmable logic controllers, but also SCADA systems and remote terminal units — devices that often sit in the field to operate and monitor equipment and processes that are distributed across large geographical distances, like electric substations. Stuxnet provided stark evidence that physical destruction of critical infrastructure – using nothing other than code – was not only possible but also likely. And once security researchers turned their sights on these systems, they found not only software security holes but also whole architecture problems that couldn't be fixed with a patch. With so many of the systems directly connected to the internet, cybersecurity suddenly became inextricably linked to national security.

The following is a small sample of the kinds of systems that PLCs and other industrial control systems operate. They control the opening and closing of cell doors and gates at high-security prisons; they manage the timing and sequencing of traffic lights; they are used to manage HVAC systems in schools, hospitals and office buildings; they raise and lower bridges on waterways; they help route commuter and freight trains and prevent crashes; they control the temperature of food pasteurization processes to make food safe; they are used to control the temperature of furnaces in the manufacturing of steel and fiberglass; they control the flow and distribution of gas through pipelines; they control the operation of dams and water and sewage treatment plants; they operate and monitor the processes in chemical and pharmaceutical plants; and they help manage and control the distribution of electricity across the nation's grids — the critical infrastructure that undergirds all other critical infrastructure.

Years ago, industrial control systems were manually operated and were not connected to the internet, keeping them safe from remote attacks. But for efficiency purposes, these systems were digitalized. And then for varying reasons, ranging from regulatory requirements to ease-of-use, many of them were connected to the internet — without proper attention to securing them. Additionally, systems that once were highly complex and used proprietary software and protocols that were hard for attackers to access and study, have been simplified and standardized, making it easier for hackers to design attacks that can have widespread impact at scale. This is not news.

In 1997, after Timothy McVeigh blew up a federal building in Oklahoma, the Marsh Commission launched an investigation into the vulnerability of critical infrastructure to both physical and digital attacks. In their report, the commissioners warned against connecting critical systems for oil, gas, and electricity to the internet. "The capability to do harm … is growing at an alarming rate; and we have little defense against it," they wrote. Commands sent to the control computer at a power plant "could be just as devastating as a backpack full of explosives," they wrote at the time. "We should attend to our critical foundations before we are confronted with a crisis, not after. Waiting for disaster would prove as expensive as it would be irresponsible."

A second report also released in 1997 by the White House National Security Telecommunications Advisory Committee warned that the nation's power grid and utilities were vulnerable to digital attack. "An electronic intruder … could dial into an unprotected port and reset the breaker to a higher level of tolerance than the device being protected by the breaker can withstand," investigators wrote. "By doing this, it would be possible to physically destroy a given piece of equipment within a substation."

But instead of heeding the warnings, critical infrastructure became more connected and more insecure.

After Stuxnet was discovered, experts expected to see a lot of copycat attacks against critical infrastructure. This surprisingly didn't occur. It wasn't until 2015 and 2016 that we saw the first Stuxnet-level attacks against critical infrastructure. These targeted Ukraine's electric grid to cause blackouts for a few hours at the height of winter. The attackers were able to take 60 substations offline in 2015, leaving about a quarter of a million customers without electricity. The attack was limited in scope — presumably it was simply done to send a message to Ukraine about who was in control of its grid not cause permanent disruption — but could have been much broader if the attackers had intended this. The subsequent attack next year showed the potential for this. The malware used in that attack, known as Industroyer and Crash Override, caused only a brief outage in parts of Kyiv. But the code was more advanced than the code used in 2015 because it had the potential to be automated so that once on a system, it could execute commands on its own such as opening circuit breakers, overwriting software or adapting to whatever environment it found itself on, without the need for direct control by the attackers. Whereas the 2015 outage required the attackers to be at the keyboards issuing a series of commands in real-time, the 2016 version could have unfolded automatically once the attackers unleashed the code.

Then in 2017, we saw an attack that went beyond disruption and destruction to target the safety system on critical infrastructure, as Stuxnet had done at Natanz. The so-called Triton attack was designed to disable the safety system at a petrochemical plant in Saudi Arabia. Presumably, the attackers intended to use it in conjunction with an attack that would have caused a chemical spill or some other dangerous condition at the plant and they wanted to prevent the equipment from automatically shutting down to contain the danger. But fortunately there was no accompanying attack in this case, and the code targeting the safety system contained a flaw that caused the safety system to trigger automatic shutdowns of the plant, alerting engineers to its presence. It's an attack that could have had a potentially deadly impact if the attackers had intended this and if they had not made a mistake.

Triton wasn't a fully developed and tested attack tool yet. But the expansive Pipedream attack platform discovered in 2022 was. Researchers at the security firm Dragos say it had the potential to cause disruption or destruction and appeared to be focused on electric and oil and gas facilities — liquified natural gas systems in particular. It could be modified, however, for use against any industrial environment and had the ability to disable or brick control systems or undermine safety systems in ways that could potentially endanger lives if an attacker can cause chemicals to spill or cause equipment to catch fire or explode. This impact can be multiplied if disabled safety systems prevent engineers from being alerted to a dangerous condition when it first starts to unfold or prevent the systems from going into automatic shutdown to contain the damage and impact.

Since 2017, hackers have increasingly been targeting critical infrastructure and industrial control systems — whether cybercriminals infecting them with ransomware to extort the infected organizations, nation-state actors targeting them to cause disruption or hacktivists impacting them to send a message. In 2022, the state-owned Khuzestan Steel Company in Iran had to halt operations after being hit with a cyberattack. The company claimed it thwarted the attack and no damage or disruption occurred. But a hacktivist group believed to be tied to Israel claimed credit for the attack and published CCTV footage as proof that it did have an impact. The video, purportedly taken from inside the plant, showed a fire breaking out from malfunctioning equipment that spilled molten steel, evidently a result of the cyberattack. Regardless of whether the hacktivist claim is true, it is possible that such an attack could result in spillage and a fire.

Small critical infrastructure organizations are more vulnerable to attack due to the fact that they tend to have insufficient funding to hire security staff and replace outdated insecure systems. By contrast, large well-resourced facilities tend to have redundant systems that make them more resilient to attack so they can prevent disruption and downtime or limit their impact. But this is not always the case. The ransomware attack against Colonial Pipeline in 2021 revealed that this company did not have a CISO in place at the time of the attack, had seemingly failed to properly segment its IT and OT networks (requiring the company to shut down the pipeline to prevent the malicious code from spreading to its OT systems) and prior to the attack ignored warnings about lax security as well as government alerts about attackers targeting pipelines.

The ransomware struck around 5am on May 7, and by 6am the company had shut down its 5,500-mile pipeline. By late afternoon CEO Joseph Blount had decided to pay the ransom, which was sent to the hackers the next day. He later said they shut down the pipeline out of fear that the ransomware might spread from the IT to the OT network, taking control of the pipeline out of their hands. The pipeline was down for nearly a week and resulted in a cascade of effects the company had no direct control over — panic buys and hoarding triggered by consumer reaction to the outage. The hack didn't inflate prices and create a fuel shortage, but consumers responding to it did.

When Colonial Pipeline was hit, many were surprised at how quickly the company paid the $4.4 million ransom. Surely a business as big and critical to the US economy — Colonial Pipeline supplies 45 percent of fuel to the East Coast, which amounts to about 2.5 million barrels daily — had sufficient backups and a response plan in place to recover from the attack without needing to pay the ransom. The company did have an emergency-response plan, the CEO told lawmakers on Capitol Hill after the attack, but it didn't include a game plan for ransomware — even though ransomware actors had been targeting critical infrastructure since 2015.

Colonial Pipeline was caught off guard. But the warnings were there if the company had been paying attention.

There had been some 400 ransomware attacks against critical infrastructure the previous year; and between November 2013 and June 2022, there were nearly 1,300. These included attacks on oil and gas facilities. The ransomware operators weren't just targeting IT systems in critical infrastructure — they were going after OT systems to disrupt critical processes.

In 2020, the year before Colonial Pipeline was hit, the security firm Mandiant reported that seven different ransomware families had struck industrial organizations since 2017, resulting in significant disruptions and delays in production as well as the delivery of goods and services. Ransomware actors were also becoming increasingly sophisticated, Mandiant reported, conducting internal reconnaissance of their victims to determine which systems were the most vital to production, in order to increase the odds that a victim would pay. The ransomware operators actually put together a “kill list” of more than 1,000 processes that ransomware operators could choose to halt to increase the odds of being paid.

If this wasn’t enough warning, that same year, DHS’s Cybersecurity Infrastructure and Security Agency published an alert warning specifically about ransomware attacks targeting pipelines. It described an attack against a natural-gas compression facility that began with a phishing campaign that infected the IT network, then spread to the facility’s improperly segmented OT network, preventing staff from obtaining real-time data from control and communication systems and forcing the company to shut down operations for two days. The plant didn’t have a response-plan for cyber attacks in place, and in its alert, CISA advised pipeline and other critical infrastructure owners to create a response plan, conduct red team exercises to simulate attacks and test internal responses, put backups offline or on fully segregated networks to keep them from being encrypted along with the rest of their systems, and build redundant workflows to maintain critical operations in the event of an attack. A year later, ransomware struck Colonial Pipeline.

The attackers got in through an employee password for the company VPN that the employee had apparently re-used for other systems. Mandiant later discovered it in a batch of passwords leaked online from a different data breach, though it’s not clear if the Colonial Pipeline hackers obtained it this way. The VPN account was a legacy system the company no longer used but had failed to disable. And because Colonial Pipeline didn’t have multi-factor authentication enabled on the account, the attackers were able to get in using just the employee’s username and password.

The company told the Associated Press that its IT and OT networks were segmented, but if Blount made the decision to shut down the pipeline because the company was afraid the ransomware would spread to the OT network, this suggests the company wasn’t as confident in the segmentation as he indicated.

He also said his company had the ability to operate the pipeline manually, but only, unfortunately, on a small scale if a portion of the pipeline went down — not in a scenario in which the entire 5,500 miles of pipeline were shut off.

In 2018, three years before the ransomware attack, an audit of Colonial Pipeline systems found that it was deficient in security best practices. Robert Smallwood, whose consulting company conducted the audit, called Colonial Pipeline's information management practices "atrocious" and said the company had a patchwork of poorly connected and secured systems and lacked security awareness.

In 2022, CISA released a lengthy list of basic security guidelines for pipelines: use strong perimeter controls to isolate ICS/SCADA systems and networks from corporate networks and the internet; limit communication leaving/entering these perimeters; use multi-factor authentication; have a cyber incident response plan in place; and maintain good offline backups.

When these came out, many wondered why CISA would distribute a list full of basic guidelines — especially after years of red flags about threats to critical infrastructure. But Colonial Pipeline — which, remember, had no CISO at the time of the hack — showed that companies were still not doing some of the basics to secure their systems and ensure they would be resilient in an attack.

Several years ago, CISA launched a "More Than a Password" campaign to increase adoption of multi-factor authentication and called the absence of MFA "exceptionally risky," particularly for critical infrastructure. A study by Google and two universities found that MFA can block up to 99% of bulk phishing attacks and about 66% of targeted attacks. Yet a survey published by Trellix found that 75 percent of respondents in the US oil and gas sector had not fully deployed MFA. Over half of them blamed a lack of in-house cyber skills for failing to implement it.

So although there has been a lot of focus from the government in establishing new security guidelines and mandates and reporting requirements for railways and pipelines and other critical infrastructure, it's not clear how these industries will reach basic levels of security without budgets and skills — and even with those, it's not clear how long it will take to get them up to speed. The fact that there aren’t more attacks against critical infrastructure isn’t because the systems are secure.

Testimony like this often ends with some sort of call to action. I don’t have any specific prescriptions to suggest because I believe my fellow panelists will do that. My goal here has been to bring attention to some issues around critical infrastructure that have been simmering for two decades but are far from being resolved, even though we’ve had decades to address them and events like Stuxnet, the Ukraine power grid hack and the Triton assault against the petrochemical plant in Saudi Arabia to illustrate the direction the US is headed if the problems aren’t addressed.

Thank you again for this opportunity to speak with you about this issue.

The Operational Technology Cybersecurity Landscape 15 Years After STUXNET

LESSONS LEARNED AND RECOMMENDATIONS FOR NATIONAL SECURITY

HEARING
BEFORE THE COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION
ONE HUNDRED NINETEENTH CONGRESS

22 JULY 2025, CANNON HOUSE OFFICE BUILDING

Robert M. Lee

Chairman Garbarino, Ranking Member Swalwell and distinguished members of the Subcommittee, thank you for providing me the opportunity to testify before you today. I am Robert M. Lee, the CEO and Co-Founder of Dragos, Inc., a leading industrial cybersecurity technology and services provider. I am also a Fellow and course author at the SANS Institute which is the leading cybersecurity training provider globally where my classes have trained thousands of the world's critical infrastructure security practitioners. Additionally, I am a veteran of the United States Air Force and National Security Agency and currently serve as a Lt. Colonel in the United States Army National Guard where I have been tasked to design operational technology (OT) and industrial control systems (ICS) defense and response strategies for the country in preparation for conflict. It has been my privilege to be on the front lines of this problem in both government and the private sector.

This committee's hearing is very timely: an examination of what we have learned in the OT/ICS community across the last fifteen years since the emergence of the malicious software capability STUXNET. I will focus my testimony on both the global infrastructure community and specifically the national security of the United States. Those two topics are intricately connected but there are U.S. centric lessons learned and examples to explore that can provide insights.

It has been well covered over the years that what made STUXNET unique was its ability to target and cause destruction to physical assets and production processes through cyber methods. It did this by targeting OT/ICS – specialized computers and networks that interact with the physical world. Sometimes these systems are typical looking Windows Operating Systems on personal computers that have specialized software to interact with physical components such as valves and circuit breaks. Sometimes they are unique computers, networks, and physical components that may only be found in specific production processes such as a purpose-built controller interacting with a P-1 gas centrifuge and its vibration monitoring sensors.

STUXNET was unique at its time in the demonstration that targeting ICS/OT with the expertise not just of software developers and cyber operators but also engineers and operators could lead to physical disruption and destruction of critical infrastructure. There were people around the world who already knew this was possible and other adversarial countries already developing their expertise in these areas. But it is fair to say that many who did not know it before now understood that the critical part of critical infrastructure is OT. Unfortunately, STUXNET did not remain unique for long in its destructive capabilities.

Over the last fifteen years we have seen a significant rise in the number of state and non-state actors that target ICS/OT. At Dragos, Inc. we currently track over 25 such groups who have focused their cyber operations on the targeting of OT. Some of those groups continue to focus their efforts on learning about the structure of, and vulnerabilities in our critical infrastructure. Those groups pose no significant immediate threat but may be developing the capacity and the knowledge needed to threaten critical infrastructure in the future. Other threat groups have caused multiple real world electric power grid outages, disruptions to water systems, and the theft of intellectual property in our defense industrial base and manufacturing communities. To date, we know of nine unique families of ICS malware that have been developed with espionage or disruption in mind.[1] The worst of these is PIPEDREAM which was the first-ever capability to be re-usable against a wide variety of industries ranging from the servo-motors on unmanned aerial vehicles to water pumps to combined cycle gas turbine control systems.[2] STUXNET was extremely tailored and capable against only one specific target whereas PIPEDREAM was built to impact any environment the adversarial country who built it wanted to disrupt.

Criminals are already responsible for thousands of attacks on industrial organizations a year with around 75% of those resulting in some disruption to operations and around 25% of those attacks resulting in full operations shutdown.[3] Alarmingly, we have recently seen the state actors who once alone possessed the capability to cause such disruption sharing their insights and resources with non-state actors including criminals. Even with that backdrop, the world right now enjoys a relative level of calm that comes from having a low frequency of high consequence attacks in comparison to what it may become. Unfortunately, non-state actors and lesser restrained states gaining such capabilities will continue to increase the frequency of these attacks and many in the cybersecurity community are sadly awaiting the days we see the direct loss of human life as a result of such attacks. I sincerely hope that we do not learn to normalize and accept this as we have sadly collectively normalized and accepted increasing attacks on civilian OT infrastructure.

I could spend the entire time of this testimony giving scary examples of what has transpired over the last fifteen years and why we need to take this threat seriously. The unclassified briefings alone of what China has done in its VOLT TYPHOON / VOLTZITE campaigns targeting U.S. and allied critical

[1] https://www.dragos.com/wp-content/uploads/2025/06/dragos-understanding-ics-malware-whitepaper-june-2025.pdf

[2] https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf

[3] https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf

infrastructure over the past few years would leave no doubt to people about the seriousness of this conversation. Let's be clear: the timeline to take action against this growing threat is short, and the consequences of failure could, and likely would be people dying. Thankfully this is not the first time Congress has taken up this discussion. Personally, this marks the fifth time I've testified to the House and Senate on such matters. Therefore, I want to focus on what problems we must solve for now and how we can solve them. I know this is a Congress that listens, and we have a critical infrastructure community that acts.

There are many areas of investment that can be made but I assess the following to be the most practical, right-sized actions against the threat, and the most effective moves to counter the risks that our communities need protection from most.

- **Recognize and Account for the Differences between Information Technology and Operational Technology Systems -** IT and OT systems differ fundamentally in both purpose and operation. IT supports how a business is managed, focusing on data security and system integrity, while OT enables the physical functions that are the core reason an organization exists, such as controlling pumps or chemical levels at a water facility. These differing missions shape how risks are assessed and managed. While an adversary might exploit similar vulnerabilities in IT and OT systems, the consequences and adversary behavior differ. A breach in an IT system might result in data theft, but in OT it could lead to physical disruption, equipment damage, or even loss of life. OT environments also have distinct operational demands: systems often run continuously for years, require availability-focused redundancy, and depend on precise millisecond-level responsiveness. While some traditional IT controls have been adapted for OT, the security mindset must differ; tailored to the unique physical environments, long hardware lifecycles, and evolving threats targeting operational infrastructure. All these differences dictate some different security practices, technologies, and policy responses. Regulators and policymakers must recognize these critical distinctions when setting policy to avoid costly and counterproductive rules. Asset operators must be mindful of these differences and avoid underinvestment in OT security – currently based on my anecdotal experience about 95% of cyber spend is focused on IT systems, with just 5% for OT – where the revenue of companies is focused and their impact to society and national security. Hearings like this one draw important attention to these distinctions.

- **Focus on the Fundamentals – Defense is Doable -** As the scale, frequency, and sophistication of threats to critical infrastructure increase it can be easy to fall into a spiral of admiring the problem and failing to defend against it. But fortunately, defense is doable. The vast majority of threats can be prevented from achieving their objectives by simply taking fundamental steps. To provide one example, the Littleton Electric Light and Water Departments in Massachusetts won a federally funded grant from the American Public Power Association and used it to install our threat visibility and mitigation technology. At the same time, the U.S. government including the Federal Bureau of Investigations (FBI) provided critical intelligence to Littleton that they were likely being targeted by VOLT TYPHOON. Upon receiving this intelligence and the deployment of our platform they quickly identified a sophisticated and persistent compromise from the Chinese government. Our team moved swiftly to contain and eliminate this adversarial presence and the utility was able to change its network architecture to remove any advantages for the adversary. This is a common phenomenon: when we gain visibility into an OT network for the first time, we often find evidence of compromise that was previously unknown. Visibility into OT networks is critical to know that you have a compromise, to know the nature of the compromise, and to detect its cause. Only with that information can political and business leaders choose the appropriate response plans and actions. Recognizing this fact, the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC) jointly created Reliability Standard CIP 015-1 Internal Network Security Monitoring. This landmark regulation will vastly improve the security of America's larger electric utilities by requiring network visibility, but it will take time to implement and smaller sites and other industries are not taking the same journey. While I highlight visibility here it is only one of a couple core security controls required. The SANS Institute analyzed all the known OT cyber incidents and determined that five security controls were the most effective and could significantly decrease the risk of cyber threats.[4] Not tens or hundreds but simply five security controls. Raising awareness of the threat is a critical part of this effort, but public and private resourcing is also vital for efforts that have been proven to work. We aren't where we need to be right now, but we know what needs to be done, and we know it can be done.

- **Create Public-Private Partnerships that work –** The necessity of public-private partnerships and information sharing is universally recognized, but the effectiveness of these arrangements is inconsistent. Constant effort must be made to improve and properly resource information sharing partnerships and learn from what is working and what isn't. As an example of successful partnership, my company, Dragos, collaborated with the NSA Cybersecurity Collaboration Center and a 3rd party to identify and analyze the PIPEDREAM malware before it was employed against its targets. In partnership with the Cybersecurity and Information Security Agency (CISA) and the Electricity Information Sharing and Analysis Center (E-ISAC), we informed industry widely about the threat we had identified, providing operators time to prepare and monitor. The mission succeeded in this instance because everyone involved was focused and understood the nature of the threat. Dragos had the technology and experts to detect the threat and analyze it in collaboration with our federal partners. E-ISAC and CISA knew who the operators were, and how to communicate the threat to them. The operators, in turn, knew how to defend against the threat once they were aware of it. E-ISAC, and its financial services counterpart FS-ISAC are examples of well-resourced industry partners with proven effectiveness that can and should be emulated. Some other public-private information sharing efforts have become too broadly based, limiting their effectiveness by making participants hesitant to be candid. Some level of federal selectivity based on ability to produce unique insights and capabilities makes sense and helps participants stay focused and effective.

- **Keep federal guidance focused and federal actions streamlined –** Federal authorities have promulgated an array of requirements and guidance documents that are often well meaning, but ultimately ineffective, or even damaging. Different federal authorities will come to operators advising or requiring them to take different sets of actions. Sometimes these actions are

[4] https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

duplicative or even contradictory; even when they're not, their sheer number muddles the mission and makes it difficult for operators to focus on what matters most. The federal government should speak with one voice, and they should keep their advice and requirements to industry streamlined and focused. Operators should be informed of the threat scenarios they should prepare for, and the specific outcomes they should be able to achieve, not how they should achieve them. Vague generalities and obscure goals can cause confusion and analysis paralysis. Empowered, focused, and threat-informed federal authorities should be allowed to have a point of view on the threat scenarios faced by critical infrastructure operators, and they should communicate the threat and desired outcomes clearly and in a unified manner while leaving the details to the industry operators who know their systems best.

- **Let the private sector lead on security technology –** Just as some federal efforts to offer guidance and regulation to the private sector are well-meaning but ultimately ineffectual, there are some federal technology initiatives that are meant to help but may simply crowd out better solutions. Federally led and funded cyber technology development efforts aimed at critical infrastructure sectors have not achieved large scale adoption and serve as a disincentive for infrastructure operators to acquire state of the art cybersecurity solutions; indeed, they discourage private sector businesses from creating them in the first place. There is no market failure to address. Companies like Dragos, but not limited to Dragos, have produced the tools needed to effectively detect and mitigate even the most advanced operational technology threats. Federal funding can be better spent facilitating the acquisition of advanced cyber technologies than it can by attempting to create them. The alarming fact is, at this moment, most critical infrastructure operators would not be able to detect STUXNET or its techniques on their systems, nor would they be able to recognize the known and highly publicized tactics and techniques of our advanced adversaries. Again, this is in spite of the fact that the technology and knowledge exist to do so. We have the ability; we know what works. We just need to do it. While innovation is always welcome, we are sorely lacking in execution of what works today. Federal attempts to build duplicative tools will only distort the market and serve as a distraction for operators whereas resourcing the asset owners and operators directly can have a direct and immediate impact.

- **Don't disregard supply chain security –** Much of my testimony is focused on what we need to do to keep external threats out of operational technology networks, but we also need to focus on making sure that the component parts of these networks and their vendors aren't degrading their security. This Committee, and Congress writ large have done important work in raising the alarm about the threat that insufficiently vetted foreign technology may pose to American telecommunications networks, ports, and other critical infrastructure. This should also extend to domestic technology providers who choose to not make good security choices. Asset operators often feel enormous pressure to go with the most economical choice when buying equipment and other vital operational technology, even if the security of these components is in doubt. This creates a large and looming cybersecurity threat that may be more expensive and complex to address than if properly vetted technology had been installed to begin with. Federal policymakers must have a clear notion of what assets count as critical infrastructure that is continuously updated, and that accounts for the upstream assets that make the operation of critical infrastructure possible. This should also include the security vendors like Dragos. Today, as the CEO of Dragos I can make choices that benefit my company financially but lower the security of our part of the supply chain. Yet I am allowed to make those changes and sell into critical infrastructure where the cost of my choices is not just passed on to the asset owners and operators but the people they serve. I have strived hard not to make such careless choices, but I am surprised with the level of freedom I have in making them and still being allowed to sell into critical infrastructure. Other companies I know of are not being so focused on these choices as market demands and pressures make it challenging for them. Policymakers should not hesitate to set basic security standards for the supply chains of our critical infrastructure or even creating selectivity based on these standards on what companies are allowed to sell into critical infrastructure. These standards should be clear, enforceable, and readily justifiable. The vendor community serving critical infrastructure sectors should know these standards and share accountability for adhering to them. You can only be confident about the security of a critical infrastructure network if you're confident about the security of its components.

- **Have a National OT/ICS Incident Response Plan and Align Authorities –** Just as it's important to align federal messaging and guidance to industry, it is also critical that we work to align federal authorities to respond to incidents. Unfortunately, incidents will happen, but their severity can be mitigated by swift and effective response. Although I am here speaking in my capacity as CEO of Dragos, I have recently taken up duties in the 91st Cyber Brigade's Information Operations Support Center of the Army National Guard to aid in this effort. I was tasked with creating a national response plan focused on OT incidents and coordinate across federal agencies. It has long been clear to me that asset owners and operators often don't know whom to call after an incident, what help they are going to be able to get when they do, and experience consistency across state lines in terms of the expertise and credentialing of the people responding. What I have found is the actual tactical and technical nature of the work is obvious. The plan itself was actually fairly easy to write in a way that would significantly enhance national security. But it is the mismatch of authorities, selecting which budgets efforts are allowed to be coordinated out of, and being able to have a point of view on what right looks like without "the concern of perception" that are hindering the roll out of the plan. I find it morally questionable that we have broad based support and a knowledge of what to do to protect our kids against foreign threats and it is only ourselves standing in the way. This is not a criticism of the many talented public servants who selflessly carry out tough and important work; it's simply a recognition that existing federal funding structures and authorities aren't always aligned in a way that is easily accessible to industry, or maximally effective in executing a response. Fixing these issues will likely require legislative action to untangle funding lines, provide indemnification to operators who choose to trust the U.S. government, and facilitate cooperation with federal agencies and between agencies. I look forward to working through some of these tough issues and I know there is a broad cross section of federal cyber leaders who share a common perception of what the problems are, and broadly how they can be fixed. It is critical that the federal government have a single response plan that provides asset owners and operators a unified means of interacting with and receiving help from federal responders in cooperation with the private sector before and after an incident.

In the 15 years that have passed since STUXNET shined a light on the threat facing OT/ICS, the threat has grown but so has our ability to respond to it. We have better technologies and trained personnel. We have an improved sense of what works, and what doesn't work, in public-private threat information sharing, incident response, regulation, resourcing and general cyber threat defense. We have a body of case studies to draw lessons from. We have real-world examples of the simple fact that defense is doable, even for smaller utilities and asset operators. That's the good news. The bad news is that major gaps remain in the implementation of OT/ICS cyber defenses, and despite improvements, federal guidance and regulations continue to be confusing, duplicative, or contradictory in many cases. Federal OT/ICS incident response plans remain tangled. The determination and sophistication of our adversaries continues to grow, and the scale of adversary infiltration into critical infrastructure networks may be far greater than we realize. Stated plainly: at this moment, we are not prepared for a large-scale attack on critical operational technology.

The threat remains, but past progress shows clearly that we can solve our current and future challenges. I'm deeply grateful for the work that this subcommittee is doing, and the needed attention it is drawing to OT/ICS cyber threats. I look forward to the rest of today's conversation.

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

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.

Dr. Nate Gleason

Program Leader, Cyber and Infrastructure Resilience Program, Lawrence Livermore National Laboratory

Testimony before the Subcommittee on Cybersecurity and Infrastructure Protection of the Committee on Homeland Security

July 22, 2025

Chairman Garbarino, Ranking Member Swalwell, Chairman Green, Ranking Member Thompson and Members of the Subcommittee, thank you for the opportunity to testify today.

My name is Dr. Nate Gleason, and I am the Program Leader for the Cyber and Infrastructure Resilience Program at Lawrence Livermore National Laboratory (LLNL) in Livermore, California. I am honored to be here today on behalf of LLNL, a National Nuclear Security Administration (NNSA) laboratory and proud member of the Department of Energy's network of national laboratories.

At the Lab, I have the privilege of leading a multidisciplinary team that includes operational technology (OT) cyber experts, threat hunters, reverse engineers, data scientists, electrical/chemical/civil/mechanical engineers, computer scientists, systems analysts and intelligence analysts in a program focused on providing the U.S. with technologies to effectively compete with nation-state adversaries like Russia and China in the domain of gray-zone conflict. Our primary emphasis is on the role of critical infrastructure in national security. I sincerely appreciate the Committee's interest in the work we do in support of the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy (DOE), the Department of Defense (DOD), and U.S. critical infrastructure writ large, as evidenced by your visit to the lab earlier this summer.

Nearly everything we do as a nation, whether it be critical national functions like energy transmission or our ability to defend our homeland and project force around the globe, depends on critical infrastructure. As reflected in reports on Volt Typhoon and other threat actors, our adversaries see our critical infrastructure as an attractive target. As CISA and the Intelligence Community (IC) have acknowledged, these adversaries seek to preposition themselves on U.S. critical infrastructure networks for disruptive or destructive cyber attacks. These adversaries are highly capable and invest significant resources in developing capabilities to hold our infrastructure systems, and the functions that depend on them, at risk. To defend against this threat, the U.S. must out-innovate the competition, work across federal, state and local authorities, and link with the public and private sectors to bring our best technology into operations.

CyberSentry

CISA plays a key role in bolstering critical infrastructure cybersecurity. The CyberSentry program is an excellent example of how CISA leverages government capabilities to identify and mitigate highly consequential cyber threats targeting critical infrastructure, and I would like to thank the Committee for its leadership on this program.

Through CyberSentry, CISA works with private sector partners who volunteer to have their systems monitored for malicious activity. Participants are from a wide range of critical infrastructure sectors including energy; water and wastewater; transportation; chemical; nuclear reactors, materials and waste; food and agriculture; dams; and critical manufacturing. Since 2020, LLNL has provided core support to the program by developing advanced analytic capabilities and leveraging artificial intelligence (AI) to detect novel adversary techniques and then deploying those analytics to operationally monitor and hunt for threats in the partner networks.

CyberSentry is valuable because it provides cyber researchers real-time access to real-world systems and network data so that we can take information on adversary intent, capability and activity from the IC, combine it with the technological and computational resources of the DOE national laboratories, and develop and deploy new tools to detect and mitigate the latest techniques of our adversaries. CISA uses the data generated from our work to then create alerts for the broader U.S. critical infrastructure operator and owner community.

2022 Discovery of Chinese Surveillance Cameras on U.S. Critical Infrastructure Networks

One of LLNL's most notable contributions to the CyberSentry program was when, in 2022, we detected high-risk Chinese surveillance cameras that were stealthily built into U.S. critical infrastructure systems. CISA had asked LLNL to develop a capability to detect subtle malicious beaconing behavior that available tools could not detect. Using our hardware-in-the-loop laboratory (dubbed the "Skyfall" lab), LLNL set up an operational technology (OT) environment where we deployed various samples of beaconing malware and tested existing commercial and open-source tools. We then developed a more advanced beacon detection analytic that built on the performance of the existing tools, both increasing the sensitivity so that it could detect more subtle threats and improving the selectivity to dramatically reduce false positives, and deployed it in the CyberSentry environment.

Almost immediately after deploying the new analytic, our threat analysts detected anomalous beacons on the OT network of a participating company. Working with that critical infrastructure partner, we identified the beaconing device as a security camera manufactured by the Chinese company Dahua, which is listed on the Federal Communications Commission (FCC) Covered List.

With this detection, we were able to create a machine learning model to automate detection of these cameras and deploy it widely across participating CyberSentry partners. Working with CISA, we discovered that the majority of entities in the program had these cameras on their networks. In some cases, we found hundreds of these devices on individual networks.

Notably, not all of the devices detected were branded as Dahua devices; many other manufacturers, both foreign and domestic, sold devices that used the same components as the Dahua camera and were behaving identically. From the network traffic, we were able to observe the devices beaconing back to suspected hostile overseas servers. Some of the devices were observed sending what appeared to be encrypted video to those servers. After acquiring and analyzing some of these devices, our reverse engineers were able to identify additional functionality that could enable back-door access to any network to which the device was connected. For purposes of today's discussion, it is worth noting that many of these cameras were sitting on OT networks, potentially granting access to control the physical processes in our infrastructure.

CISA partnered with the Department of Energy's Office of Cybersecurity, Energy Security and Emergency Response (CESER) and the DOE Office of Intelligence and Counterintelligence (DOE IN) to communicate our findings, first throughout the IC and then broadly out to the energy sector. Among the products of this collaboration was a set of playbooks we created that were published by CISA that allowed asset owners to detect these devices in their own systems. In this way, the security gains derived from this partnership between a few dozen critical infrastructure asset owners and CISA reverberated widely across U.S. critical infrastructure.

Immune Infrastructure Framework

Detection and mitigation represent just one aspect of defense against nation-state cyber threats to our critical infrastructure. Today, we are dealing with highly capable adversaries who bring a wide spectrum of capabilities to bear, including network operations, supply chain compromise, insider access, and close-access operations. The current threat picture demands that we take a multi-layer approach to ensure the resilience of the functions that depend on our infrastructure.

At LLNL, we approach the challenge of securing U.S. critical infrastructure through a structure called the "Immune Infrastructure Framework." We developed this framework to help define the parameters of critical infrastructure resilience and identify strengths and gaps in our nation's capabilities. It is largely reflected in the approach taken within DOE to help protect the energy sector, including the DOE Cyber Resilience R&D Capabilities Catalog issued by the DOE Chief Information Officer (CIO). The Immune Infrastructure Framework accepts that it is not practical to prevent all compromises, and structures defense in four layers to make it as difficult as possible for adversaries to achieve their goals and enable our critical infrastructure to operate through compromise.

- <u>Layer 1 focuses on understanding U.S. critical infrastructure systems</u>. This involves developing tools to characterize, model, and analyze our critical infrastructure so that we can understand our vulnerabilities and also identify where the most attractive targets for an adversary might be. This essentially allows us to look at U.S. infrastructure through the eyes of our adversaries.

- <u>Layer 2 attempts to keep the adversary out of our systems</u>. This largely involves assuring our supply chain to minimize both vulnerabilities and malicious functionality on the devices and software we put into our infrastructure systems. A key emphasis is on creating scalable capabilities to allow us to exponentially increase the number of devices that can be examined that are present within U.S. critical infrastructure.

- <u>Layer 3 focuses on detecting and responding to intrusions in our systems</u>. The majority of cyber attacks on critical infrastructure come from lower tier adversaries – individual hackers, criminal organizations, hacktivist groups – and use known malware and established tactics. The commercial security industry is quite capable of detecting these threat signatures and known adversary behaviors, so as a national laboratory we focus on "zero day" threats. We use advanced analytics and AI in conjunction with information from the IC to detect novel adversary tactics, capabilities, and activities that do not necessarily involve malware. More specifically, as a national security lab, we put significant energy towards assessing the unique capabilities that China, Russia, and Iran are developing that could hold our systems at risk that may never have been seen before.

- Layer 4 is about engineering our systems to operate through compromise. Despite our best efforts, the most determined and capable adversaries will compromise our systems; we must build in resilience by leveraging the distributed nature of our infrastructure and using techniques like collaborative autonomy, a set of algorithms designed to provide redundant, decentralized control of the system.

Support for Sector Risk Management Agencies

As defined in Presidential Policy Directive 21, CISA coordinates the national effort to secure and protect against critical infrastructure risks, but securing our nation's critical infrastructure is a distributed responsibility. There are 16 critical infrastructure sectors, with responsibilities distributed across Federal agencies, State and local governments, and asset owners and operators.

While all of the sectors are important, at LLNL, we pay particular attention to four sectors because of their close connection to national security concerns – energy, water, transportation, and communications. Sector Risk Management Agencies, such as DOE and DOD, have significant responsibilities to provide sector-specific expertise and coordinate activities within their sectors. We and our partners at other DOE national laboratories serve a vital connective tissue between Sector Risk Management Agencies, States, and local utilities and work directly with private sector entities to help ensure efforts are coordinated.

Among the sectors, the energy sector tends to be one of the most forward-leaning about cybersecurity because of the interdependencies between energy and every other sector. For its part, DOE CESER invests resources in creating capabilities for the energy sector that, in coordination with CISA, help set the pace for other sectors. For example, DOE is leaning forward to support industry in integrating AI securely. LLNL is leading CESER's analysis of the potential risks and benefits of AI to the energy sector. We are also developing testbeds for CESER to assess both the security and efficacy of various AI capabilities for the energy sector and researching new AI capabilities to improve the security and resilience of U.S. energy infrastructure.

Another way CESER is working to enhance the cybersecurity of the energy sector is through its Energy Cyber Sense Program which illuminates and reduces vulnerabilities to supply chains. LLNL leads national security-focused efforts as part of this work. LLNL also develops advanced tools and methodologies to understand and automate supply chain assurance with some of the critical partners in industry involved in these efforts.

In addition to our work on behalf of CISA and CESER efforts, our program has worked closely with the DOD, DOE, and CISA on efforts to enhance the security and resilience of Defense Critical Infrastructure (DCI). These assets are those portions of our nation's infrastructure that directly contribute to the mobilization and sustainment of military forces. We lead DOE's Defense Critical Energy Infrastructure analysis efforts and support multiple offices in DOD for broader DCI efforts. Our work has been critical in identifying potential risks posed by adversaries who, with advanced knowledge of our infrastructure and the interdependencies that exist between different components, could target assets in combination to cause damage that could not be realized in a single attack against one asset. LLNL's high-performance computing modeling and simulation capabilities and advanced optimization tools, codified in the Octopus and Teragrine toolsets, move beyond traditional natural hazard-focused planning processes which often only consider failures of single system elements and are not designed to identify cascading consequences from multiple simultaneous disruptions.

Conclusion

Thank you again for giving me the opportunity to share with you how LLNL, as a DOE national laboratory, deploys its multidisciplinary teams in partnership with CISA, CESER, DOD and other Federal partners to bolster the cybersecurity of the nation's critical infrastructure systems and advance U.S. national security. I would be happy to answer any questions.