FULLY OPERATIONAL: STUXNET 15 YEARS LATER AND THE EVOLUTION OF CYBER THREATS TO CRITICAL INFRASTRUCTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JULY 22, 2025

Serial No. 119–24

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

62–627 PDF WASHINGTON : 2026

COMMITTEE ON HOMELAND SECURITY

ANDREW R. GARBARINO, New York, *Chairman*

MICHAEL T. MCCAUL, Texas, *Vice Chair*
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona
ANDREW OGLES, Tennessee
SHERI BIGGS, South Carolina
GABE EVANS, Colorado
RYAN MACKENZIE, Pennsylvania
BRAD KNOTT, North Carolina
VACANT

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
ERIC SWALWELL, California
J. LUIS CORREA, California
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
DANIEL S. GOLDMAN, New York
DELIA C. RAMIREZ, Illinois
TIMOTHY M. KENNEDY, New York
LAMONICA MCIVER, New Jersey
JULIE JOHNSON, Texas, *Vice Ranking Member*
PABLO JOSÉ HERNÁNDEZ, Puerto Rico
NELLIE POU, New Jersey
TROY A. CARTER, Louisiana
AL GREEN, Texas
VACANT

ERIC HEIGHBERGER, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

VACANT, *Chairman*

CLAY HIGGINS, Louisiana
CARLOS A. GIMENEZ, Florida
MORGAN LUTTRELL, Texas
ANDREW OGLES, Tennessee
ANDREW R. GARBARINO, New York *(ex officio)*

ERIC SWALWELL, California, *Ranking Member*
SETH MAGAZINER, Rhode Island
LAMONICA MCIVER, New Jersey
VACANT
BENNIE G. THOMPSON, Mississippi *(ex officio)*

ALEXANDRA SEYMOUR, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

FULLY OPERATIONAL: STUXNET 15 YEARS LATER AND THE EVOLUTION OF CYBER THREATS TO CRITICAL INFRASTRUCTURE

Tuesday, July 22, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:12 a.m., at Room 310, Cannon House Office Building, Hon. Andrew R. Garbarino [Chairman of the committee] presiding.

Present: Representatives Garbarino, Gimenez, Luttrell, Ogles, Swalwell, and McIver.

Mr. GARBARINO. The Committee on Homeland Security, Subcommittee on Cybersecurity Infrastructure Protection will come to order. Without objection, the Chair may declare the committee in recess at any point.

The purpose of this hearing is to examine the evolution of cybersecurity threats to U.S. critical infrastructure following discovery of the Stuxnet malware 15 years ago. We will highlight the importance of securing operational technology, or OT, to bolster critical infrastructure resilience.

I now recognize myself for an opening statement.

Fifteen years ago, the world learned of Stuxnet, a computer worm that forever altered the cyber threat landscape. Regarded as the world's first digital weapon, it was designed to target industrial control systems. It was used against Iran's nuclear program, reportedly destroying a thousand centrifuges at the Natanz enrichment plant. Malware or malicious software has existed since at least 1970's. However, Stuxnet was different from its predecessor. The discovery of it demonstrated both the physical impact of malware and raised important questions about cybersecurity defense and offense. These are issues we continue to face today.

It revealed the significant impact that offensive cyber tools can have on critical infrastructure. It also demonstrated the importance of securing operational technology. By exploiting key vulnerabilities in industrial control systems, it proved that that cybersecurity is not only an IT issue. Cybersecurity threats can affect critical infrastructure we depend on daily, from water treatment to energy facilities. The cybersecurity threat landscape continues to expand and we need to make sure our cyber professionals are prepared to

defend both IT and OT. Doing so will strengthen the public and private sector's ability to rapidly respond to threats.

Since discovering Stuxnet 15 years ago, cybersecurity threats to critical infrastructure have drastically evolved and spread beyond just malware. We now see various cyber capabilities being used to hack critical infrastructure, including phishing, social engineering, denial-of-service attacks, and more.

While cyber attack vectors have grown and matured, malware is still of great concern. Malware comes in many forms, such as keyloggers, spyware, viruses, and ransomware, with ransomware comprising one-third of all cyber attacks in 2024. The interconnected nature of our networks, devices, and infrastructure means that critical infrastructure owners and operators now experience far more attacks than when Stuxnet was unleashed. Zero-day vulnerabilities are far from being eliminated.

Strengthening domestic cybersecurity resilience remains a key priority for this committee. Considering the sophisticated cybersecurity threats we now face, we are once again reminded of the importance of reauthorizing two key authorities ahead of their expiration this year: the Cybersecurity Information Sharing Act and the State and Local Cybersecurity Grant Program.

Reauthorizing CISA 2015 will ensure we keep encouraging rapid and trusted information sharing among public and private-sector entities and extending the State and Local Cybersecurity Grant Program will make sure that States and localities have reliable funding to strengthen their cybersecurity posture.

It is also worth examining the state of the Iranian cyber threat and potential impact Stuxnet had on Iran's cybersecurity posture. According to Nozomi Networks Labs, cyber attacks from Iranian threat actors surged by 133 percent in May and June 2025. An active Department of Homeland Security National Terrorism Advisory System notice also emphasizes the need to remain on high alert to Iranian cybersecurity threats to U.S. critical infrastructure.

Iran has embraced the targeting of critical infrastructure. The Islamic Revolutionary Guards Corps' affiliated actors have recently targeted OT such as U.S. industrial control systems in key sectors such as water and health care.

I look forward to examining the current threats facing U.S. critical infrastructure and enduring significance of Stuxnet with our panel of expert witnesses today. Today's witnesses represent a range of perspectives and I thank you all for contributing to our discussion about this pivotal moment in the history of cybersecurity. I am confident that your testimony will help us form a better understanding of today's digital weapons and the state of U.S. critical infrastructure resilience.

[The statement of Chairman Garbarino follows:]

STATEMENT OF CHAIRMAN ANDREW GARBARINO

JULY 22, 2025

Fifteen years ago, the world learned of Stuxnet—a computer worm that forever altered the cyber threat landscape. Regarded as "the world's first digital weapon," Stuxnet was designed to target industrial control systems. It was used against Iran's nuclear program, reportedly destroying 1,000 centrifuges at the Natanz enrichment plant.

Malware, or malicious software, has existed since at least the 1970's. However, Stuxnet was different from its predecessors. The discovery of Stuxnet demonstrated both the physical impact of malware and raised important questions about cybersecurity defense and offense. These are issues we continue to face today.

Stuxnet revealed the significant impact that offensive cyber tools can have on critical infrastructure. Stuxnet also demonstrated the importance of securing operational technology (OT). By exploiting key vulnerabilities in industrial control systems, Stuxnet proved that cybersecurity is not only an IT issue. Cybersecurity threats can affect critical infrastructure we depend on daily, from water treatment to energy facilities. The cybersecurity threat landscape continues to expand, and we need to make sure our cyber professionals are prepared to defend both IT and OT. Doing so will strengthen the public and private sectors' ability to rapidly respond to threats.

Since discovering Stuxnet 15 years ago, cybersecurity threats to critical infrastructure have drastically evolved and spread beyond just malware. We now see various cyber capabilities being used to hack critical infrastructure, including phishing, social engineering, denial-of-service attacks, and more. While cyber attack vectors have grown and matured, malware is still of great concern. Malware comes in many forms, such as keyloggers, spyware, viruses, and ransomware, with ransomware comprising one-third of all cyber attacks in 2024.

The interconnected nature of our networks, devices, and infrastructure means that critical infrastructure owners and operators now experience far more attacks than when Stuxnet was unleashed. And zero-day vulnerabilities are far from being eliminated.

Strengthening domestic cybersecurity resilience remains a key priority for this committee. Considering the sophisticated cybersecurity threats we now face, we are once again reminded of the importance of reauthorizing two key authorities ahead of their expiration this year: the Cybersecurity Information Sharing Act (CISA 2015) and the State and Local Cybersecurity Grant Program.

Reauthorizing CISA 2015 will ensure we keep encouraging rapid and trusted information sharing among public and private-sector entities; and Extending the State and Local Cybersecurity Grant Program will make sure that States and localities have reliable funding to strengthen their cybersecurity posture.

It is also worth examining the state of the Iranian cyber threat and the potential impact Stuxnet had on Iran's cybersecurity posture. According to Nozomi Networks Labs, cyber attacks from Iranian threat actors surged by 133 percent in May and June 2025. An active Department of Homeland Security National Terrorism Advisory System notice also emphasizes the need to remain on high alert to Iranian cybersecurity threats to U.S. critical infrastructure.

Iran has embraced the targeting of critical infrastructure. Islamic Revolutionary Guard Corps-affiliated actors have recently targeted OT, such as U.S. industrial control systems, in key sectors such as water and health care.

I look forward to examining the current threats facing U.S. critical infrastructure and the enduring significance of Stuxnet with our panel of expert witnesses. Today's witnesses represent a range of perspectives, and I thank you all for contributing to our discussion about this pivotal moment in the history of cybersecurity. I am confident that your testimony will help us form a better understanding of today's "digital weapons" and the state of U.S. critical infrastructure resilience.

Mr. GARBARINO. I now recognize the Ranking Member, the gentleman from California, Mr. Swalwell, for his opening statement.

Mr. SWALWELL. Thank you, Chairman.

Chairman, that was an elegant, impactful, artful statement, but you buried the lede. Our Chairman of the subcommittee has been selected by his colleagues to be the Chairman of the full committee with the resignation of Chairman Green effective earlier this week. So congratulations. I am excited for what that means for the full committee. You and I have worked quite well over the last 3 years on this committee, especially to take on our cyber challenges. To have somebody at the full committee with your cyber knowledge and expertise as our cyber threats are only escalating and AI has made that even more challenging and the threat of quantum computing and what that means for cryptology, you are the right person to help lead the committee to do that. So looking forward to

working with you and I think I speak on behalf of my colleagues that we congratulate you on that win.

Earlier this summer, Chairman Mark Green and I went out to my Congressional district and visited Lawrence Livermore National Laboratory and committee staff from both sides were there as well. As you know, Lawrence Livermore National Lab is the Nation's premier research and development facility. It attracts the best and brightest minds from around the world and helps keep the United States on the cutting edge of innovation, particularly related to national security technologies. Lawrence Livermore and our national labs are indispensable partners in our national effort to defend cyber space, keeping their finger on the pulse of our adversaries' tactics and motivations while helping to develop novel technologies to detect and disrupt malicious cyber campaigns. We saw Lawrence Livermore works first-hand and it is critical to national efforts to secure critical infrastructure our constituents rely on every day and the operational technology that underpins it.

The Lab's work is paying off dividends, especially related to the Chinese threat actors like Volt Typhoon, and I am pleased that the Lab today, through Dr. Gleason's testimony, will talk about its important work. Notably, the Lab is a key partner in CISA's CyberSentry program, which places sensors on private-sector networks on a voluntary basis to monitor for and detect cyber threats. The Lab contextualizes data from the CyberSentry program with other intelligence feeds, generates unique insights into malicious cyber activity, and provides network defenders the know-how to kick out the adversaries. The knowledge derived through the Lab's work benefits programs and activities across CISA. I am eager to learn how Lawrence Livermore and the national lab community can continue to support Federal efforts to better secure operational technology.

Additionally, I am interested to learn how other programs at sector risk management agencies and CISA, like the Joint Cyber Defense Collaborative, JCDC, support efforts to mature our collective approach to security. It is incumbent on the Federal Government to collaborate with its private-sector partners to bring security resources to bear to these under resourced sectors.

Also at this point I want to just remind the committee and the public that CISA can only function when it is fully staffed. It should not be free from reforms, but currently it has lost approximately 1,000 employees since the DOGE cuts began to take place. That affects its ability to work with the private sector and be responsive. Fewer brains and reduced funding means less capability, less capacity, and less collaboration, which is detrimental to ongoing efforts to mature operational technology security programs.

Also I would like to reiterate my strong support for the reauthorization of the other CISA, CISA 2015. Stakeholders have referred to CISA 2015 as the most successful cyber law ever passed and I was a part of writing it and passing it in 2015 as a Member of both this committee and the House Intelligence Committee. We cannot allow this critical authority to lapse.

Toward that end, I was pleased to see a clean 10-year extension included in the Senate Intelligence Authorization Act for Fiscal Year 2026. It sends a clear message to our partners and our adver-

saries that cybersecurity continues to be a bipartisan priority in Congress. I look forward to working with my House colleagues to provide non-Federal stakeholders the certainty they need to continue their strategic collaboration with the Government by passing a clean authorization before it lapses later this fall.

With that, I yield back.

Mr. GARBARINO. The gentleman yields back.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 22, 2025

The threat landscape facing our Nation is clear—critical infrastructure operational technology is a target for our adversaries, and our cyber defenses are not sufficient for current threats. Under the Biden administration, Congress and the Executive branch took important steps to strengthen OT security.

We invested $1 billion in State and local cybersecurity, and we have seen States use that money to better defend vulnerable water utilities and other high-risk sectors. We enacted the Cyber Incident Reporting for Critical Infrastructure Act so that the Federal Government would have better visibility into the threats facing our Nation.

CISA established the Joint Cyber Defense Collaborative, including a focus on industrial control system security, and improved its partnerships with sector-risk management agencies, hiring sector-specific experts to coordinate with their partner agencies. CISA further developed cyber performance goals to help critical infrastructure better understand how to improve their security. And the Biden administration initiated a series of sprints to strengthen the security of specific, under-resourced sectors.

Unfortunately, under the Trump administration, we have seen the Executive branch step back from prioritizing cybersecurity. Secretary Noem has overseen the loss of hundreds of cybersecurity experts from CISA, devastating the agency's capacity for responding to cyber threats. The President's budget request included a proposed 25 percent cut to CISA's programs, including eliminating its efforts to train the OT workforce. Secretary Noem eliminated the Critical Infrastructure Partnership Advisory Council, devastating the private sector's ability to collaborate on cybersecurity threats. And CISA has stalled efforts to carry out its statutorily-mandated obligations under CIRCIA.

With a Department of Homeland Security focused exclusively on mass deportations, our Nation is more at risk to cyber attacks from China, Russia, Iran, and other adversaries. Unfortunately, Republican leadership in Congress has not been much better. Former Chairman Green failed to move forward legislation to reauthorize the Cybersecurity Information Sharing Act of 2015, leaving us just 17 legislative days away from this vital authority expiring. And House Republicans are proposing to cut CISA's budget by $135 million.

I know this subcommittee recognizes the serious cyber threats facing our Nation, and I hope that this hearing will build greater awareness in Congress of the threats facing operational technology and the need for sustained investment in improved security.

Mr. GARBARINO. I am pleased to have a distinguished panel of witnesses before us today. I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. GARBARINO. Let the record reflect that the witnesses have answered in the affirmative. Thank you and please be seated.

I would now like to formally introduce our witnesses.

Ms. Kim Zetter is the author of "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon," and an adjunct professor at Georgetown University. She is also an award-winning investigative journalist who has written on cyberse-

curity and national security for more than 20 years. Ms. Zetter began her career covering security and privacy issues for *Wired,* where she wrote for 13 years.

Mr. Robert Lee is the chief executive officer and co-founder of Dragos, a global technology leader in cybersecurity for OT and ICS environments. Mr. Lee also serves as a lieutenant colonel in the Army National Guard, where he designs and leads OT cybersecurity response efforts. He is a member of the World Economics Forum Subcommittees for the oil, gas, and electricity communities, and he serves on the advisory boards of the International Society of Automation and National Cryptologic Foundation.

Tatyana Bolton currently serves as executive director of the Operational Technology Cybersecurity Coalition, where she advocates for effective OT cybersecurity and critical infrastructure resilience. Prior to her current role, Ms. Bolten served as a senior security policy manager at Google's Security Center of Excellence. Before joining Google, Ms. Bolton directed the Cybersecurity Emerging Threats Program at the R Street Institute and served as policy director of the Cyberspace Solarium Commission.

Dr. Nate Gleason is the program leader for cybersecurity infrastructure resilience within the Energy and Homeland Security Program at Lawrence Livermore National Laboratory. Prior to joining Lawrence Livermore, Dr. Gleason spent 12 years at Sandia National Laboratories in a variety of technical and management positions, including deputy to the vice president for the California Laboratory and deputy program director for Sandia's Homeland Security Program.

I thank the witnesses for being here today.

I now recognize Ms. Zetter for 5 minutes to summarize your opening statement.

STATEMENT OF KIM ZETTER, AUTHOR AND JOURNALIST, "COUNTDOWN TO ZERO DAY: STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON"

Ms. ZETTER. Thank you. Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee, thank you for this opportunity to testify about Stuxnet and threats to critical infrastructure. My name is Kim Zetter, and I'm a cybersecurity national security journalist, as well as an adjunct professor at Georgetown University and the author of the book on Stuxnet, "Countdown to Zero Day."

It was 15 years ago that Stuxnet was discovered on systems in Iran, but despite the passage of time, its impact is still felt today. Stuxnet was a digital weapon designed to sabotage Iran's nuclear program by targeting industrial control systems at its uranium enrichment plant at Natanz. But these are the same kinds of systems used in U.S. critical infrastructure. I've been asked to describe how Stuxnet operated and the implications for U.S. critical infrastructure and whether these systems are any more secure today than when Stuxnet was discovered.

Stuxnet was a first-of-its-kind attack, the first known case of malicious code designed to leap from the digital world to the physical realm to cause disruption and destruction not of the computers it infected, but of equipment and processes these computers con-

trolled, in this case the centrifuges at Natanz. The same techniques Stuxnet use can be used against critical infrastructure in the United States to disrupt services the public, Government, and military rely on, or to damage equipment that can also cause death, either directly by causing passenger trains to collide or indirectly by preventing patients from being treated at hospitals because the electricity is out. I provided in my written testimony details about how Stuxnet operated, so I won't go into them here, but I want to point out two things that are relevant.

First, Stuxnet spread to millions of computers, but it only unleashed its destructive payload on the specific systems its creators were targeting. It didn't sabotage other systems because Stuxnet was a highly sophisticated, carefully crafted and tested, precision weapon designed to avoid collateral damage. Other attacks, however, don't need to be precise or sophisticated to cause disruption or damage. This is worth noting given the recent warnings about the potential for Iran to launch cyber attacks against the United States. Iranian hackers don't have the skills to pull off a Stuxnet-like attack, but they don't need them to disrupt or damage systems.

Second, when Stuxnet was first discovered, researchers believed it was an espionage tool. This is because every time it infected a new system, it searched for the presence of Siemens' industrial control system software. Siemens software is used to control manufacturing assembly lines and other industrial processes, so researchers believed whoever was behind the malware was trying to steal blueprints or designs to for industrial plants. After reverse engineering the code, however, they realized it was designed for sabotage.

This is significant because disruptive or damaging attacks can be indistinguishable from espionage in the initial stages of infection. Both can use the same tools and techniques to gain access and move within networks to find data or the systems they want to disrupt. What's more, intrusions done initially for intelligence purposes can morph into disruptive or destructive operations.

I say this because a lot has been written recently about the SALT and Volt Typhoon intrusions of telecoms and critical infrastructure that are attributed to China. These compromises don't appear now to be aimed at disruption or damage, but could morph into such operations in the future.

One of the most significant impacts of Stuxnet was—Stuxnet had was to raise awareness about vulnerabilities in critical infrastructure. Prior to Stuxnet, the security community was focused on IT networks, the business networks that you use to send email. But Stuxnet put OT networks in the spotlight, and once researchers began to examine them, they discovered serious software flaws as well as architectural problems that couldn't be fixed with a software patch. They also found many systems connected to the internet.

The following is a small sample of processes that industrial control systems control: opening and closing cell doors at high security prisons, operating traffic lights and HVAC systems, routing computers—routing commuter and freight trains to prevent collisions, controlling temperature at which food is pasteurized and steel is forged, operating chemical and pharmaceutical plants, and control of the flow of electricity.

A lot has been done since Stuxnet to secure critical infrastructure in the United States, but many issues persist. I'll just give one example before I close. In 2009, in Washington, DC, a Metro train plowed into the back of another train stopped at a station during the afternoon commute. Sensors on the track should have indicated to the incoming train that a train was stopped ahead of it, but the sensors failed and the collision killed 9 people and injured 80 others. This wasn't caused by a cyber attack, but this month CISA issued a security alert about a decade-old flaw in train braking systems that hackers could exploit to cause a collision like the one in 2009. That flaw exists in the protocol that devices located in the front and back of trains use to communicate with each other to engage the brakes. The protocol uses weak authentication, which means an attacker can impersonate one of these devices to cause a train to suddenly halt or the brakes to fail. The flaw can't be exploited over the internet. An attacker needs proximity to send a command. But this doesn't make it any less dangerous.

The researcher who discovered the flaw discovered it in 2012 and reported it to the Association of American Railroads. But the AAR reportedly dismissed it, believing no one could exploit it. It was only this year, after the research in CISA threatened to go public, that the AAR announced it would replace the protocol. A new protocol won't be ready until 2027 at the earliest.

Thank you.

[The prepared statement of Ms. Zetter follows:]

PREPARED STATEMENT OF KIM ZETTER

22 JULY 2025

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 Weapon.* 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, 3 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 United States 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 cyber attacks against U.S. critical infrastructure, following the recent U.S. 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 U.S. critical infrastructure.

Although a lot has been done since the discovery of Stuxnet to try to secure critical infrastructure in the United States, 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 9 people and injured 80 others. This incident, as far as anyone knows, wasn't the result of a cyber attack.

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 or 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 shut down 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 indi-

rectly 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 cyber crime 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 on-going 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 stand-alone 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 2 hours or until the pressure inside the affected centrifuges rose 5 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 occur-

ring. 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 2-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 15 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 3 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 wide-spread 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 off-line 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 cyber criminals 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 cyber attack. 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 cyber attack. 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 U.S. economy—Colonial Pipeline supplies 45 percent of fuel to the East Coast, which amounts to about 2.5 million barrels daily—had sufficient back-ups 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 7 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 2 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 back-ups off-line 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 on-line 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, 3 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 off-line 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 2 universities found that MFA can block up to 99 percent of bulk phishing attacks and about 66 percent of targeted attacks. Yet a survey published by Trellix found that 75 percent of respondents in the U.S. 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 2 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 United States is headed if the problems aren't addressed.

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

Mr. GARBARINO. Thank you, Ms. Zetter.

I now recognize Mr. Lee for 5 minutes to summarize his opening statement.

STATEMENT OF ROBERT M. LEE, CHIEF EXECUTIVE OFFICER AND CO-FOUNDER, DRAGOS INC.

Mr. LEE. Chairman Garbarino, Ranking Member Swalwell, Members of the subcommittee, 15 years ago, Stuxnet proved cyber attacks could cause physical destructions. Attacks on OT networks are under sustained and sophisticated assault from our adversaries today. I'm Robert Lee, CEO of Dragos, a former Air Force officer in NSA, and now serving since the last time we all met in this committee in my role as lieutenant colonel in the Army Guard designing out OT defense strategies. I spent my career protecting these industrial systems that power our society.

Let me be blunt. We are not prepared for a major attack on our critical infrastructure. We know that such an attack would be part of any major conflict with an adversary, but we are not doing enough to prepare and the results of continued failure could be catastrophic, including the loss of life. At Dragos, we track over 25 state and non-state actors that target operational technology directly. Nine different malware families have been built specifically for industrial systems. The most versatile is very opposite to

Stuxnet. Where Stuxnet was very, very targeted, Pipedream can be used against everything from unmanned aerial vehicles to water systems to power systems.

Increasingly, homogenous machinery and technical systems have increased the OT attack surface and raised the potential consequences of a large-scale attack, but defense is doable. One example, Littleton Electric in Massachusetts used a Federal grant to install our technology on the network after FBI intel indicated to them that they were being targeted by Volt Typhoon. We detected, isolated, and mitigated the attack with their partnership. They were able to do this because they had visibility in their OT networks and they were proactive in their security. Most companies don't do this. We know what works. Here are a few things that I recommend that we can do.

First, we must stop treating OT like IT. These systems have different risks and require different defense strategies. Hearings like this one are critical to raise awareness of this distinction. A significant portion of the funding and resourcing in the community goes to IT, whereas the critical part of critical infrastructure is OT.

Second, make public-private partnerships count. At Dragos, we uncovered Pipedream in coordination with the NSA and an undisclosed third party. We ended up coordinating with CISA and the electric ISAC and that allowed us to warn operators before the adversary was even allowed to deploy it against targets across the United States. Broad, unfocused information-sharing efforts, though, do not work. Targeted, focused coordination does.

Third, we must streamline Federal guidance. Right now, too many agencies are sending too many messages, many of which are overlapping and often contradictory to our industry. We have to tell the industry, here's the threat, here's what success looks like. We have to let them handle the how. Right now it is extremely confusing for asset owners and operators on turning to who is going to be the one to help them and, most importantly, what the actual guidance is that they should follow beyond regulatory.

Fourth, we have to let the private sector lead on technology. We already have the tools to detect advanced threats. Federal efforts to replicate them just waste money and slow adoption. Fund deployment, not reinvention. Government should focus on over-the-horizon threats. The private sector has already created the tools and techniques needed to deal with the threats in the here to now, it's just about execution. Government tools have consistently underperformed in comparison to private-sector tools and at a higher cost to taxpayers.

Fifth, secure the supply chain. Critical infrastructure vendors must meet real security standards. Right now, all of the focus is placed on asset owners and operators and not the vendors. Asset operators and their vendor community should share responsibility for meeting basic security requirements for all the components that are installed into our critical infrastructure, even the security vendors. As the CEO of Dragos, I'm surprised that I have the amount of flexibility I do to make willfully poor security choices to increase my margins. Though we have not done that and would not do that, I'm surprised by the ability of CEOs to make that decision. I be-

lieve we need higher standards and more selectivity into who can sell into critical infrastructure and how.

Finally, we need to fix Federal response coordination. Most operators simply don't know who to turn to or to call after an incident or what they'll get in response. Responses differ across State lines and there's no basic credentialing for who shows up and what they can do. I'm helping write a national OT response plan in my role at the 91st Cyber Brigade, but we need legislative support to cut through the bureaucracy. I found great partnership in this effort with CISA, particularly strong support with Shawn Plankey, and I look forward to his confirmation. We simply know what needs to be done and it's time to stop standing in our own way. Our kids' lives depend on it.

To close, our adversaries are gaining ground, but we have the tools, the knowledge, and the people to win. Now we need large-scale execution in the public and private sectors. We know what needs to be done, we just need to do it.

I'm grateful to all of you for holding this hearing and look forward to the rest of our conversation.

I yield back my time.

[The prepared statement of Mr. Lee follows:]

PREPARED STATEMENT OF ROBERT M. LEE

22 JULY 2025

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 15 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 15 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 9 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 percent of those resulting in some disruption to operations and around 25 percent 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 15 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 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 me 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 life cycles, and evolving threats targeting operational infrastructure. All these differences dictate some different security practices, technologies, and policy responses. Regulators and policy makers must

[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*.

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 percent of cyber spend is focused on IT systems, with just 5 percent 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 5 security controls were the most effective and could significantly decrease the risk of cyber threats.[4] Not tens or hundreds but simply 5 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 third 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

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

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 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 policy makers 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. Policy makers 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.

Mr. GARBARINO. Thank you, Mr. Lee.

I now recognize Ms. Bolton for 5 minutes to summarize her opening statement.

STATEMENT OF TATYANA BOLTON, EXECUTIVE DIRECTOR, THE OPERATIONAL TECHNOLOGY CYBER COALITION

Ms. BOLTON. Thank you, Chairman. Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee, thank you so much for the opportunity to testify today. 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'm the executive director of the Operational Technology Cybersecurity Coalition. The OTCC is a coalition of OT cybersecurity organizations created critical infrastructure operators and thought leaders representing the entire OT life cycle and protecting our Nation's critical infrastructure assets. We provide vendor-neutral perspectives on securing our collective defense and advocate for improved OT security policy.

Stuxnet marked a pivotal moment in cyber warfare by demonstrating that digital tools could indeed cause real-world physical destruction to systems known as operational technology, or OT. OT is the technology that makes machines run, like pumps and valves on the manufacturing room floor or machines that control compressors and filters in a water treatment facility. It's crucial to recognize, as Rob said, that operational technology, OT, is distinct from information technology, IT. Their respective security requirements differ considerably. OT cybersecurity must prioritize safety, reliability, and physical process continuity, and these systems can be older, having been built to last decades, and many never designed to be connected to the internet in the first place.

Despite the elevated risks associated with attacks on OT systems, this area of cybersecurity remains significantly under prioritized and underfunded. The OTCC is working on a number of efforts and has provided multiple recommendations to the committee and I'd like to highlight a few of them here from my written testimony.

First, we need to focus on awareness. The United States must prioritize OT cybersecurity to prepare critical infrastructure against the growing threats. Our Government has acknowledged that U.S. infrastructure is at risk. However, it has not taken sufficient steps to address the growing vulnerabilities in the wake of attacks like Cyber Avengers or Volt and Salt Typhoon. While securing IT is important, the OT systems that, if attacked, turn off our lights, bring hospitals to a standstill, and disrupt essential services. Congress must urgently answer the question of who holds responsibility for these risks, as a debilitating cyber attack on our critical infrastructure would demand clear accountability.

Second, Congress must reauthorize CISA 2015. In May, our Coalition submitted a letter to this committee urging the reauthorization of the Cybersecurity and Information Sharing Act of 2015, which will expire in September of this year. As you well know, this legislation is crucial to information sharing and strengthening U.S. collective defense. Both public and private-sector security teams rely on information sharing from other organizations to strengthen their defenses. If the legal protections established by this act were to lapse, this flow of information would be disrupted up to 80 to 90 percent and national security put in jeopardy.

Third, we must better resource OT security. From addressing the growing tech debt, hiring cybersecurity experts, to procuring and building updated and secure systems, OT owners and operators don't have the necessary funding to defend their networks and often 99 cents of every dollar is spent on physical security. We need to address critical infrastructure security through a whole-of-nation approach. Just as we wouldn't expect an individual county, such as Polk County in Texas, to defend themselves against missile strikes

from a nation-state actor, we shouldn't expect them to respond to cyber attacks on their own.

This is a national security priority. This is why the State and Local Cybersecurity Grant Program must be reauthorized. These resources allow underfunded critical entities to remove Chinese routers, hire cybersecurity staff and replace outdated servers. Congress should also explore whether there are other opportunities to provide economic incentives to critical infrastructure owners and operators to invest in OT security. The biggest vulnerability in any of your States and all of the States is your lowest common denominator, so we must increase the security baseline of across the board.

The threat to critical infrastructure and operational technology from our adversaries, including Iran, is real and growing. OTCC aims to work with this committee and our stakeholders to achieve our common objective. With the right policies, resources, and partnerships, we can build a more resilient and secure Nation.

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

[The prepared statement of Ms. Bolton follows:]

PREPARED STATEMENT OF TATYANA BOLTON

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 life cycle 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 cyber attack 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 policy makers 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 cyber attack on our critical infrastructure would demand clear accountability.

As you examine these issues, there are 3 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. critical infrastructure, particularly in the transportation and manufacturing sectors, with Nozomi Networks Labs observing a 133 percent 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 cyber attacks on their own. Of America's 3,144 counties, about 1,500 of them can be classified as rural.[3] These

---

[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.*

[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/*.

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 1-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 8-day national disruption would total a 1 percent 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, health care, and financial services. The intricate interconnectedness of these systems means a successful cyber attack 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.

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 policy makers.

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.

---

[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.*

[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.

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.

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 road map 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 road map 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.

March 21, 2025.

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, DC 201515.

The Honorable *Hakeem Jeffries*,
Minority Leader, U.S. House of Representatives, Washington, DC 20515.

Via Electronic Mail

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

[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.*

[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).

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] 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 9 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 cyber criminals 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.

Mr. GARBARINO. Thank you very much.

I now recognize Dr. Gleason for 5 minutes to summarize his opening statement.

---

[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), including our communications systems—*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.

STATEMENT OF NATHANIEL GLEASON, PH.D., PROGRAM LEADER, LAWRENCE LIVERMORE NATIONAL LABORATORY

Mr. GLEASON. Chairman Garbarino, Ranking Member Swalwell, and Members of the subcommittee, thank you for the opportunity to testify today. My name is Dr. Nate Gleason. I'm the program leader for the Cyber and Infrastructure Resilience Program at Lawrence Livermore National Laboratory in Livermore, California. I lead a multidisciplinary team that works to develop technologies to develop—to address nation-state threats in the domain of gray zone conflict. Our primary emphasis is on the role of critical infrastructure and national security. I appreciate the committee's interest in our work, particularly your visit to the Lab earlier this summer, which reflects your commitment to bolstering the Nation's cybersecurity. I'm honored to be here on behalf of Lawrence Livermore and National Nuclear Security Administration Laboratory and a proud member of DOE's Network of National laboratories.

Nearly everything we do as a Nation, from energy transmission to projecting force around the globe depends on critical infrastructure. This makes these systems prime targets. Our adversaries are highly capable and invest heavily to hold our infrastructure systems and the functions that depend on them at risk. To defend against this threat, Government and the private sector must partner to out-innovate the competition and bring our best technology into operations.

One way CISA helps address this need is through the CyberSentry program. Since 2020, it has looked to Lawrence Livermore for core support for CyberSentry, with our role being to develop and deploy advanced analytics to monitor and hunt for threats. Through CyberSentry, cyber researchers gain real-time access to operational networks and can leverage significant investments in national laboratory computational and analytical capability, combined with information from the intelligence community, to develop and deploy tools to detect the latest attack techniques.

As one example of program success, in 2022, we detected high-risk Chinese surveillance cameras, just like these on the table in front of me, that were stealthily built into U.S. infrastructure systems. We leveraged our Skyfall laboratory to develop an advanced beacon detection analytic that increased sensitivity to detect these threats while improving selectivity to dramatically reduce false positives. When we deployed the analytic to CyberSentry partners, almost immediately our analysts detected anomalous beacons on the OT network of a participating company. Our team identified the beaconing device as a camera manufactured by the Chinese company Dahua. Livermore developed a machine learning model to detect these devices at scale and deployed it. We found cameras on most of the participating CyberSentry entities, in some cases hundreds of them.

Network traffic showed that these devices were beaconing to suspected hostile overseas servers. Some appeared to be transmitting encrypted video. Reverse engineering of the devices revealed they were also capable of providing a backdoor to any connected network. Notably, these devices were mostly sitting on OT networks, providing direct access to the physical processes.

We worked with CISA to create and publish a set of playbooks that went out broadly to help asset owners who are not part of CyberSentry detect these devices on their own systems. This illustrates how the CyberSentry partnership between just a few dozen critical infrastructure asset owners, national labs, and CISA enhances cybersecurity across U.S. critical infrastructure.

It's important to recognize detection represents just one aspect of defense against cyber threats to our infrastructure. The current threat picture demands a multilayer approach. At Livermore, we use what we call the Immune Infrastructure Framework. This 4-layer approach recognizes that we can't stop all attacks and instead, seeks to make it as difficult as possible for adversaries to achieve their goals.

Layer 1 focuses on understanding critical infrastructure systems through modeling, simulation, and analysis. This essentially allows us to look at U.S. infrastructure through the eyes of our adversaries. Layer 2 attempts to keep the adversary out of our systems through supply chain assurance. Layer 3 focuses on detecting and responding to intrusions. We put significant focus on addressing the previously unseen over the horizon threats that China, Russia, and Iran are developing that could hold our systems at risk. In layer 4, we engineer our systems to operate through compromise by using techniques like collaborative autonomy, which are designed to provide redundant decentralized control of systems.

While all 16 critical infrastructure sectors are important, we pay particular attention to energy, water, transportation, and communication because of their close connection to national security. The energy sector is among the most forward-leaning in cybersecurity. Its Sector Risk Management Agency, DOE CESER, invests resources in creating capabilities for the energy sector that, in coordination with CISA, help set the pace for other sectors. CESER is currently working to ensure that AI can be securely integrated into energy sector operations. Livermore is leading its analysis of potential risks and benefits of AI in the energy sector. We are also developing testbeds to assess the security and efficacy of various AI capabilities for the sector.

Another way CESER is working to enhance cybersecurity is through its Energy Cyber Sense Program, which focuses on supply chain security. We also work closely with the Defense Department on defense-critical infrastructure. Through this work we have identified how adversaries with advanced knowledge of our infrastructure and interdependencies that exist between components could exploit multiple assets simultaneously to create cascading damage far worse than any single point attack.

Thank you again for the opportunity to testify. I would be happy to answer any questions.

[The prepared statement of Dr. Gleason follows:]

PREPARED STATEMENT OF NATE GLEASON

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 United States 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 pre-position 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 United States 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 4 layers to make it as difficult as possible for adversaries to achieve their goals and enable our critical infrastructure to operate through compromise.

- Layer 1 focuses on understanding U.S. critical infrastructure systems. 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.
- Layer 2 attempts to keep the adversary out of our systems. 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.
- Layer 3 focuses on detecting and responding to intrusions in our systems. 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 toward 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 4 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.

Mr. GARBARINO. Thank you, Dr. Gleason.

Members will be recognized by order of seniority for their 5 minutes of questioning. An additional round of questioning may be called after all Members have been recognized.

I recognize the gentleman from Florida, Mr. Gimenez, for 5 minutes.

Mr. GIMENEZ. Thank you, Mr. Chairman. Let me congratulate you on winning the Chairmanship of the entire committee. It Is well done and I look forward to working with you.

I also share the concerns of the Ranking Member about the reauthorization of CISA 2015. Now that the Chairman of the subcommittee, now the Chair of the entire committee, I am sure that we're going to be accelerating that process. It is a clean reauthorization, but then eventually we are going to have to look and see how we can tweak that. But first, we need a clean reauthorization.

Ms. Zetter, I am curious about the viruses and the malware, and I am wondering if they are starting to act like real viruses. A real virus, when they enter the body and the body starts to attack it, can react, it evolves to defend itself. Have you seen that progress with computer viruses, with cyber viruses? Ability of a virus to evolve so that it can protect itself from any kind of defense mechanism?

Ms. ZETTER. We've seen the early stages of that. I don't think that we've seen something that's fully, I would say, mature and operational. Rob has a better idea of that because he deals with the malware that comes in. But we've seen sort-of—even sort-of hints of that, even years ago, just not fully developed. Obviously, now with AI, that opportunity exists to make something even more autonomous, and also the ability to morph very rapidly to the environment.

Mr. GIMENEZ. Interesting that is a scary thought, right? That whatever we do, the virus will protect itself somehow and find a new way to do what it needs to do.

I also, you know, I agree that OT is actually the more important aspect of cyber attack. That is really the stuff that is really going to hurt us, cause accidents, kill people, disrupt everything that we do. You know, I mean, if I can foresee a day where, you know, somebody presses a button and the next, all the lights go out in North America, right? That would be a little bit disruptive, I believe.

Ms. Bolton, you talked about the lack of coordination here in the United States. I would think that if you kind-of map out who has got what, who is responsible for what, it would look like a bowl of spaghetti. Am I too far off?

Ms. BOLTON. I'd say you're not very far off at all. I think there are a wide range of frameworks that are in place, a wide range of coordination mechanisms, as Rob mentioned in his testimony. Also difficulty for the industry to come into the Federal Government. There's not one specific door. There's not one agency that's responsible for cyber incident response. So they all work together.

So—but we've got local and State agencies responding to incidents. You've got vendors and industry. You've also got Federal Government involvement. So I absolutely believe that we need to streamline that process. I know the committee is working on harmonization, cyber harmonization. We very much support that effort because we need to have one easy way, one door for the industry to come into the Federal Government for support, and then also for the response and collaboration to be more clear.

Mr. GIMENEZ. Now, you said that they work with each other, but do they really? Don't they—do you see turf guarding a lot?

Ms. BOLTON. I can't say that we don't see turf guarding. I will say that there are experts, national security, you know, professionals who are absolutely intent on securing the networks for which they're responsible.

Mr. GIMENEZ. But a lot of people will say, well, that's, is really, my realm. Well, no, it is my realm and all. I mean, look, that is just the norm in any bureaucracy, OK? So we have so many agencies doing the same things, that is a natural tendency of bureaucracy to try to protect themselves, OK, and turf guard.

Mr. Gleason, in terms of China, I serve on the Select Committee on China, and I have been calling for—we cannot decouple fast enough from China. Things that may be innocuous, cameras, all right, there is nothing innocuous about them. They are malicious. They are relentless in their attacks on us. I mean, I was thinking, yes, cameras is one way. Then they report back to China. Right? They can also integrate themselves into the IT system. That becomes an OT problem, maybe. All right.

We had issues where I used to be the mayor of Miami-Dade County with cameras at our port system that was reporting back to China. We don't know what it was reporting, probably what kind of commerce we were doing at that port. We also found that they had infected our systems. They were just lying around. OK? We don't know what they were lying around for, but I am sure that it wasn't for a good purpose.

So what can we do to stop this, you know, this relentless attacks that we are getting from these systems?

I am sorry, my time is up and I yield back.

Mr. GARBARINO. OK. I was going to say they can answer the question, if you want.

Mr. LUTTRELL. I will ask it for you.

Mr. GARBARINO. I now recognize the gentleman from Texas, Mr. Luttrell, for 5 minutes.

Mr. LUTTRELL. If you are reading my notes, sir.

Mr. GIMENEZ. I stole it.

Mr. LUTTRELL. Yes. What can we do to—I don't even know how you scale something to this size. What can we do looking forward or looking downstream? I cast that out to Mr. Gleason, you can start.

Mr. GLEASON. Yes, I think everything you are mentioning I would agree with. I think what this phenomena that we're seeing is, is China has recognized that critical infrastructure is a new domain of conflict. I think we are catching up to that still. They put a lot of energy into this. They are very good. We are not going to stop them.

One of the goals that we have with the approach we've taken, as I mentioned, the immune infrastructure framework, our goal is to make it as hard as possible for them to achieve their objective at each layer. That includes understanding what they're trying to do. It includes securing our supply chains, includes detecting, responding, and, most importantly, it includes building our systems so that we can live even if they compromise them. That doesn't make our mission fail.

Mr. LUTTRELL. The cyber defense is very reactionary. We have no idea what's coming at us. The challenging part, I think personally, is, you know, and I am not speaking for—look, I mean there is only 4 of us. It is hard to dork out on cybersecurity, cyber risk, and cyber threat. You really got to be passionate about this. The number of subject-matter experts that walk into our offices every single day that say they are the absolute best at what they do is mind-numbing.

The committee is very open-minded to the collective, your group, of saying the best way forward to defensively and offensively, this is what we need. This is most likely the best way forward OT, IT. OK. How do we get that done? Because it changes every single second of every minute of every hour of every day. The cyber profile, the cyber technology, the cyber understanding, everybody is trying to be—to outdo somebody else. Again, very reactionary. How do you defend against something like that?

Ms. BOLTON. So I would say we need to start even at the very beginning. Most agency—most sectors have not done an OT asset inventory. So they don't even know what they have.

Mr. LUTTRELL. Scale that to the Continental United States.

Ms. BOLTON. Absolutely, absolutely. So I'll give you an example. There was an incident response team that went out to a pipeline, this was several years ago. They asked them how many open ports or ports they have. They said, well, just these that you see in this room here, and that was all their IT systems. By doing investigations through the internet billing that that pipeline had, they found they had over 10,000 open unprotected ports. So that's—you know, you need to be able to at least on some kind of spreadsheet be able to tell what you have in order to be able to start fixing it. That includes things like putting in multifactor authentication where it's possible, doing supply chain security, as you said, building defense in-depth, and building resilience.

Mr. LUTTRELL. Is that even a probability to do?

Mr. LEE. Yes, if I could add to that, we very much know what to do. But again, if you think about it from a Government perspective with private sector, if I'm in the water sector and I'm trying to look to CISA, EPA, and all the other components and players on what should I focus on, there's a lot of go be cyber safe, go be cyber secure, go do cyber, cyber, cyber something. Not actual guidance, not, well, we want to prepare for Volt Typhoon. This is what we're looking at. Here is what we think success looks like. However you want to figure it out, go, and then resourcing it. Like, we have the technologies that exist, we have the people trained, but there is a lot of overlapping guidance and it's paralyzing the private sector.

Mr. LUTTRELL. We weren't ready for Volt Typhoon and Stuxnet. Ms. Zetter, I am going to shift over to you. I don't know how long whomever created that and handed that football off to where it landed. I mean, but the technology in the early 2000's is not the same as it is in 2025 with the use of AI, AGI. I am assuming that you can take the baseline algorithm from Stuxnet because it had a few bugs in it. That is how we found it, if I am speaking correctly. When they started digging in and found Stuxnet, there were just a small bit of glitches in there. Like, all right, here it is. Now we are tracking. Then we unpacked it and, OK, here it is.

Ms. ZETTER. The core—I'm sorry.

Mr. LUTTRELL. Yes, ma'am, go ahead.

Ms. ZETTER. The core of Stuxnet did not have glitches, but the spreading mechanisms were reckless and it caused Stuxnet to spread around the world, and this is why it got caught?

Mr. LUTTRELL. OK. Are we doing—OK. Well, I am going to make the assumption that since that thing has been handed back to us and globally, that technology and AI, AGI will advance Stuxnet, SolarWinds in some way, and we won't be able to not only keep up, catch up, but I am assuming there is a probability that it is just going to outrun everything. Is that a fair statement?

Ms. ZETTER. Yes. I mean, the details that I provided in the written testimony goes in depth into how Stuxnet operated and how sophisticated it was. That was state-of-the-art in 2010, and it was really genius the way that it was designed. If you can imagine now, 15 years later, how much more advanced that that should be at this point.

Mr. LUTTRELL. Yes.

Ms. ZETTER. Then also with AI, then, yes, it's going to really fast forward.

Mr. LUTTRELL. I yield back.

Mr. GARBARINO. The gentleman yields back. Thank you very much.

I now recognize Ranking Member Mr. Swalwell for 5 minutes of questioning.

Mr. SWALWELL. Thank you. As part of the fiscal year 2022 NDAA, the National Defense Authorization Act, Congress authorized the CyberSentry program, which deploys sensors on a voluntary basis on critical infrastructure partners in order to detect malicious activity, as I noted in my opening statement. A critical part of that program is the role that Lawrence Livermore National Laboratory plays in analyzing CyberSentry data.

Dr. Gleason, what is the current status of Lawrence Livermore's partnership with CISA on CyberSentry?

Mr. GLEASON. We've supported CISA in various aspects of critical infrastructure security for about a decade. Currently, we have agreements that are making, our funding agreements, are making their way through DHS processes. Unfortunately, those are still making their way through DHS processes. Our work with CISA expired last Sunday.

Mr. SWALWELL. What does it mean that it expired? Is it turned off? Are you able to operate without authorities or funding? What is the posture right now for this important work?

Mr. GLEASON. National laboratories are not legally able to operate without being funded by a Government agency. So our threat-hunters stopped monitoring networks on Sunday.

Mr. SWALWELL. Who needs to turn it back on?

Mr. GLEASON. We need the interagency agreement between DHS and DOE to be completed.

Mr. SWALWELL. Would this be a sign-off from the Secretaries of both Energy and Homeland Security?

Mr. GLEASON. Somewhere in that chain, yes. I'm not completely familiar with the funding processes that exist in those agencies right now, but yes, it needs to be signed off by both organizations.

Mr. SWALWELL. Earlier in your testimony, you alluded to some cameras and malicious activity that you had found that have been Chinese-placed. Is that the type of work that the Sentry program does?

Mr. GLEASON. Absolutely. We're looking for threats that haven't been seen before. We're looking for threats that exist right now in our infrastructure. One of the great things about the CyberSentry program is it takes the research and marries it with what is actually happening on the real networks. So we're not just doing science projects. We're deploying that technology out in the real world, detecting real threats.

Mr. SWALWELL. Just so I understand you have—so you now with the program that has at least lapsed, or hopefully temporarily lapsed, the sensors are still deployed, is that right?

Mr. GLEASON. That's correct. The sensors are still deployed. They're still gathering data. We just aren't analyzing the data that's coming in.

Mr. SWALWELL. So I guess you are telling me because you don't have the funding, you are not allowed to look at the data legally. That is the problem.

Mr. GLEASON. That's correct.

Mr. SWALWELL. So, theoretically, we have deployed sensors on critical infrastructure, and there could be a malicious attack occurring right now that you are not legally able to see until the program is refunded.

Mr. GLEASON. That is correct. Lawrence Livermore analysts are not able to monitor that data right now.

Mr. SWALWELL. What is the risk of you being blind to what these sensors are detecting?

Mr. GLEASON. I think everything that we've talked about in this hearing, we've seen how important critical infrastructure is to everything we do as a country. I think I'll echo a talking point I frequently hear from Dragos. One of the most important things is getting visibility into what's happening on our OT networks. We don't have enough of that. So losing this visibility through this program is a significant loss.

Mr. SWALWELL. A major priority of mine has been to improve operational collaboration between the Federal Government and the private sector. To do so, CISA must have the appropriate forms for such collaboration, including the JCDC and CPAC.

Ms. Bolton, how can JCDC be strengthened so that it can better facilitate OT security collaboration? Why is it important that CPAC be restored?

Ms. BOLTON. Thank you for the question. I think CPAC is an organization that allows industry to talk to the Government. Right now, industry is not able to convene with the liability protections that come or the information-sharing protections that come with CPAC authorities. So that becomes a bit of a—that becomes a problem. It's a national security concern when operational collaboration can't happen between those two entities.

I believe it's very important for CPAC authorities to come back. I think as much as possible, industry is continuing to try to work with—through other mechanisms. But there was nothing specifically like CPAC. We also are—we're continuing to work with JCDC

and other areas within CISA on OT security issues. I think what we'd like to see from JCDC, if we're talking about additional work, is more concrete OT efforts that industry can get involved with from the ground up.

Mr. SWALWELL. Great. Thank you.

Yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentleman from Tennessee, Mr. Ogles, for 5 minutes of questions.

Mr. OGLES. Thank you, Mr. Chairman, and thank you to the witnesses for being here.

Obviously, this is a high-stakes issue. I mean, it is the next battlefront, if not the battlefront, as we move forward. When you look at the China threat that Ms. Zetter, I think, you know, you have touched on, or all of you have touched on. But specifically I want to start with Ms. Bolton.

So formerly I was county executive in my community. What I can say is that, you know, although we were one of the fastest-growing counties in the State of Tennessee, No. 1 producer for manufacturing jobs in the State of Tennessee while I was county executive, I can tell you that from a cyber and IT/OT perspective, we were arguably vulnerable. Please expand on that vulnerability. When you look at bad actors as it relates to kind of, you know, just our infrastructure security and what the consequences might be if there was a coordinated systematic attack against those local communities.

Ms. BOLTON. So a lot of what we see, and you're completely right, a lot of what we see is that the threat actors are targeting the most vulnerable organizations, right? Many times those are smaller organizations without cybersecurity expertise. They're at the county level, they're at the local level. You see actors either targeting those for, you know, for target practice, learning, and then moving to bigger systems, or they're doing it in a coordinated manner across a number of different States and localities. Particularly we see that in the energy sector, and they're using that as a means to prepare the battlefield, if you will, for if they're—in a contingency.

If it's China, for example, if they're sitting on our networks, that is extremely dangerous. Even if they're not conducting any particular operations right now, No. 1, we can't guarantee that they're off the networks. Even when we find them, we find them too late. We find them 3 years after the fact. What we don't want to have happen, if, for example, we're planning for a 2027 contingency, then we need to start doing the work now to build resiliency, defense-in-depth, the ability for those smaller local and county entities to be able to secure their—to secure all of those ports, right? Secure the remote access, put in stronger multifactor authentication, modernize their legacy IT. That's why I think it's so important to reauthorize the State and Local Cyber Grant Program, because without those resources, like I said, most of those localities are using the funding for physical security and not OT.

Mr. OGLES. Mr. Chairman, you know, again, coming from that local governance background, county executive, and I will speak for Tennessee, obviously everybody knows Nashville and knows Mem-

phis, larger cities with more arguably or hopefully more robust systems. But a lot of Tennessee is rural, just like a lot of States across the country. What you see are electric cooperatives. So just like the county may be vulnerable to that infrastructure attack, my guess is in most cases, so are those local cooperatives, so is some of the water cooperatives as well.

So as we look forward to, again, the next battlefield and what keeps me up at night, and, quite frankly, Mr. Chairman, what I would argue, the most important, some of the most important work that we'll do on this committee, this whole committee, is what we are doing in cyber as we prepare this country for that next battle. It is going to be on our computers, it is going to be across our networks, and I would argue it is going to be in our local rural communities that they are going to hit first because then they can Swiss cheese our electrical grids and our water systems and our water treatment plants, et cetera. That is what keeps me up at night.

So with that, I would love to stay on this topic and just kind-of go down the line. We will start with you, Ms. Zetter, to see what you might want to add to this subject matter, please.

Ms. ZETTER. I think you're absolutely right in terms of the small utilities and cooperatives like that. They don't have the money, they don't have the resources, they don't have the expertise on staff. They don't even hire security people. But I want to also say that, you know, we sort-of anticipate that the large organizations would be more secure. If you look at what happened to Colonial Pipeline in 2021, we see that this was really a major organization, critical infrastructure, supplying a lot of gasoline to the East Coast. Yet Colonial Pipeline, at the time that it was attacked, did not have a CISO on staff. They also had a legacy system that the attackers got in an old VPN account they were no longer using, but hadn't bothered to disable. They came in through a password that potentially was—well, it was leaked on the internet. So the employee who had the password had used it for other accounts, and then it was leaked on the internet and other breaches.

One other point about that was the attackers, we think, only got to the IT network, didn't actually make it to the OT network. But Colonial Pipeline shut down the pipeline because they feared that the attackers would get to the OT network and then encrypt it and lock it. But when the CEO of Colonial Pipeline testified to Congress, he testified that they had very secure, highly segmented OT and IT networks. But if they were that confident that the networks were segmented, then they wouldn't have had to shut down the pipeline as a precaution.

So I just want to say that, yes, those smaller entities are a big issue and a prime concern, but also the larger entities are having the same problems and not keeping up.

Mr. OGLES. Yes. Thank you, ma'am.

I apologize, Mr. Chairman, I am over time, but I yield back.

Mr. GARBARINO. Not a problem. The gentleman yields back.

I now recognize myself for 5 minutes of questions.

We all know CISA plays an important role, sector risk management agency for 8 of the 16 critical infrastructure sectors, as well as the national coordinator of the sector risk management agencies.

They do a lot of work. I would like to hear from you all. What do you think—how would you assess CISA's effectiveness is as a partner when it comes to OT cybersecurity? We can start with Ms. Zetter if you want.

Ms. ZETTER. I don't have direct, because I'm not a practitioner, so I don't have that assessment to know first-hand. But what I do know is that CISA in the past had, I would say in the last decade, really, a lot of expertise that they were able to give to critical infrastructure, either to go out into the field and do critical assessments of the networks, give them risk assessments about what they needed to do, and then also they had flyaway teams that when a system was compromised, that they would be able to go out and assist directly in doing some kind of remediation. So I think that the impact of CISA has been really great. But, of course, they're limited in their resources and who they can operate—who they can give assistance to.

Mr. LEE. I would say that my commentary about CISA probably is reflective of a number of Government agencies that deal in this space, which is really good Americans trying really hard to do good work that have very talented people, but are hardly being effective for the amount of money we're spending on it in comparison to what's happening elsewhere. As an example, flyaway teams, the incident response teams, et cetera, there's absolutely nothing unique happening there in comparison already in the private sector. I think there's a very important role and responsibility for Government to play, and I think a focused CISA would be extremely impactful. You know, in passing, talked to Shawn Plankey, I'm really excited about the way they're looking at it now, but I think a lot of times we overstate the effectiveness.

I'm sure that this is not going to earn me any friends at CISA, and many of my friends are there, but I will say that we've got a couple of years before we have significant issues and I'm very concerned about the next couple of years going to war with China and it being focused on our OT. I would really like to move past pleasantries, so we should focus them a heck of a lot more.

Mr. GARBARINO. Thank you.

Ms. BOLTON. I would say that I think CISA, you know, can certainly grow in its effectiveness and I think we will see that under Sean Plankey. I think things like automated information sharing, the Einstein program, CyberSentry, I think there's a number of places there where we can modernize some of that legacy infrastructure. They're operating not necessarily with the most updated sensors. I understand that it is expensive to upgrade the systems. But if we want CISA to be acting as the, you know, the front-line defense for cybersecurity and as an expert, they need to have, you know, up-to-date systems. They need to have sensors on the networks that are what is modern right now. But I think that'll—that's about it.

Mr. GARBARINO. Dr. Gleason.

Mr. GLEASON. I would say some of our best and most effective work with CISA has been when they've worked in partnership with some of the other Federal departments with stake in the space, in particular with the Department of Energy looking at threats to the

energy sector and the Department of Defense looking at defense critical infrastructure.

Just to echo on some earlier comments, I think CISA also works best when they do work that is appropriate to the Government to do and not trying to do what the private sector is already taking care of. The Government has specific advantages in our access to the intelligence community and the ability to do things that the private sector is not or shouldn't be doing. I think the more that the Government sticks to that space, the more effective that that those programs will be.

I also want to echo, I definitely look forward to Sean Plankey coming in and very excited about Nick Anderson coming in. We've had great experiences working with him previously and think their leadership will be very effective.

Mr. GARBARINO. I think we can all agree that we are very excited to see Sean Plankey get confirmed as soon as possible. It will be a good day for, I think, for CISA to have him in there.

Mr. Lee, I want to go back to this. Because you were very passionate in your answer to that and you really want to get them focused. Can you go a little more in depth? Because this is, like, this is the stuff we are going to have to work on.

Mr. LEE. SANS Institute, which is the leading cybersecurity provider, analyzed every single industrial cyber attack that's happening ever taken place and just asked the basic question of what security controls actually worked. It was 5, and we know exactly what those 5 are, we know exactly how to do it. If you look at regulations, standards and everything else, it's not 5.

Further, when you look at our rural communities, as mentioned, about 98 percent of this country is in that sort-of below the cyber poverty line discussion. They're not doing pretty much anything unless it's really passionate members there trying to help. But going back to what Kim said as well, you've got a large number of companies that will stand up and say how robust their security programs are, and I'm in a lot of those environments and they're terrifying.

So I have 3 kids. I did not really want to go back in the Army for, you know, extra time. It was I really want to get this right. I think if we're going to be serious about the conversation, it's focus on what we can actually do across the next couple of years. Pick a point of view. You're going to upset some people in doing so, but we need to do it. At the same time, I would say you can roll out quickly.

I think about 95 percent, anecdotally, about 95 percent of all cyber spend goes to enterprise IT, about 5 percent to OT. That is where your national security is, your environments, your local communities, and all of your ability to generate revenue. You look at sort-of the visibility in this country. If you actually want to monitor your OT infrastructure, figure out is China already there, I would say probably about 10 percent of the infrastructure around the country is being monitored. So when we're having big discussions about what comes next, I would just highlight that we're not even really being serious about what we know today.

Mr. GARBARINO. I appreciate that. Thank you very much.

We are going to start our second round of questions.

So I recognize, second round, the gentleman from Florida, Mr. Gimenez, for 5 minutes.

Mr. GIMENEZ. Thank you, Mr. Chairman. I am going to pivot a little bit. So do you all know what MAD is? Mutually assured destruction. MAD is not really all that MAD. MAD kept us safe for about, you know, 50 years, 60 years. Right. Where, yes, the Soviet Union had thousands of nuclear weapons, but so did we. If they ever used it, then we would use it on them. That kept us safe in a frightening kind of way, but it did. It kept us safe. All right.

So my question to you is, there is the Department of Defense, but part of the Department of Defense is the Department of Offense. So if we were just a—well, we are here to defend the homeland and we are going to play defense, well, you are inviting attacks because there is no counterpunch. What is our offensive capability? Where is your assessment of our offensive capability in this realm?

Mr. LEE. I'll take first pass that we are very, very good at our offensive capability. I think some concerns I have, you have to be able to get to root cause analysis on determining if we were attacked for us to go back and do something. I'm aware of numerous cases the Government is currently tracking as maintenance issues for explosions otherwise, that were actually cyber attacks. If we're not detecting what's happening, then we're just going to say, oh, it must have been something random, and we're never going to get offensive. But putting my military hat on now, even just down the 91st Brigade alone, we've got a lot of offensive capability and I would not want to be on the other side of us. But we also have to make it extremely hard for our competition to come back at us and at least know when they do it so that we can unleash our warriors.

Mr. GIMENEZ. Do we do that often enough? Do we flex our muscle often enough?

Mr. LEE. I think just looking back to testimony and commentary from Joe Nakasone, General Haugh, and others, I would say that we do not. I do not want to see an offensive world. I do not want to see targeting civilian infrastructure. But when our adversaries make it very clear that they want to hurt us and hurt our families, I think we have to be very serious about showing them that we can do the same.

Mr. GIMENEZ. I agree. So, I mean, if we actually flexed our muscle every once in a while, I mean, the DOD flexes its muscle every once in a while, right? So I guess you are saying we don't flex our muscle often.

Mr. LEE. I'm saying we don't flex it enough. But I would also advise that we had to be very serious on defense because we will see things back. Even if one agency in a Government authorizes something at us and we are doing something that we view to be retaliatory, other agencies in that same Government may not be aware of it unless we're able to call it out. Then all of a sudden you have a very escalatory situation.

Mr. GIMENEZ. You know, we have a new realm of warfare. I guess defense and offense is space. So we created the Space Force. Right? Should we create a Cyber Force?

Mr. LEE. I'll stick with it and then open up to the panelists. I think it's time. I was very against it when I was in the Air Force. I was very against it for the years after looking at how it was going

to be orchestrated. I think it's time to do it, sticking to its OT&E mission of organizing, training, and equipping. Let Cyber Command and the Combatant Commands be the actual Title 10 authorities that we have. But we definitely need a dedicated service.

But I think if you're going to do it right, you have to do it extremely big and right because the problem that you'll have is all that infighting and the stuff that people say, oh, we politely work together in interagency. No, we don't. People are very territorial and people will keep their best cyber warriors to themselves.

Mr. GIMENEZ. So you are going back to my first round of questioning, right?

Mr. LEE. Yes.

Mr. GIMENEZ. That there is turf guarding.

Mr. LEE. There's a lot of turf guarding.

Mr. GIMENEZ. Or there is a lot of turf guarding. So I would figure that now with Space Force and the Air Force, there is probably a lot of turf guarding there. Right?

Mr. LEE. I don't see it as much myself, but I did leave the Air Force a while ago. I will say the Army would be very happy to have a Cyber Force under it from a department level, but I'm not so sure that it shouldn't just be made a department-level service.

Mr. GIMENEZ. OK, fair enough.

OK. That is all the questions I have, and I yield back the rest of my time. Thank you.

Mr. GARBARINO. The gentlemen yields back.

I now recognize the gentleman from Texas, Mr. Luttrell, for 5 minutes of questions.

Mr. LUTTRELL. Good to hear you say—I have been working on that Cyber Force idea for a while, and General Haugh and I had some pretty interesting conversations behind closed doors. Absolutely a brilliant guy in his stance, but I think he was trying to protect the nest. But I think we are far enough along where a cyber force should be—absolutely, the conversation should be had.

To the conversations that you were having with the Chairman and you listed 5 things. I come from a very rural district and I have had CISA out to the district to talk to our business owners, but where is the piece of paper at? What can I hand off to everybody that is in my district and to my State and say, here, implementation of these 5 things will get you to a better place?

Of course, as you said, everybody is going to beat it up, because they are not going to be the ones that are involved in it or whatever. But, I mean, from our nursing homes to our banks to our school districts, they have all been hit. We have those—again, you heard me say it in my last line of question. Very reactionary because we don't know what we don't know. Where does that live? Hand it to me. I mean, help me out here.

Mr. LEE. Yes, sir. Yes. The SANS Institute published the 5 critical controls. It's been backed by other governments as well.

Mr. LUTTRELL. The what did?

Mr. LEE. The SANS, S-A-N-S, Institute.

Mr. LUTTRELL. Where does that live? Because if I walked into Conroe, Texas, and said, hey, go visit this place, they're going to look, I mean, they are looking at me like I am crazy.

Mr. LEE. Yes.

Mr. LUTTRELL. The legislation all the way up needs to be talking about it. I mean, I like to say we need to Facebook this thing so everybody and their cousin knows about it.

Mr. LEE. Yes, sir. Yes, I would love to see again Government have a single voice to say, here's actually what's working. As a rural guy from Alabama who joined the military, if I can figure it out, I promise everyone in your district can as well. But we need to speak again with one voice of Government. If CISA had a single page of here's the resources available to you, this is what you can do, and every agency around supported it instead of their own thing, I think you'd see a lot more outcomes.

Mr. LUTTRELL. If we do do that, will the bad actors globally pinpoint those specific IT, OT, and go after it, and then we are just dead in the water?

Mr. LEE. No, I don't think it would work in that such way. Even if you advertise broadly what your strategy for security is, it's the fact that your actually doing and implementing it that makes you defended. The fact that your adversary knows you want to invest in secure monitoring or secure mode access or monitoring, that doesn't make you any less secure.

Mr. LUTTRELL. Well, they will most likely look somewhere else.

Mr. LEE. I hope so. Right now it is way too easy to target our systems, and right now we are doing very little. I would love to raise the bar where they actually have to come up with something creative.

Mr. LUTTRELL. Raise it. I mean, you are sitting in front of the group that is sitting here, hey, we are asking you. I won't speak for my colleagues, but, hey, I am asking you right now, on record, do it. Bring it to us right now.

Mr. LEE. Yes, sir. Provide some written testimony, I'm happy to brief you at any time. I am trying my best.

Mr. LUTTRELL. I will absolutely see you after class, sir.

With that, Mr. Chairman, I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the gentlelady from New Jersey, Mrs. McIver, for 5 minutes of questions.

Mrs. MCIVER. Thank you so much, Chairman. Thank you to our Ranking Member.

My district sits at the heart of our Nation's largest metropolitan area and is home to a major airport, one of our Nation's busiest ports, numerous railroads, and pipelines, and key industrial facilities, among other critical infrastructure. Securing these facilities requires resources and for publicly-owned critical infrastructure those resources have often been lacking. As part of the Infrastructure Investment and Jobs Act, Congress provided 1 billion to establish the State and local cybersecurity grant program. State and local governments can use this funding to strengthen the OT security of publicly-owned critical infrastructure. Unfortunately, under current law, the program is set to inspire to expire in just over 2 months.

Ms. Bolton, I have a question for you. How important is it to continue funding for the State and Local Cybersecurity Grant Program?

Ms. BOLTON. I think it's critical to continue that funding. I mentioned in my testimony that most—a third of districts around the country are rural districts. Obviously that's not the case for your district, but I think it's still incredibly important. There are not only large ports and airports in your district, but also smaller entities, and those are the ones that really desperately need help.

I will add to your question earlier as well that CISA has released a top 5 OT cybersecurity guide. So I think that also can help to provide guidance to those entities as to what they can use their cybersecurity spend on. At OTCC we're also working on guidance as well.

Mrs. MCIVER. Thank you. Can you just elaborate a little bit more on how should State and local governments prioritize their resources to strengthen their OT security?

Ms. BOLTON. So I think it's very important to start at the very beginning. We do know some of the controls that work and so we should put those in place. Multifactor authentication, segmenting, even micro-segmentation of networks, making sure that we are securing remote access.

Also I'd add that, you know, most of the attacks that are happening on our critical infrastructure aren't zero days. They're not the most sophisticated vulnerability or the most sophisticated attacks. They are using things that we've seen before, sometimes not changed at all, sometimes mildly changed. We continue to be hit by these attacks.

I think, for example, CISA releases a top 12 cyber vulnerabilities—top 12 routinely exploited vulnerabilities list. Why would the Government or any State entity still be able to buy those products off of that list? If one side of the Government is saying these are commonly and routinely exploited, we should never be allowed to buy those. So things like that I think are extremely important.

Mrs. MCIVER. Thank you so much. I want to thank the witnesses for being here today for providing testimony, and I really do appreciate the Chairman and the Ranking Member's, you know, steadfast focus on this issue and also being supporters of the reauthorizing of the State and Local Cybersecurity Grant Program. So I look forward to continuing to work with both of you in this committee to provide State and local governments the resources they so desperately need to secure their critical infrastructure.

With that, I yield back.

Mr. LUTTRELL. Will the gentlewoman yield? Can I borrow your minute?

Mrs. MCIVER. Sure.

Mr. LUTTRELL. This is piggybacking off one of the questions you asked. You said CISA listed 5 things as well. Is it the exact same list as what you are saying?

Ms. BOLTON. No, it is not. This is another issue that we have.

Mr. LUTTRELL. OK. So there's a problem. I have now taking 2 lists——

Ms. BOLTON. Yep.

Mr. LUTTRELL [continuing]. And saying here you go. Then that is an issue.

Ms. BOLTON. Absolutely.

Mr. LUTTRELL. On top of those 2 and the 10,000, 100 million that everybody else brings to you. For a poor district like ours, like, I mean, yes, here we go.

Ms. BOLTON. Yes.

Mr. LUTTRELL. Thank you very much.

Ms. BOLTON. Well, and I will say this. The cybersecurity industry as a whole is, is aligned on things like implementing multifactor authentication, network segmentation, continuous monitoring and detection. But there are sort-of these conflicting guidances that do exist. Same with frameworks, conflicting frameworks for OT. So the people in your district or the operators in your district that are trying to just do the right thing, they don't know where to start.

Mr. LUTTRELL. Correct.

Ms. BOLTON. Especially when it's like NIST Cybersecurity Framework 2.0, there's like 80 pages. Right? People who are running these OT networks don't have the knowledge to read through an 80-page document and know where to start. So one of the things is like NIST is creating some quick start guides. I think that would be very important to do for OT security.

Mr. LUTTRELL. Thank you. I yield back. Thank you, ma'am.

Mr. GARBARINO. The gentlelady yields.

Thank you very much for your enthusiasm about State and local, the grant program. I hope it is something that we can get reauthorized right away. I think it could be a very big bipartisan issue.

I now recognize the gentleman from Tennessee, Mr. Ogles, for his second 5 minutes of questions.

Mr. OGLES. Thank you, Mr. Chairman.

Mr. Lee, I think you said 98 percent of communities were below the cyber poverty line?

Mr. LEE. Yes, Congressman, about—if you look at companies under about 100 million in revenue across all of our electric and water utilities, that's about 95 to 98 percent of them.

Mr. OGLES. Goodness gracious. So I want to go back and just double down on this issue. Again, coming from the county executive level and, you know, to my good friend to my left here, you know, his district as well, I am sure he is seeing the same thing, is that, you know, your IT director is also the guy that is setting up emails and plugging in keyboards and probably spends 60, 80 percent of his time not in his office, not at his desk, not being offensive because a good defense is a good offense, you know, looking for those weaknesses, looking for those back doors, looking for those left-around passwords, and such. So, and I will use the word "framework" in the context of more like a toolbox.

You know, I want to be careful here because, you know, borrowing from Reagan, you know, he said the scariest phrase in the English language is "I'm from the Government and I'm here to help." What we don't want to do is create a monster that suddenly is nothing more than a big bureaucracy that is designed to grow and gobble up resources. But what I do see here, again, coming from that local background, is there is a vacuum here, there is a void. Quite frankly, our communities don't have the expertise. Even if they do have the expertise, I am not sure they have the bandwidth, bandwidth in the context of man or woman hours.

So we have got to figure out how we move forward and how we, quite frankly, equip some of our local communities. Because, again, if I am on the other side of the pond and I am seeing the opportunity that most moment to seize, I am going after the locals, I am going after those water systems and, you know, talk about creating pandemonium. Suddenly your small rural cooperative electric or water system goes down and it is not working and it is not coming back on-line for a few weeks. That has been Swiss cheese across the country. That is what, again, I go back having been the county executive, that is what keeps me up at night.

Mr. Chairman, I think my challenge to the committee is that is something that we need to work on, being careful not to create, again, a monster that grows and grows and feeds at the trough, that Government trough.

Then back to the whole idea of creating a department-level service with cyber force, I think that is incredibly, incredibly important. Because cyber is not just across the networks, it touches into the drones and the capability of jamming and all sorts of things. So those capabilities have to become—we have to lead on that frontier and, quite frankly, become untouchable in the same way we are untouchable in air space and communications.

With that, Mr. Chairman, I yield back.

Mr. GARBARINO. The gentleman yields back.

I now recognize the Ranking Member, the gentleman from California, Mr. Swalwell, for his second 5 minutes of questions.

Mr. SWALWELL. Dr. Gleason, what is the status of Lawrence Livermore's other partnerships, including its support for the National Infrastructure Simulation and Analysis Center?

Mr. GLEASON. Those are in a similar status to our support for CyberSentry. Our work for National Risk Management Center, again, looking at infrastructure interdependencies and cascading consequences of disruption to infrastructure, has been going on for a decade. Our interagency agreement expired in March for that work.

Mr. SWALWELL. What is the risk to what you are able to see or what you were able to see and what you don't see now as far as cyber vulnerabilities that are out there?

Mr. GLEASON. I think one of the big things that we miss, and I want to emphasize the idea of cascading consequences. A lot of times when we're thinking about cyber attacks on critical infrastructure, the target may not be that infrastructure system itself. It may be what is supported by that infrastructure system. When we fail to understand those interdependencies, we are opening up avenues for our adversaries to disrupt key national security capabilities.

A great example of this is some of the capabilities on the territory of Guam. This is a small, very hard-working, very dedicated power company, but very under-resourced. Some of our most important capabilities for defending against a potential China invasion scenario are based in Guam. There are ways to defeat those capabilities that go through, for lack of a better word, the back door, by exploiting kind-of the weak underbelly, the under-defended part of our critical infrastructure because those are very small systems. By not understanding those interdependencies, it's not that they

don't exist. Our adversaries know them. If we don't, we're not looking in the right place for our defense.

Mr. SWALWELL. In just over 2 months, the—I am sorry, did someone else—you are good. In just over 2 months, the Cybersecurity Information Sharing Act of 2015, the other CISA, is set to expire and Mr. Gimenez alluded to this. It is essential that we act promptly to reauthorize it in a clean way. I am open to any reforms that we could discuss down the road under the Chairman's leadership of the full committee. But I think there is a wide consensus that we don't have time to do that now. Congress will be in recess, effective this week until after Labor Day, and then we will be right up against CISA's expiration.

Ms. Bolton, your testimony discusses the importance of reauthorizing CISA 2015. What would be the national security impact if the law lapses?

Ms. BOLTON. The estimates are that about 80 to 90 percent of information sharing would be cut off from the Federal Government. When I was at the Cyberspace Solarium Commission, one of the main things that we tried to do was to make sure that the Federal Government at least had a full threat picture. This authority is part of that work, a significant part of that work. We must reauthorize it.

If we are about 2 years away from a contingency with China in 2027, as ODNI has said, then we have to be fully prepared. We have to be taking steps now and not just addressing, you know, the information-sharing piece. That should be a baseline, it should be a given, and we should be focused on the additional steps that we need to take.

So I hope that that gets reauthorized quickly and that we can move on to some of these other topics that we've been discussing and addressing some of the other extremely serious issues, because China is not waiting. China is preparing now and so are all our other adversaries.

Mr. SWALWELL. Mr. Lee, your experience in the private sector, is there any world where CISA 2015 lapses and a private-sector company that has been hit would still be willing to come forward and share information with the Department of Homeland Security?

Mr. LEE. No, I think it's incredibly important to reauthorize it. The bidirectional communication from Government to private sector, especially on the threat picture overall, is exactly one of the roles and responsibilities that makes a lot of sense.

Mr. SWALWELL. Then that's because no CISO would be able to go to the DHS without liability protection and their fiduciary duty to the shareholders. I mean, they would be exposing themselves to a lot of risk. Is that right?

Mr. LEE. Absolutely. That's actually a broader issue. Even looking from a National Guard perspective of could we go in and respond if a utility gets hit, we have no indemnification to give utilities. So they're not going to let us touch anything and do any action on it. There are very simple bureaucratic things that could be fixed to increase national security tomorrow.

Mr. SWALWELL. Thank you. Yield back.

Mr. GARBARINO. The gentleman yields back.

I can't agree with him and the witnesses more and my other colleagues that we have to reauthorize. We do have to change the name, though.

Mr. SWALWELL. Yes.

Mr. GARBARINO. OK. That has got to be at least one change we have to do. You know, I understand people want to do clean and we have to get it done, but I do want to hear from you all because I think there should be changes. There should be—it is a 10-year-old law and, you know, clean reauth it doesn't include things that we have learned over the last 10 years.

So I would like to hear from you all, is there language or are there changes or focuses that we should implement into the law that we should consider to ensure OT is better protected or covered?

Ms. BOLTON. Well, I would just add that, and I think you all are already considering this, but including OT much more directly within the language. It's currently not in the bill or not in the legislation.

I would also say that identifying DHS and CISA as the main sort-of gateway for sharing would be ideal because, as we've spoken before, the confusion for industry of coming into and talking with the Federal Government, sharing information with the Federal Government, that remains a problem. We hear that all the time from our member companies and from other companies that I work with that they don't know where to go. They say, well I need to talk to—maybe I should talk to TSA, maybe I need to talk to FBI, and then maybe FBI will tell CISA. That can't be assumed. So we need to make sure that that language is clear within the legislation.

Mr. LEE. Yes, I would completely agree with that. Also there needs to be, here's what you get in return. Here is what we can do to help you because you gave us this information. A lot of times a lot of asset owners and operators feel that it's a one-way communication in the Government with no expectation of what comes out of it. You want somebody to go through the risk of sharing information? There's got to be a very clear and here's the rules of the road of what we can provide for you as a result, cross agency, without any drama.

We talked about turf wars. I led the OT portion of the incident response for Colonial Pipeline. I witnessed a lot of turf wars between FBI and CISA. It needs to be very clean or no asset owner-operator will want to work with them. They view them as children.

Mr. GARBARINO. Yes, I've heard from a bunch of—it is very important this was a major part of my, by the way, my presentation to become Chair of the full committee was making sure that this does not lapse. So it is a top priority for me and as I know, for the other Members on the committee. I have spoken to many people in the private sector that said it would be devastating and they would not be able to talk to the Government if this expires, and it would be devastating for us.

I do want to get back to the Stuxnet, and, you know, we are very privileged to have Ms. Zetter here to talk about it. So I want to get it back into what is the significance of Stuxnet today and what les-

sons did we learn? What lessons should we have learned that we have not learned yet from it?

Ms. ZETTER. I mean, the primary lesson is the focus on OT systems that Stuxnet showed the danger that weapons like this can have against critical infrastructure and, of course, not just doing what a normal virus does, but causing destruction. I think, also, the—basically the small utilities and the small organizations, I just want to emphasize that because it's been brought up a lot.

I talked about when you asked me how effective CISA has been, and I said that they've been effective in terms of providing these small organizations with a service that they can't otherwise get. The panelists had said that the CISA shouldn't be doing what local—or what private industry can be doing. The problem is that those small utilities and small organizations don't have the funds, or haven't had the funds, in many cases to actually get it privately. So they have relied on CISA for that kind of service. I think that when we have legislation, of course, that has that ability to provide the funds, that's really significant for those organizations, and that shouldn't go away.

So I think that the overall lesson from Stuxnet is that the capabilities out there are really sophisticated, really advanced, and we haven't seen the full use of the capabilities that Stuxnet showed, for various reasons. Probably deterrence is one of the good ones, at least from the U.S. perspective, that adversaries are, you know, having second thoughts about targeting U.S. infrastructure. But, also, I sort-of make a distinction between those who have the will and those who have the ability. Those who have the ability haven't until now really had the will to go after U.S. critical infrastructure. Those who have had the will, perhaps maybe terrorist groups, others, haven't necessarily had the ability. It doesn't take much to marry those two together. Even someone that has will and doesn't have ability can purchase that ability, can purchase that capability.

Now we're entering into a phase where even we've relied on the large nation-states, China and Russia, we've relied on them not having the will to target U.S. infrastructure. I think what we're talking about and going into potential conflict with China, we've reduced—we've eliminated that gate now, and they do have the will potentially to go after U.S. infrastructure. So I think that that's the lesson learned from Stuxnet.

Mr. GARBARINO. That is a scary way to end this committee hearing, but I appreciate it, and that is a big concern for me, is when the people with the will and the ability are the same person. Because that is a scary thought, and that is what we have to be prepared for.

I want to thank all the witnesses and all the Members. I mean, the fact that so many people stuck around for second round of questions just shows you how important this topic is. So I want to thank you all for your valuable testimony, the Members for their questions.

The Members of the committee may have additional questions for the witnesses, and we ask that you all respond to those in writing. Pursuant to committee rule VII(E), the hearing record will be held open for 10 days.

Without objection, this committee stands adjourned.
[Whereupon, at 11:23 a.m., the subcommittee was adjourned.]

APPENDIX I

STATEMENT OF IAN JEFFERIES, PRESIDENT AND CHIEF EXECUTIVE OFFICER, ASSOCIATION OF AMERICAN RAILROADS

JULY 22, 2025

INTRODUCTION

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to submit this statement for the record regarding the rail industry's work to address cybersecurity threats, including our on-going collaboration with the Government. AAR's freight railroad members include the 6 Class I railroads, as well as scores of U.S. short line and regional railroads. Together, they account for the vast majority of freight railroad mileage, employees, and traffic in the United States.

Freight railroads integrate skilled personnel and ingenuity with technology to keep the network infrastructure safe and the supply chain moving every day. Advanced information and communications technologies are helping our employees across all aspects of operations, including train control, track and equipment inspections, emergency response, dispatching, railcar tracking, locomotive fuel management, predictive performance analysis, employee training, and more. Cybersecurity is an on-going arms race between attackers and defenders, which is why our highly-skilled, highly-trained employees work diligently to continually strengthen their capabilities and guard against cyber attacks that threaten the safety and integrity of rail operations. Railroads continually evaluate and enhance cybersecurity through recurring exercises and frequent consultations with Government and private-sector security experts. These efforts ensure maximum sustained effectiveness, supported by a strong working relationship with the Federal Government.

For more than 25 years, railroads have maintained a dedicated coordinating committee focused on cyber threats, effective risk mitigation practices, and engagement with appropriate Government entities. Railroads leverage a strong mix of public and private capabilities to help effectively prevent and respond to malicious cyber activity. As threats continue to evolve, our industry strives to remain agile and innovative to address the dynamic cyber threat landscape.

A UNIFIED COMMITMENT TO OVERALL SECURITY PREPAREDNESS

The rail industry addresses cybersecurity head-on through a long-standing, industry-wide, risk-based, and intelligence-driven plan. Railroads' specialized and highly-skilled cybersecurity teams carry out comprehensive, multifaceted cybersecurity plans focused on the factors experts have identified as the most effective in preventing cyber attacks.

Two AAR committees lead the industry's cybersecurity preparedness. First, the Rail Information Security Committee (RISC) is comprised of the chief information security officers and cybersecurity leads from major North American railroads. These committee members coordinate cybersecurity efforts, share information on threats, and discuss effective protective measures and risk-mitigating actions. Initially, the RISC included only Class I railroads and Amtrak, but membership has since expanded to include representatives from short-line and commuter railroads, as well as Railinc—a wholly-owned subsidiary of AAR that provides essential information technology support to enhance safety, efficiency, and smarter operations across the rail network. Second, the Rail Security Working Committee includes senior law enforcement and security officials focused on countering domestic and international terrorism. Together, these committees form the Rail Sector Coordinating Council (RSCC), the rail industry's primary channel for communication and coordination with Government agencies on cybersecurity initiatives.

The importance of the industry's cybersecurity posture and its collaboration with Government agencies can be highlighted through the recent publication of an advisory last week regarding a vulnerability in end-of-train devices from the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

RAILROAD RESPONSE TO END OF DEVICE VULNERABILITY

The Federal Railroad Administration requires that all freight trains operating in excess of 30 miles per hour be equipped with End-of-Train (EoT) and Head-of-Train devices, while AAR updates and maintains the device standards. EoT devices collect brake line pressure data and send the information via radio signal to a head-end device aboard the locomotive, allowing the engineer to monitor the braking system. EoT devices also relay data about whether the rear end of a train is stopped or moving forward or backward and allow simultaneous brake application from both ends of the train in emergencies.

Recently, two independent researchers shared with CISA a vulnerability in EoT devices that could potentially allow an attacker to disrupt communications between the EoT and the head-end device and thereby stop the train. CISA's acting executive assistant director for cybersecurity, Chris Butera, stated:

"The End-of-Train (EOT) and Head-of-Train (HOT) vulnerability has been understood and monitored by rail sector stakeholders for over a decade. To exploit this issue, a threat actor would require physical access to rail lines, deep protocol knowledge, and specialized equipment, which limits the feasibility of widespread exploitation—particularly without a large, distributed presence in the U.S.

"While the vulnerability remains technically significant, CISA has been working with industry partners to drive mitigation strategies. Fixing this issue requires changes to a standards-enforced protocol, and that work is currently under way. CISA continues to encourage manufacturers to adopt Secure by Design principles to reduce the attack surface and ensure resilient communications systems for operators."

While there is no evidence that the vulnerability has ever been exploited, the rail industry takes all cybersecurity threats very seriously and is working with the original equipment manufacturers to develop solutions compatible with all current-generation systems. Moreover, the industry has also been working on updates to develop the next generation of EoT technology for several years. These next generation EoT devices have the potential to significantly improve communication between lead locomotives and the end of the train, enhance reliability and security, and streamline operations.

The rail industry recognizes and remains supportive of the good work that CISA provides. The industry will continue to build and maintain our partnerships with DHS, the Transportation Security Administration, and the Federal Railroad Administration through joint efforts such as Project CHARIOT—an initiative focused on identifying vulnerabilities and developing robust mitigation strategies to reduce cyber risks. This collaboration will lead to the evaluation of a wide array of technologies and equipment and the ultimate hardening of critical infrastructure, ensuring the safe delivery of freight for customers across the network.

REAUTHORIZING THE CYBERSECURITY INFORMATION SHARING ACT OF 2015

In addition to the rail industry's on-going efforts in cybersecurity preparedness, the Cybersecurity Information Sharing Act of 2015 (CISA 2015) provides legal safeguards that have enabled the private sector and the Federal Government in combating cybersecurity threats. Private entities need the antitrust exemptions and civil liability protections, disclosure law exemptions, and regulatory use exemptions in CISA 2015 to enable and sustain the unencumbered flow of cybersecurity information between reporting entities and the Federal Government. However, CISA 2015 is set to expire this year—unless Congress acts quickly to extend its protections.

Including the protections of CISA 2015 in all future cybersecurity legislation will build upon the successful legacy and partnerships that CISA 2015 helped to establish. Under CISA 2015, when a private organization shares information about a cybersecurity threat with DHS, that information is analyzed to identify possible threat actors and the threat actor's tactics, techniques, and procedures. Currently, the Government is obligated to protect the private organization's sensitive information. Losing these privacy protections would greatly disincentivize companies from coming forward. If private organizations stop sharing information on the details of cyber attacks with the Government, those private entities fighting cybersecurity threats

would lose visibility on shifting tactics of malicious actors, thereby increasing the threats of bad actors for companies across the United States.

However, the law has been underutilized because the information permitted to be shared is too narrow. Under CISA 2015, a private company receives liability protections only if it shares through DHS's Automated Indicator Sharing system. These protections must expressly extend to sharing with other U.S. departments and agencies, such as the FBI and Secret Service, which are positioned to help private organizations improve their cybersecurity. Additionally, CISA 2015 permits information sharing where there is a "cybersecurity purpose," which is narrowly defined as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability." This definition should be expanded to encompass other systems beyond an "information system." Expanding the scope of CISA 2015 will allow the private sector to share more information, leading to an even greater ability for collaboration than what is currently realistic under current law. More collaboration between the Government and the private sector will allow for both to be better prepared against cybersecurity threats.

CONCLUSION

Railroad operations are resilient thanks to years of proactive and extensive efforts by highly-skilled railroad employees to develop, implement, and continuously improve plans, practices, and measures for cybersecurity as threats and security concerns emerge. However, risks are constantly evolving, and real-time adaptation is essential to reduce risk. Fortunately, the railroad industry and the Government share a common purpose: ensuring that effective and sustainable measures are in place and regularly reviewed for continuous improvement, in order to mitigate risk in the face of ever-evolving cyber threats. Railroads and their employees will continue to work cooperatively with private and public entities to ensure that our Nation's rail network—and the people, firms, and communities we serve remain safe, efficient, and secure.

APPENDIX II

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR KIM ZETTER

Question 1. Since Stuxnet's creation, how have you seen cyber attacks against critical infrastructure evolve, especially during heightened conflicts?

Answer. Following the discovery of Stuxnet, everyone expected that we would see similar copycat attacks against critical infrastructure, but we've seen surprisingly few operations that target critical infrastructure at this level. There have been ransomware operations against critical infrastructure, of course—the 2021 attacks against Colonial Pipeline and JBS Foods being 2 of the most famous ones. But in terms of cyber physical attacks that had a destructive or damaging intent that rise to the level of Stuxnet, we've had very few examples. The most significant are the 2015 and 2016 Russian attacks on Ukraine's energy infrastructure, and the 2017 attack against a petro-chemical plant in Saudi Arabia, both of which I discuss in my written witness testimony. For quick reference, here is what I wrote previously:

"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."

These three attacks are noteworthy for the way they showed an advancement in techniques and skill from Russia. The 2015 attack on Ukraine's power grid was a time-and-resource-heavy manual attack that was customized to target 3 different energy distribution companies, each of which used different models of control systems and had different configurations that the attackers had to study. It also required the operators to conduct the attack in real time with their hands on keyboards. The 2016 attack, however, had automation capabilities, which made it more dangerous. And the Triton attack showed that attackers were upping their game in terms of potential consequences.

The subsequent Pipedream attack platform discovered in 2022 went even further. It appeared to be focused on electric and oil and gas facilities—liquified natural gas systems in particular. But it could be modified for use against any industrial envi-

ronment and had the ability to disable or brick control systems and undermine safety systems in ways that could potentially endanger lives—for example, if it was used to cause a chemical spill or cause equipment to catch fire or explode. This impact can be multiplied if safety systems are simultaneously disabled as Stuxnet did and as Triton was designed to do.

So in summary, we've seen threat actors testing and toying with increasingly destructive capabilities, though we haven't yet seen them deployed to their full ability.

With regard to attacks during heightened conflict, we so far only have a limited view of attacks that have occurred during conflict. Your committee no doubt has access to more extensive information about what has occurred that may not be publicly known.

In the case of Ukraine, we expected Russia to engage in more destructive attacks against Ukrainian critical infrastructure, but Russia's actions in cyber space have been fairly mild in comparison to what they could have done. In the early days of the invasion these operations were mostly limited to denial-of-service attacks and wipers that erased data and system files on government and military networks. But there have been a couple of examples that went beyond this—Russia's attack against Viasat modems used for satellite communications and internet connectivity. The attack was time to occur at the start of the invasion and succeeded to wipe thousands of modems to render them inoperable. Users were unable to get internet access and wind turbine operators were unable to monitor their systems over the internet. The attack also likely had some impact on the ability of Ukraine's military to use satellite communications during a critical time at the start of the invasion, but there are conflicting reports about the extent of the impact and we likely won't have a complete picture of what occurred until after the war.

A second consequential—and potentially destructive attack—was discovered before it could work. I'm referring to the discovery of malware in the early days of the war that could have taken out power in part of Ukraine had it not been discovered first. Since then there have been attacks designed to subvert drones and drone operators. But the war in Ukraine has mostly been dominated by kinetic operations rather than cyber ones—with the caveat that we don't know what we don't know. No doubt more information about cyber operations conducted during this conflict will come out after the conflict ends.

The reasons for Russia's limited showing in cyber space during the conflict are varied. Russia intended Kyiv to fall within 3 days after the invasion and therefore may have decided not to damage grid and other critical systems because it would have needed these systems to be active for when it took control of Ukraine. There are also suggestions that assistance from US Cyber Command and private security firms in the days leading up to the invasion helped Ukraine root out Russian hackers who were lying in wait inside critical infrastructure systems. Booting them out before the invasion left them with no access to these networks when the invasion occurred.

The other recent conflict that has been included digital attacks is the conflict between Israel and Iran—but many of these operations have been conducted under a guise of hacktivism, so it's unclear which operations can be directly attributed to either of these nations or to hacktivists working on their behalf or direction. In the case of Iran, we have seen attempts to target critical infrastructure in Israel, but these have not been very successful. Against Iran, we have seen more successful operations, such as one that led to a fire at a steel plant. But again, we have a limited view of what's occurred. Israel has extensive capabilities in cyber space and it will take time to discern how it used them during this conflict.

All of this is to say that attacks against critical infrastructure have, in practice, been less damaging than they could be—certainly less damaging than the adversaries conducting them are capable of doing.

Question 2. Why is it significant that Stuxnet exploited 4 zero days?

Answer. It's only significant for what it told us about the attack and the attackers behind it. At the time Stuxnet was discovered in 2010, zero-day exploits were rarely discovered in the wild. Out of 12 million pieces of malware that security firms captured and examined each year, only about 12 of these were zero-day exploits. The rest were exploits targeting known, and patched, vulnerabilities.

Zero-day exploits were rare in part because they were resource-heavy to discover and use, and they were expensive to purchase for anyone who didn't have the ability to discover them on their own. A researcher could take days picking through software code to discover a zero-day vulnerability, then someone would have to write exploit code to attack the vulnerability, and test that attack code to make sure it worked as intended. All of this took time and money, which is why most attacks involved non-zero-day exploits that targeted already-known and patched vulnerabilities.

So when researchers discovered that Stuxnet was using 4 zero-day exploits (it actually used 5 zero days, but Microsoft patched the fifth vulnerability the exploit was designed to target, before the attackers could use their exploit). The number of zero days in one attack made it immediately clear to the researchers who studied it that Stuxnet was the product of a nation-state. Only a state agency or military would possess a stockpile of zero days so large that it could afford to waste 4 zero days in a single attack. I say "waste" because once Stuxnet was discovered, those exploits became mostly obsolete, due to software vendors patching the vulnerabilities they attacked and antivirus firms adding detection capabilities to their products to catch any exploits targeting those vulnerabilities.

But the use of 4 (5) zero days also revealed something else. It revealed that the attackers were so determined—or desperate—to get their weapon onto the targeted systems that they were willing to burn 5 zero days to accomplish this.

Question 3. How did Stuxnet transform the interest of nation-states, such as China and Russia, in developing cyber capabilities to disrupt critical infrastructure?

Answer. Stuxnet put critical infrastructure on the map. It put this infrastructure on the map for defenders—in terms of raising awareness that these systems were highly vulnerable to attack—but it also put infrastructure on the map for attackers. Stuxnet was proof of concept for attackers that causing physically damaging critical infrastructure was possible using nothing other than malicious code. It also provided a detailed blueprint for how they could do this.

Post-Stuxnet, countries that until then had only conducted cyber espionage, invested heavily in building teams capable of conducting cyber offensive operations against critical infrastructure. Iran is among the countries that only began to develop these capabilities after the discovery of Stuxnet, and directly in response to Stuxnet. It's a cliche to say that Stuxnet opened a Pandora's box, but it really did.

Question 4. Did the development and execution of Stuxnet drive improvements around the security of sensitive and/or critical programs and operations in the United States? Please explain.

Answer. It did and it didn't. Certainly Stuxnet created awareness that critical infrastructure systems were poorly designed and vulnerable to attack, and as a result of this there were increased efforts to address this. An entire industry of people and companies emerged to focus on securing critical infrastructure. Researchers interested in uncovering vulnerabilities in the systems in order to fix them also emerged. And vendors who had poorly designed the systems in the first place began to develop new ones that were more secure.

But securely-built systems aren't the only problem with critical infrastructure. A larger problem is resources and policies and a willingness to do what needs to be done.

For example, the intrusion into the Oldsmar water plant in 2021 highlighted the vulnerability of water treatment systems in particular, which are often managed by poorly resourced municipalities that lack people and money to secure and manage these systems. Oldsmar was using wildly outdated software and had poor password practices that left it vulnerable, and many small critical infrastructure facilities don't have the knowledge or staff to ensure that their systems and networks are secure.

But as I pointed out in my written testimony, even large critical infrastructure facilities like Colonial Pipeline are not up to speed. Colonial Pipeline failed to heed warnings about attacks that had been hitting pipelines for more than a year and also failed to follow a number of best practices that might have prevented the attack or mitigated its impact. Colonial Pipeline, despite its critical role in distributing fuel, had no chief information security officer and instead had left its deputy IT director to manage security duties on top of his regular ones.

For many of these operations it comes down to priorities and cost. Security isn't cheap or easy to implement and it also isn't static. You can't simply install a firewall and antivirus software and implement multi-factor authentication and call it a day. Threats evolve and networks constantly change each time you install new software or swap out a server with a different one. Security requires constant attention, re-evaluation and upkeep, and this is expensive.

I want to mention one last thing before I end, because this often doesn't get addressed in discussions about critical infrastructure. Election systems are critical infrastructure as well, and they are no more secure than any other critical infrastructure though every bit as important. Many State, county, and municipal departments that run elections don't have the resources to secure their voting machines and back-end infrastructure and now have even less assistance to help them do this following recent cuts to Federal funding and staff. I've been writing about election security since 2004, and although awareness of election security has grown immensely

in the last decade, the systems themselves are far from secure given the current nature of threats against them.

I'd be happy to elaborate further on anything I've written here.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR ROBERT M. LEE

Question 1. While the cyber threat landscape has changed significantly since the discovery of Stuxnet, the use of malware to disrupt critical infrastructure continues to occur. How has malware evolved since Stuxnet?

Answer. Malware has become more sophisticated in the 15 years since Stuxnet, and its use has scaled up dramatically. Stuxnet was a bespoke, targeted weapon and existed in a context of fewer, and less sophisticated cyber threats. The threat landscape today is a sprawling interplay of criminal groups and state actors working to rapidly identify and exploit vulnerabilities for a range of economic, ideological, and espionage purposes. Attacker tactics and techniques have evolved to a degree that perimeter-based cyber defenses are obsolete, and sophisticated actors can, and do, enter advanced enterprise networks and remain undetected for months or years. Ransomware has developed into a full-fledged industry. In an operational technology context, malware, like PIPEDREAM has evolved to target a range of industrial control systems. Criminal and state actors are increasingly turning their attention to OT environments, because they know how critical they are to the basic functions of civilization. That prioritization means more numerous, and more sophisticated types of malware targeting these systems. All of this means that operational technology networks are under unprecedented threat, and the potential damage from an attack has grown in tandem.

Question 2. How often are zero days exploited now, and what steps can operational technology (OT) providers take to reduce the presence of zero days in OT environments?

Answer. Zero-day vulnerabilities are a real problem, and operators need to be diligent about patching vulnerabilities as quickly as possible and monitoring their networks for threats and anomalies. That said, the vast majority of attacks continue to exploit known vulnerabilities, and human error. By implementing the 5 critical controls that I, and Tim Conway, laid out in our SANS Institute paper on the topic, operators can protect themselves from most attacks. Most critically, operators need to know what's in their network. Network visibility is key to mitigating all vulnerabilities, including zero days. Visibility is what enables you to find vulnerabilities and find out if you've had any vulnerabilities exploited. Most of our adversaries don't rely on vulnerabilities—they rely on the inability of operators to see them when they breach a network. This enables them to live off the land and sustain breaches for long periods of time. OT network visibility is what enables you to detect, stop, and mitigate attacks. Of course, we should be diligent about finding and patching vulnerabilities, but for operators, the use of key security controls, and maintaining strong network visibility is where the focus should be. We have the tools and practices to protect utilities from these threats. As I said in my testimony, defense is doable and should focus on the fundamentals.

Question 3. Given our scarcity of cyber professionals, many State and local critical infrastructure owners and operators may not have someone on staff who focuses on cybersecurity. For those owners and operators who lack skilled cyber talent and have scarce resources, what cybersecurity measures would you recommend they prioritize to secure their systems?

Answer. Under-resourced utilities face a tough set of challenges stemming from a lack of skilled cyber professionals, and from the cost of implementing strong cybersecurity protections. Dragos has worked to address these challenges through our Community Defense Program, which provides our full security platform to American utilities with $100 million or less in annual revenue. We also have the free OT CERT program, which provides a number of free training, threat intelligence, and best-practices resources to under-resourced utilities. I'd urge eligible utilities to take advantage of the resources we offer. Beyond that, I again must emphasize the importance of fundamentals. Implementing the basic controls I outlined during the hearing, and in these responses, will eliminate most threats. It's also critical that governments don't overload small operators with contradictory and confusing rules that distract from basic security work.

Question 4. What new risks do artificial intelligence (AI)-enabled cyber tools introduce to critical infrastructure that we did not face during the Stuxnet era?

Answer. The full effect that AI will have for both attackers and defenders remains to be seen, but AI will very likely increase the scale and sophistication of threats against OT systems. Stuxnet was carefully produced with a distinct target in mind. Since that attack, we've seen malware like PIPEDREAM developed that can target

multiple types of systems. AI may enable adaptive malware that can morph and evolve in response to the defenses it encounters, with the goal of overcoming them. So AI will likely continue the evolution of malware to become more capable and more ubiquitous. But that's not the only consideration when it comes to AI in an OT environment. AI is already being connected to OT networks to harvest data. This is done for operational purposes: to improve automation, make systems more efficient, and the like. This increases the attack surface for OT systems and introduces a new attack vector that hasn't been fully considered by many operators.

Question 5. Can you describe the trends you have seen regarding how hacktivists target Western critical infrastructure? What are their motivations, capabilities, and primary targets?

Answer. Dragos has observed a large increase in the number of attacks being carried out by, or under the guise of, hacktivist groups. State-aligned hackers are using cyber operations to hit critical infrastructure in conflict hotspots like Ukraine, Russia, and the Middle East, while hacktivist groups are stepping up their own attacks on energy and water systems worldwide. These actors have managed to penetrate further into OT networks than was ever the case previously. In some cases, they are teaming up with government-backed actors, giving nations a deniable way to cause disruption. It is reasonable to expect that we will see a hacktivism component to any major conflict in the future, and the already blurred line between the goals and motivations of hacktivist groups and the states they are aligned with could get yet more confusing. This is part of the reason that network monitoring is critical. Network monitoring increases the chances that an attack will be detected, and properly attributed, and that the effects of an attack won't be passed off as an unrelated technical issue. This gives operators, and policy makers a more stable environment to make decisions about how best to defend networks, and how to identify and stop bad actors.

Question 6a. What unique cyber threats does the defense industrial base face from other sectors, particularly from Iranian-affiliated actors?

Answer. The defense industrial base is one of, if not the most targeted sectors of our economy for obvious reasons. While Iranian-affiliated actors aren't as advanced as other adversaries, they are highly motivated at this time. As with all critical infrastructure sectors, when thinking about the defense industrial base, we can't only consider production facilities, company headquarters, and the like. We also need to consider the upstream utilities that make the operations of those facilities possible. Iran has targeted American utilities in the past and could do so again as a way of disrupting the DIB.

Question 6b. Although the Cybersecurity and Infrastructure Security Agency (CISA) is not the Sector Risk Management Agency for the DIB, how can CISA be a helpful partner to the DIB in its role as National Coordinator of Sector Risk Management Agencies?

Answer. CISA is well placed to serve as the lead coordinator, and main policy-setting authority for different industries. As I made clear in my testimony, I believe that CISA can be most effective in this role by being selective in whom it involves in threat sharing and policy setting efforts. Involving too many individuals or entities makes these programs unwieldy and unfocused. CISA can help the DIB by coordinating threat information sharing in a sensible and focused way and helping to set outcome-based rules and standards. As I advocated in the hearing and elsewhere, I believe the National Guard can best serve as a nationwide incident response force for OT attacks, including those targeting the DIB, but this should occur in conjunction with CISA as the primary Federal policy coordinator.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR TATYANA BOLTON

Question 1. Has the intrusion of Volt Typhoon, a People's Republic of China (PRC) state-sponsored cyber actor, spurred more awareness in the cybersecurity community about risks facing operational technology (OT) environments? Why or why not?

Answer. The intrusion of Volt Typhoon has undeniably amplified awareness within the cybersecurity community regarding the specific risks facing operational technology (OT) environments. The public nature and scale of this and other similar breaches, such as the National Guard breach, have served as a stark reminder of the persistent and sophisticated threats posed by state-sponsored actors.

While there is heightened awareness, the OTCC members have observed that this has not consistently translated into widespread, measurable behavioral changes across all critical infrastructure sectors. The initial alarm generated by these events often fades, and organizations may return to pre-incident operational norms without implementing the robust, long-term security measures necessary to mitigate future risks.

A critical vulnerability highlighted by these intrusions is the interconnectedness of information technology (IT) and OT networks. Many attacks on critical infrastructure have originated in the IT environment before penetrating the more sensitive OT systems. This underscores the urgent need for a "survivability" mindset, where OT systems are designed and protected to remain operational even if the IT network is compromised. This can only be achieved through rigorous network segmentation, physically and logically separating OT from IT to create a resilient defense.

A significant gap remains between awareness and action, as I mentioned in my opening statement. The prioritization and allocation of resources to defend our Nation's critical infrastructure must increase to a level commensurate with the severity of the threat.

Question 2. Which sectors of U.S. critical infrastructure are most dependent on OT systems for daily operations? How do you assess the current state of OT resilience for those sectors?

Answer. The short answer is: all 16 critical infrastructure sectors rely on OT systems for daily operations, from water and health care to chemical facilities and the Defense Industrial Base. However, some are so fundamentally reliant that any disruption to their OT would have an immediate and catastrophic impact. These include:

- *The Energy Sector*.—The electric grid, oil and gas pipelines, and power generation facilities are controlled almost entirely by OT systems.
- *Water and Wastewater Systems*.—OT systems manage everything from water purification and pumping to distribution and wastewater treatment.
- *The Manufacturing Sector*.—OT is essential for continuous and automated processes in areas like chemicals, food and agriculture, and critical defense manufacturing.

The current state of OT resilience across these sectors is inconsistent. While awareness of cyber threats to OT has grown significantly, major gaps and vulnerabilities remain.

1. Legacy Systems and Convergence.—Many critical infrastructure facilities still run on legacy OT systems that were never designed with modern cybersecurity in mind. The increasing convergence of IT and OT networks—while efficient—has created new pathways for attackers to move from an enterprise network to a core industrial control system.

2. Fragmented Regulations.—The regulatory landscape is a patchwork. Some sectors, like the electric grid, have well-established mandatory standards (e.g., NERC CIP), while others have minimal or voluntary frameworks. This leads to inconsistent levels of security and makes the entire ecosystem more vulnerable.

3. Resource Disparity.—Smaller entities within these sectors, such as small water utilities and regional manufacturers, often lack the financial resources and technical expertise to implement robust cybersecurity measures, as was discussed during the hearing.

Addressing these challenges requires a comprehensive and collaborative approach. The Operational Technology Cybersecurity Coalition (OTCC) is currently working on publishing a Maturity Model for Sector Risk Management Agencies (SRMAs). This model is designed to provide a standardized, risk-based framework for organizations that lead critical infrastructure engagement. It's a vital step toward creating a consistent and repeatable process for assessing and improving OT security.

However, more must be done, especially to support the most critically underresourced sectors. Providing financial aid, technical assistance, and clear, actionable guidance is essential. The Government must work hand-in-hand with the private sector to build a more resilient and secure critical infrastructure for our Nation.

Question 3. How do organizations safely integrate information technology (IT) systems with OT? Please provide some best practices.

Answer. Safely integrating information technology (IT) and operational technology (OT) systems is a complex but necessary process that requires a strategic approach. The goal is to leverage the benefits of IT/OT convergence—such as enhanced data analytics, efficiency, and predictive maintenance—without compromising the safety, reliability, and security of critical OT environments. The fundamental principle is to establish a secure boundary between the two systems while allowing for controlled and monitored communication.

Here are some best practices for safely integrating IT and OT systems:

1. Network Segmentation and Zero Trust Architecture

- *Implement Network Segmentation*.—This is the most crucial step. Physically and logically separate the OT network from the IT network using firewalls and demilitarized zones (DMZs). This creates a buffer zone where data can be exchanged, but direct connections between the two environments are prohibited.

This prevents threats that compromise the IT network from easily propagating to the OT network.

- *Micro-segmentation*.—Further segment the OT network into smaller zones to limit the lateral movement of a threat if a breach occurs within the OT environment itself.
- *Adopt a Zero Trust Model*.—The principle of "never trust, always verify" is essential. Assume that any user, device, or connection, whether inside or outside the network, is a potential threat. All access requests must be authenticated and authorized, even for traffic moving between IT and OT systems. While Zero Trust for OT is not the same as Zero Trust in IT, these main principles remain.

2. Comprehensive Asset Inventory and Monitoring

- *Establish a Complete Asset Inventory*.—Maintain a detailed and continuously updated inventory of all OT assets, including hardware, software, firmware, and their vulnerabilities. This provides a clear understanding of the attack surface and helps in prioritizing security efforts.
- *Continuous Monitoring*.—Use specialized monitoring tools that understand OT protocols to track network traffic and asset behavior. This helps in detecting unusual activity and identifying potential threats in real time, enabling a faster response.

3. Strict Access Control and Authentication

- *Principle of Least Privilege*.—Grant users and devices only the minimum level of access required to perform their functions. This limits the potential damage if an account is compromised.
- *Role-Based Access Control (RBAC)*.—Assign access based on job roles to streamline management and ensure that permissions are appropriate for each user's responsibilities.
- *Multi-Factor Authentication (MFA)*.—Require multiple verification methods for access to critical systems, especially for remote access. This adds a crucial layer of security, making it much harder for an attacker to gain unauthorized access even if they have a password.

4. Holistic Risk Management and Governance

- *Develop a Joint IT/OT Security Policy*.—Create unified security policies that address the unique requirements and risk tolerance of both IT and OT environments. This requires close collaboration between IT and OT teams to ensure a shared understanding of security goals and operational priorities.
- *Regular Risk Assessments*.—Conduct frequent risk assessments to identify and prioritize vulnerabilities. This process should be specific to the OT environment and consider the potential physical and safety consequences of a cyber attack.
- *Create a Culture of Collaboration*.—Bridge the cultural and knowledge gap between IT and OT teams. Provide cross-training to ensure both teams understand each other's priorities, challenges, and security needs.

5. Incident Response and Recovery Planning

- *Develop a Specific OT Incident Response Plan*.—Create a detailed incident response plan that outlines procedures for detecting, containing, and recovering from security incidents in the OT environment. This plan should account for the unique operational constraints of industrial systems and prioritize safety and continuity.
- *Regular Drills and Exercises*.—Regularly test the incident response plan through tabletop exercises and simulated attacks. This ensures that teams are prepared to respond effectively and efficiently in a real-world scenario, minimizing downtime and damage.

6. Patch Management and Compensating Controls

- *Careful Patch Management*.—Develop a systematic and tested approach to patching OT systems. Patches should be thoroughly tested in a controlled environment before deployment to avoid disrupting critical operations.
- *Compensating Controls*.—For legacy OT systems that cannot be patched, implement compensating controls, such as network segmentation, virtual patching, and rigorous monitoring, to mitigate known vulnerabilities.

Question 4. How can the United States ensure it has a workforce that is sufficiently trained and large enough in size to protect both OT and IT systems? Please describe the current level of coordination among professionals with these individual skill sets in the United States, as well as assess the state of individuals in the U.S. cyber workforce that have both skill sets.

Answer. The United States faces a growing shortage of cybersecurity professionals in both operational technology (OT) and information technology (IT), creating a serious risk to national infrastructure. OT cybersecurity requires specialized knowledge of physical systems, industrial protocols, and real-time operations. Unlike IT, which focuses on data protection, OT is tied to the safety and continuity of physical proc-

esses. Yet most training programs and workforce strategies still focus heavily on IT, leaving a gap in OT expertise.

Professionals trained in both domains are scarce, and coordination between OT and IT teams remains limited. Many organizations lack clear pathways for talent development in industrial cybersecurity roles.

To address this, the OTCC recommends the following:

- Create targeted training programs, apprenticeships, and curricula that combine engineering and cybersecurity skills, tailored to OT environments.
- Expand upskilling efforts to help existing IT and engineering professionals transition into OT cybersecurity roles through hands-on, practical training.
- Establish clear career pathways within industrial cybersecurity, including:
  - Junior IT and OT roles that lead to OT GRC or Security Analyst positions
  - OT Analysts progressing to Security Architect or Director of OT Security.
- Encourage integrated OT–IT teams across public and private sectors to improve collaboration and break down operational silos.

A resilient cyber workforce must be equipped to secure both digital networks and the physical systems that depend on them. The OTCC urges Federal leaders to prioritize OT cybersecurity workforce development in all national security planning. Congress can directly help by funding workforce grants focused on OT training, supporting partnerships with industry for hands-on experience, and ensuring Federal cybersecurity initiatives include OT-specific talent development goals.

Question 5. What resources exist for State and local OT operators to best protect themselves from cyber threats, especially from nation-state actors?

Answer. There are many resources available to help State and local governments strengthen the cybersecurity of their operational technology and industrial control systems (OT/ICS). Several of the most useful are listed below. However, the real gap is not in the availability of guidance—it is in the capacity to use it.

Most State and local governments do not have full-time staff with expertise in OT security. Aside from State departments of transportation and the occasional water utility, these governments typically lack the dedicated personnel needed to apply technical guidance, assess vulnerabilities, or manage secure system design. Budget constraints are the main barrier.

As a result, many governments rely heavily on outside vendors—systems integrators and OT product suppliers—to design and deploy secure systems. This approach is expensive, and because internal staff often lack the technical knowledge to request or evaluate cybersecurity features during procurement, essential protections are frequently left out altogether.

Even when governments want to improve, they struggle to act on best practices outlined in standards such as those from NIST or ISA/IEC 62443. These frameworks are valuable, but without the staffing and resources to implement and verify the work, they have limited practical impact. It is like giving someone a detailed blueprint without an architect—they can see the plan, but not how to build it.

In addition to resourcing, our coalition encourages the Federal Government to provide the same level of support to State and local operators under attack as they would a kinetic act of war. While OT systems need better cybersecurity, the reality is that States and small or medium-sized OT owners and operators do not have the resources necessary to defend against a nation-state actor.

Expiring Provisions That Congress Must Swiftly Reauthorize

- *State and Local Cybersecurity Grant Program (SLCGP).*—Provides dedicated funding to help State and local governments build foundational cybersecurity capabilities. Grants can support hiring staff, developing cybersecurity plans, improving incident response, and securing critical infrastructure systems, particularly where in-house expertise is limited.
- *Cybersecurity Information Sharing Act of 2015 (CISA 2015).*—Enables timely, secure sharing of cyber threat information between the Federal Government and non-Federal entities—including State and local governments—by offering liability protections and privacy safeguards. These protections make it easier for governments to participate in information-sharing programs and benefit from real-time threat intelligence.

Training & Webinars

- *Critical Infrastructure Training Portal*.—Offers free independent study, sector-specific trainings (e.g., Chemical, Dams, Nuclear), and instructor-led modules to infrastructure owners and operators. (CISA)
- *Critical Infrastructure Learning Series*.—No-cost, hour-long expert-led webinars on infrastructure security best practices. (CISA)

- *Cybersecurity Training & Exercises*.—Includes no-cost incident response training, cyber range exercises, tabletop exercise packages, and participation in large-scale drills like Cyber Storm. (CISA)
- *NICCS/FedVTE/CISA Learning*.—The NICCS portal provides access to thousands of cybersecurity courses. FedVTE (now evolving into CISA Learning) delivers free on-line training in areas like ethical hacking, risk management, and malware analysis. (CISA)

Assessment Tools & Services

- *Infrastructure Survey Tool (IST)*.—Web-based assessment to evaluate facility security and resilience. (CISA)
- *Regional Resiliency Assessment Program (RRAP) and Resilience Planning Framework/Playbook*.—Tools for identifying risks and building resilience at the facility or regional level. (CISA)

Cybersecurity Tools & Services

- *Free Cybersecurity Services & Tools Catalog*.—An interactive database of free CISA-provided and external tools, searchable by readiness level, performance goals, or provider. (CISA)
- *Cyber Hygiene Services*.—Free vulnerability scanning of internet-facing systems with automated weekly reporting. (CISA)
- *Cybersecurity Evaluation Tool (CSET)*.—A downloadable tool to assess cybersecurity posture using recognized frameworks; supports both IT/OT systems. (CISA)
- *Ransomware Guides, Alerts & Advisories*.—Regularly updated publications, playbooks, and advisories to help organizations detect and respond to threats. (CISA)

Other Non-CISA resources available:

National Institute of Standards and Technology (NIST)

- *NIST Cybersecurity Framework (CSF)*.—Free, widely-adopted framework for assessing and improving cybersecurity posture.
- *Special Publications (SP 800 series)*.—Free, detailed guidance on topics like risk management, access control, industrial control systems (ICS), and supply chain risk.
- *Self-assessment tools*.—For example, the Baldrige Cybersecurity Excellence Builder (free) helps align cybersecurity activities with business strategy.
- *https://www.nist.gov/cyberframework*.

Department of Energy (DOE)—Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

- *Cybersecurity Capability Maturity Model (C2M2)*.—Free tool for energy and utility companies to evaluate and improve cybersecurity posture.
- *Free Technical Assistance Programs*.—Offered through national labs to help electric utilities with risk assessments and vulnerability mitigation.
- *Risk-informed Planning Resources*.—Playbooks and templates specific to energy infrastructure resilience.
- *https://www.energy.gov/ceser*.

Multi-State Information Sharing and Analysis Center (MS–ISAC)

Run by CIS (Center for Internet Security) and funded by DHS/CISA, this is free for SLTTs (State, Local, Tribal, and Territorial entities):

- Free endpoint detection (Albert Sensor).
- Vulnerability assessments and scanning.
- 24/7 SOC and incident response.
- Security advisories and intelligence feeds.
- *https://www.cisecurity.org/ms-isac*.

U.S. Cyber Command/Joint Cyber Defense Collaborative (JCDC)

- *Threat intel sharing (via JCDC)*.—Public-private partnerships to proactively share and address threats to national critical infrastructure.
- *Cyber Hunt & Response Teams (CHRTs)*.—Deployable Federal experts for incident response (in coordination with CISA/FBI).
- *https://www.cybercom.mil/*.

Question 6. What steps should the U.S. Government take beyond issuing the June 22 DHS National Terrorism Advisory System alert, if any, to support OT partners?

Answer. In addition to issuing the June 22 DHS National Terrorism Advisory System (NTAS) alert, the U.S. Government should take proactive steps to materially support operational technology (OT) stakeholders in defending critical infrastruc-

ture. Alerts are important, but without sustained resourcing and implementation support, their impact is limited.

To move beyond awareness and toward resilience, the Government should prioritize the following:

- *Mandate and fund OT asset inventories across Federal agencies,* beginning with the Department of Defense and expanding to all departments responsible for critical infrastructure. Without clear visibility into deployed systems, agencies cannot assess or mitigate risk.
- *Explicitly prioritize OT security in national cybersecurity strategies and funding allocations.* OT systems are often underrepresented in policy and budget planning, despite being essential to physical infrastructure operations. They require distinct attention apart from traditional IT systems.
- *Expand the State and Local Cybersecurity Grant Program (SLCGP)* by creating a dedicated track for OT-related needs. This funding should be directed to small and rural infrastructure operators, such as water utilities and local transportation agencies, which are frequent targets but often lack full-time cybersecurity staff.
- *Invest in technical workforce development focused on OT environments.* Many public entities are aware of their risks but lack the personnel with specialized expertise to apply frameworks such as ISA/IEC 62443 or NIST's Cybersecurity Framework in operational settings.
- *Support the use of the OTCC-developed Sector Risk Management Agency (SRMA) Maturity Model,* which helps identify gaps in sector preparedness and guides incremental, practical investment. The model allows Federal leaders to tailor guidance based on a sector's current level of maturity and progress toward resilience.

Ultimately, NTAS alerts should be matched with sustained public-private coordination and the delivery of meaningful resources. The risk to OT systems is not hypothetical. Our adversaries are actively preparing to exploit these vulnerabilities, and national policy must reflect that urgency.

QUESTIONS FROM CHAIRMAN ANDREW R. GARBARINO FOR NATE GLEASON

Question 1. What resources exist for State and local operational technology (OT) operators to best protect themselves from cyber threats, especially from nation-state actors?

Answer. The vast majority of cyber attacks on critical infrastructure systems take advantage of poor cyber hygiene practices and known vulnerabilities and exploits. Ensuring basic cyber hygiene is an important step that operational technology (OT) operators can take to protect themselves. There are existing resources that can help an operator improve their preparedness:

- The NIST Cybersecurity Framework provides high-level structure and can help develop a strategic view of cyber defense.
- The CIS Critical Security Controls provide more detailed information on how to implement the strategy in the cybersecurity framework.
- The SANS Top 5 Critical Security Controls emphasize the 5 most important recommendations out of the CIS Critical Security Controls.
- CISA's Cross-Sector Cybersecurity Performance Goals provide a checklist to ensure a baseline level of protection.

An organization might choose to use the CISA Cross-Sector Cybersecurity Performance Goals to achieve a minimum level of capability, then expand that capability over time using the CIS Critical Security Controls. Federal funding opportunities like the Department of Homeland Security's State and Local Cybersecurity Grant Program can help provide resources for implementation.

Products like the Section 9 Risk Register, developed for the energy sector by the Department of Energy's (DOE) Office of Cybersecurity, Energy Security and Emergency Response (CESER), can help operators understand their level of preparedness against current nation-state threats. The Risk Register uses current intelligence information to develop a set of unclassified attack scenarios that broadly capture the intent and capability of current nation-state adversaries. Operators can select characteristics of their system and receive a score that indicates how difficult it would be for adversaries to achieve certain outcomes. Operators can then explore how various additional hardening and mitigation options would affect that score.

Participation in Federal public-private partnership programs allows operators to both leverage Federal capabilities and threat information as well as benefit from the expertise and experience of other critical infrastructure operators.

- DHS CISA invites the country's most critical infrastructure entities to participate in the CyberSentry program. This program brings advanced detection ca-

pabilities to program participants and helps enrich Federal Government understanding of current threats being seen on U.S. OT networks.
- DOE's Cybersecurity Risk Information Sharing Program (CRISP) is a partnership between the electric power industry, DOE and the Electricity Information Sharing and Analysis Center (E–ISAC) that enables utility network traffic to be analyzed against a wide variety of threat indicators from Government and intelligence sources. Participants can share their information anonymously and receive near-real-time alerts and mitigation guidance.
- DHS CISA offers their Cyber Hygiene Services (CyHy) at no cost to critical infrastructure operators. The CyHy service provides vulnerability scanning for internet-accessible assets and delivers a weekly report to help organizations reduce their attack surface.

The Federal Government also offers various tools and training to help critical infrastructure operators defend their systems. CISA's Malcolm tool, developed in collaboration with Idaho National Laboratory, is an open-source network traffic analysis tool suite that works with OT protocols. CISA offers both on-line and in-person training for OT operators. And DOE CESER, also in collaboration with Idaho National Laboratory, leads the Operational Technology Defender Fellowship Program, which is a year-long education and development program for OT security or operations managers at energy sector organizations.

For additional help, CISA has more than 100 cybersecurity advisors deployed around the country that can be accessed through the CISA regional offices. Emerging initiatives outside of the government, like DEF CON Franklin, are also seeking to organize community volunteers to help improve cybersecurity at critical infrastructure entities.

Question 2. In what ways can artificial intelligence (AI) improve the detection and response capabilities of defenders protecting OT environments from cyber attacks?

Answer. AI is rapidly transforming the way defenders detect and respond to cyber attacks in OT environments. OT systems—such as those controlling power plants, manufacturing lines, or water treatment facilities—are increasingly targeted by sophisticated cyber threats. Traditional approaches to identifying anomalous network activity and vulnerable software rely on exhaustively enumerating potential concerns and continuously scanning for them. Examples include rules-based security tools (for example, flagging logins at unusual hours or blocking known malicious IP addresses) or static software analysis tools (which examine code without executing it, looking for potential weaknesses that could be exploited by malicious actors). These approaches remain important, but they have significant limitations, particularly when dealing with nation-state threats. These methods often generate large volumes of alerts, most of which turn out to be benign. This high rate of false positives can overwhelm security teams, making it difficult to identify true threats, especially those that are subtle or novel. These approaches can also be computationally expensive, which make it infeasible to scan for all vulnerabilities exhaustively.

AI enhances detection and response in several key ways:
- *Contextual Analysis*.—AI can analyze vast amounts of network and device data to understand normal OT operations and relationships.
- *Alert Prioritization*.—AI can filter and prioritize alerts, reducing noise and helping defenders focus on the most credible threats.
- *Anomaly Detection*.—Machine learning models can identify subtle deviations from normal behavior that are often missed by static rules.
- *Threat Correlation*.—AI can correlate events across different systems and time frames, revealing attack patterns that humans might miss.
- *Automated Response*.—AI can trigger automated containment or investigation actions, enabling faster, more consistent responses.

At Lawrence Livermore National Laboratory (LLNL), we have developed several AI-driven tools to address these challenges. Some examples include:
- OTDetect learns the typical communication patterns between devices in an OT network and flags unusual interactions that could indicate a compromise.
- Greywind is designed to detect sophisticated beaconing or "phoning home" behavior by compromised devices.
- NetWolf integrates data from multiple sources to provide a holistic, AI-driven view of network activity, enabling defenders to see the bigger picture and respond more effectively.
- OGhidra is an advanced bridge connecting local Large Language Models (LLMs) with the Ghidra reverse engineering platform to provide an AI-driven interface for binary analysis.

Detecting and responding to intrusions is critical, but those activities alone cannot secure OT environments. LLNL has developed a multilayered framework called Im-

mune Infrastructure, which also includes focuses on understanding the systems, keeping the adversary out, and operating through compromise. For example, adversaries can work through hardware and software supply chains as an initial avenue to compromise an OT environment or as a mode to create malicious effects. AI can be a force multiplier to illuminating supply chains, identifying vulnerabilities in hardware and software, and supporting the secure implementation of devices in OT environments. To help drive this, LLNL is leading efforts to incorporate AI into the Energy Cyber Sense program focused on Energy Sector supply chain risk management.

These AI-based tools do not replace human defenders but rather amplify their effectiveness. By automating the analysis of complex data and highlighting the most significant threats, AI allows security teams to respond faster and more accurately—critical in environments where down time or disruption can have serious safety and operational consequences.

In summary, AI augments the detection and response capabilities of OT defenders by:

- Reducing alert fatigue through smarter filtering and prioritization
- Detecting sophisticated and previously unknown attacks
- Enabling faster, more coordinated responses
- Providing actionable insights that support both immediate and long-term security improvements.

As cyber threats to OT environments continue to evolve, integrating AI-driven tools is becoming essential for maintaining robust, resilient operations.

Question 3. Are you concerned about the risks to OT posed by quantum computers that are capable of breaking cryptography? If yes, what is the role of the Federal Government in helping critical infrastructure owners and operators address the potential threat to their OT posed by advancements in quantum computing?

Answer. While encryption on OT networks can increase the security of the system, there are concerns that it could impact network performance, introduce challenges with some legacy devices and reduce visibility into the network. As a result, encryption is not widely used on OT networks, so once an adversary has access to an OT network, breaking cryptography is often unnecessary, rendering risks from quantum attacks somewhat limited.

However, there are cases where the risk of quantum attacks is of concern for OT systems.

- If access to the OT systems is provided through VPNs or other remote access solutions (RDP, SSH) that rely on weak cryptography for security, then they may be vulnerable to quantum attacks.
- With more prominent cloud adoption by OT operators, any OT services or data leveraging the cloud, where encryption is heavily used, could be susceptible to quantum attacks.
- There is potential that adversaries are currently collecting encrypted traffic that could contain credentials or other sensitive information that once decrypted would allow adversaries to access the OT systems even if quantum-safe encryption was adopted.
- OT services that use encryption will need to be updated with quantum resistant algorithms. However, many OT devices have limited processing power and memory, which could make transition to more complex, quantum-safe encryption algorithms challenging.
- Many firmware updates are digitally signed. Quantum algorithms could be used to derive underlying private keys, allowing the adversary to make malicious modifications to a device's firmware and forge the digital signature of the vendor, allowing it to be run on the device.

In summary, there are use cases that need to be considered for OT systems in a post-quantum world and there is a need to identify risks, enumerate vulnerable OT applications and design effective mitigations. Collaboration between vendors, operators, service providers, regulators, and sector risk management agencies is essential to get ahead of this threat.

Question 4. Can you describe the trends you have seen regarding how hacktivists target Western critical infrastructure? What are their motivations, capabilities, and primary targets?

Answer.

Rising threats to Western critical infrastructure

Over the past 20 years, cyber defenders have witnessed a notable rise in the volume, sophistication, and targeting of Western critical infrastructure by threat actors. In today's cyber landscape, attackers can directly impact the physical systems

supported by information or operational technology, resulting in cyber-physical effects such as power or water outages and degraded services.

Traditional social protest cyber attacks continue to grow, disrupting fuel stations and web services to draw attention to activist causes. The availability of attack tools, safe havens for operations, and the expanded attack surface of Western infrastructure contribute to a persistent opportunity for hacktivists. Increasingly, such activity also serves as a front for hybrid, nation-state-sponsored campaigns aimed at advancing geopolitical objectives.

Motivations and key actors

Hacktivists targeting Western critical infrastructure are motivated by geopolitical agendas, political objectives, or social protest. The majority of current activity comes from pro-Russian, pro-Iranian, and vigilante groups, with many receiving direction and funding from state sponsors. This blurs the line between independent activism and state-backed cyber operations.

These hybrid threats often masquerade as hacktivist activity but later prove to involve nation-state actors, as seen in the 2015 Ukrainian energy grid attacks.[1] They merge elements of hacktivism, financial crime, and geopolitical strategy, exploiting global events to advance their sponsors' interests.[2]

Notable examples include:

- The Cyber Army of Russia Reborn hacktivist group has targeted critical sectors in the United States—specifically water and wastewater and oil and natural gas—with confirmed incidents in California, Florida, and Pennsylvania.[3] Target selection for this group is designed to support Russian interests, and reports have tied them to Sandworm, a Russian military intelligence unit.[4] The group has been sanctioned by the U.S. Department of Treasury.
- Since 2022, utilities in North America and Europe have reported a surge in attacks from pro-Russian hacktivists against water and wastewater treatment facilities, dams, energy providers, and the food and agriculture sectors.[5]
- In 2023, CyberAv3ngers (linked to Iran) attacked water treatment facilities in the United States and Israel where they demonstrated access to Human Machine Interface (HMI) devices by defacing the device by leaving a message threatening Israeli-made equipment.[6]
- GhostSec attacked programmable logic controllers (PLCs) of Israeli companies as part of their "Free Palestine" campaign.[7]

Advances in AI and availability of tools enable hacktivists

Hacktivists have a treasure trove of cyber capabilities to enable their operations. Their main techniques are distributed-denial-of-service (DDoS), hack and leak, website defacements, publishing personally identifiable information, and network intrusions.[8] Hacktivists have access to a bevy of tools on the internet and can purchase exploits on the Dark Web, often with technical support included. Training in hacking is readily accessible through free and paid services, enabling hacktivists to upskill quickly to target specific technologies or take advantage of well-publicized exploits. In addition, services that sell credentials from information stealers can be used as part of operations for initial entry, giving hacktivists access to critical infrastructure organizations for a fee. Network intrusions can lead to the most crippling effects, which could include data wiping of critical equipment.[9] Wiper and ransomware software is readily available for sale, and in some cases with technical support arranged as part of the purchase.[10]

In today's cyber space, a motivated and financed hacktivist can upskill, find, target, and even leverage AI to exploit poorly-defended critical infrastructure assets.

---

[1] *https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/*.

[2] *https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/4040975/resilient-nations-and-hybrid-threats-what-can-the-united-states-learn-from-swed/*.

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

[4] *https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/*.

[5] *https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf*.

[6] *https://claroty.com/team82/research/from-exploits-to-forensics-unraveling-the-unitronics-attack*.

[7] *https://www.otorio.com/blog/pro-palestinian-hacking-group-compromises-berghof-plcs-in-israel/*.

[8] *https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism*.

[9] *https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf*.

[10] *https://www.justice.gov/usao-edny/pr/hacker-and-ransomware-designer-charged-use-and-sale-ransomware-and-profit-sharing*.

Hacktivist techniques are regularly observed through the CyberSentry Program

Through participation in the CyberSentry program, LLNL threat hunters have observed many cyber intrusions to critical infrastructure. Attribution of these attacks is difficult to conclusively prove, as the emergence of hybrid threats blends criminal with geopolitical motivations. LLNL analysts have observed exfiltration of sensitive data, attempted extortion, attempted ransomware deployment and cryptocurrency mining, some of which could be hacktivist-related.

Over the past few years, targeted threat hunts have been conducted against ongoing hacktivist campaigns. CyberSentry partners have notified CyberSentry of ongoing DDoS attacks, a known tactic of hacktivists, which were never attributed to a known threat actor. Without further visibility, monitoring and analysis of CyberSentry data, it will remain unseen if hacktivists are targeting our CyberSentry partners.

National security implications

Although the primary target of hacktivist groups may be a privately-owned energy or water facility, the impact could have cascading effects on national security. LLNL works closely with DOE to identify cyber risks that could impact Defense Critical Electric Infrastructure. This work with the DOE is instrumental in modeling the second and third order effects of cyber attacks and the consequences to national defense. These cyber weaknesses, much like the Goth's targeting of Rome's aqueducts, could lead to catastrophic consequences.[11] Western critical infrastructure is the underlying backbone for our Nation's and Western allies' ability to conduct defense, and without the water, energy, and communications infrastructure our military capability could significantly be degraded.

The threat of hacktivism to Western critical infrastructure has significantly morphed over the past 20 years—from groups motivated by inspiring social change with little to no cyber skills to present-day state-sponsored hybrid threats with deep experience in hacking and network intrusion. The combination of more internet-connected devices managing cyber physical systems and the proliferation of attack tools and training available to would-be hackers has intensified the risk of significant cyber events impacting critical infrastructure.

[11] *https://historyofthegermans.com/2021/12/17/totila/*.