The Operational Technology Cybersecurity Landscape 15 Years After STUXNET

LESSONS LEARNED AND RECOMMENDATIONS FOR NATIONAL SECURITY

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

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION
ONE HUNDRED NINETEENTH CONGRESS

22 JULY 2025, CANNON HOUSE OFFICE BUILDING

Robert M. Lee

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DRAGOS®