SECURING OPERATIONAL TECNOLOGY IN THE NATION'S CRITICAL INFRASTRUCTURE

INDUSTRIAL (ICS/OT) CYBER THREATS TO THE WATER SECTOR AND WHAT TO DO ABOUT THEM

HEARING
BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION
ONE HUNDRED EIGHTEENTH CONGRESS

_____

6 FEBRUARY 2024, 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. My name is Robert M. Lee and I am the CEO and Co-Founder of Dragos, Inc. a leading industrial cybersecurity technology and services provider. Additionally, I serve in advisory roles to numerous governments and international organizations across the world including the United States Department of Energy (DOE), Singapore's Cyber Security Agency, and the World Economic Forum's cybersecurity committees on oil and gas and electricity. I am a veteran of the United States Air Force and National Security Agency. It has been my privilege to be on the front lines of this problem in both government and the private sector.

Both government and industry have invested significantly in the cybersecurity of our nation's critical infrastructure. However, a vast majority of the focus has been on securing information technology (IT) networks. Less emphasis was traditionally placed on cybersecurity for operational technology (OT) and industrial control systems (ICS). These systems are the specialized computers and networks that interact with the physical world, including assets like a control system that opens a circuit breaker on an electric substation or operates pumps at a water facility. Most executives and policy leaders are shocked to find that upwards of 95% of cybersecurity budgets go to the Enterprise IT portions of the business and not the OT networks that can impact safety, the environment, and generate the revenue for the organization. OT systems are the critical part of critical infrastructure.

Even twenty years ago, ICS and OT were largely disconnected from other networks. The infrastructure was also complex and heterogenous with little in common between two facilities even in the same industry, making it more difficult and more costly for adversaries to create attacks that caused disruption or physical destruction in a way that was repeatable across sites and industries. Now, these systems,

including those in the water and wastewater sector, are increasingly digital and homogenous by necessity. Threat groups can develop capabilities that target devices commonly used in OT environments across sectors and have found new ways to access and manipulate them causing disruption and posing safety risks.

In 2018, I testified before Congress that Dragos, Inc. tracked five state actor cyber groups that targeted industrial networks specifically. At the time, I noted that while that sounded alarming, we had time to address these issues if we worked diligently. Today, Dragos tracks over 20 such groups and my message has more urgency. Water utilities and other critical infrastructure organizations are also facing challenges stemming from the current geopolitical environment. They find themselves on the front lines, often with very limited resources, needing to defend against both state actor cyber groups and criminal groups.

To protect and defend OT in the water sector requires both an understanding of the environment and investment in the right resources. My testimony focuses on three key points that are relevant to the Subcommittee and this hearing's focus.

- The first point is that there are fundamental differences between the operational technology and information technology that underpin our nation's critical infrastructure. IT is focused on how you enable and manage the business while OT is focused on why you are a business. The different missions, or purposes, of IT and OT systems dictate what is required of them and how organizations manage risk to them. The risks and threats to those systems, how the threats operate, the consequence of attacks, as well as the controls used to manage that risk, are also different across OT and IT environments.

- The second point is that the cyber threat landscape for operational technology and industrial control systems, including those used in facilities in the water and wastewater sector, has shifted irreversibly in recent years. The same digitalization, connectivity and uniformity in OT that is enhancing efficiency and reliability for infrastructure owners and operators is also adding risk. This digital transformation of our industrial industries is necessary but without investing in cybersecurity in advance of that transformation the consequences will be dire. To minimize that risk and defend water systems and other infrastructure against those adversaries, the community must invest in and prioritize the cybersecurity of OT and ICS networks with a focus on implementing security controls that have demonstrated success against the methods used by those threat groups.

- The third point is that the public and private sectors must continue to work together to make sure infrastructure owners and operators, including small and under-resourced organizations, have the information, tools and resources they need to protect their systems. Both government and industry have unique capabilities and insights that provide real value to operators of infrastructure, including water and wastewater systems. We need to remove barriers that those operators face in accessing information, tools and equipment they need to defend their systems. We must also not forget that the issues are primarily an economics and awareness issue at our numerous municipally owned water utilities across this country. No amount of free vendor tools

or tax payer funded cybersecurity services will alleviate this issue without addressing the core economic challenge.

I. IT and OT Are Fundamentally Different

Both conceptually and functionally, IT and OT are fundamentally different. The biggest difference between IT and OT is the mission or business purpose of the system. Generally, IT systems are designed to support how you manage business. OT systems focus on the reason the business or organization exists. OT systems are the specialized computers and networks that interact with the physical environment to do things like control the pumps or chemical levels at a water treatment facility.

The distinct mission, or purpose, of those systems dictates what is required of them and informs how risks and threats to the system are defined and managed. For example, a Windows operating system computer hosting a database for a financial institution has a distinctly different purpose and impact of failure than a Windows operating system hosting the Human Machine Interface (HMI) for a nuclear power plant. An adversary may be able to exploit a targeted Windows system in a similar way across IT and OT, but their behavior within that system will differ depending on whether they are focused on intellectual property theft of the financial institution's database or on causing an unsafe operating condition and physical impact.[1]

The impact of a breach or compromise is different as well. IT tends to be focused on system and data security, and OT tends to focus on the system of systems and physics. In many IT compromises, gaining access to the system and understanding the system or its data are critical. The goal is likely data theft or disabling the systems. The adversary, in this case, does not often seek to cause physical impacts. In the OT cybersecurity community, the types of attacks that cause the greatest concern are those that seek to disrupt operations, cause physical damage, or even cause safety-related incidents that lead to equipment damage or loss of life. The threats operate differently, often using unique methods and capabilities to achieve their goals in OT networks.

OT also has unique requirements. While the requirements of both IT and OT environments sound similar– high uptime, redundancy, low latency – OT must support specific circumstances. High uptime for OT, for instance, is often measured in years, not months, with systems that literally run for multiple years between rounds of maintenance. Redundancy for OT focuses on availability more than security. Many OT critical components can't be turned off. Instead of the time it takes to move data from one place to another, latency in OT deals with the milliseconds that determine whether an assembly line functions correctly.

OT security requires a different mentality. It is unique from IT security. This is due to the nature of the physical environments and also because the threats that target them are different. The way threat groups operate, as well as the tactics and techniques they use, are different across IT and OT environments. Even just a decade ago, the threat landscape for operational technology (OT) and industrial control systems (ICS) was very limited. As a result, many of the security controls for OT have

[1] https://www.sans.org/white-papers/36297/

traditionally been IT controls that can be applied to OT environments. Many standards, regulations, and "best practices" are often focused on how to apply IT security controls to OT and not whether they should be applied. There are many IT cybersecurity practices, such as vulnerability management and endpoint protection systems, that have a completely different value proposition, emphasis, and effect in OT networks. Applying all of the IT cybersecurity controls of a business to the OT networks would yield wasted resources and likely cause more disruption to the environment than all the state actors currently tracked combined. Simply put, organizations should look to unique OT cybersecurity controls and then evaluate the IT cybersecurity controls based on what risk they reduce and, if so, the unique way they should be applied. Our communities cannot afford for companies to "gold plate" the problem nor can they afford them to ignore it.

II. The Cyber Threat Landscape for OT Has Shifted Irreversibly

Increasing digitalization, connectivity, and homogeneity in OT is changing the threat landscape

The same digitalization, connectivity, and uniformity in OT that is enhancing efficiency and reliability for infrastructure owners and operators is also adding risk. At the same time, a growing number of threat groups are targeting OT. To minimize that risk and defend water systems and other infrastructure against those adversaries, the community must invest in and prioritize the cybersecurity of OT and ICS networks with a focus on implementing security controls that have demonstrated success against the methods used by those threat groups.

Twenty years ago, manual and truly disconnected OT environments meant that cyber adversaries could not as easily reach or interact with OT systems through cyber means. However, as those environments started becoming connected and digitalized, adversaries have paid attention. In 2015 and 2016 Ukraine experienced the first power outages due to cyber attacks that used malicious software, or malware, that could be deployed at other electric transmission substations around the world. In 2017 the first ever cyber attack that targeted human life directly took place in a Saudi Arabian petrochemical facility by targeting an OT safety system.

As industry has moved towards more homogenous infrastructure with common software packages, common network protocols and common facility designs, it has brought both cost and operating efficiencies. At the same time, it has also reduced the complexity in which adversaries have to operate and opened the door for reusable, scalable adversary capabilities that can be used to target the OT of multiple organizations within and across sectors. Threat groups are also taking advantage of native functionality in increasingly digitalized and connected systems, demanding an emphasis on detection and response efforts, in addition to prevention.

In 2022, Dragos and its third-party partner in collaboration with the U.S. government discovered and analyzed PIPEDREAM, the first reusable cross-industry capability that can cause physical disruption or destruction. The PIPEDREAM toolkit has the capabilities to impact devices that control critical infrastructure in different sectors – devices that manage electrical systems, oil and gas pipelines, water systems, manufacturing plants, and even the control systems in military assets such as unmanned aerial vehicles and naval ships. PIPEDREAM also cannot simply be patched away as it takes advantage of native

functionality in the software and network protocols available cross-industry. Prevention is important to attempt but the necessity is on identifying, detecting, responding, and recovering correctly. At best guess currently less than 5% of global infrastructure has the ability to achieve this against PIPEDREAM-like capabilities.

Though a capability like PIPEDREAM is concerning, it is important to take a moment to acknowledge the victory here as well. Dragos and its partners worked with federal agencies to identify, analyze, and report on PIPEDREAM to the broader infrastructure community prior to PIPEDREAM being employed. This is one of the most significant public-private partnership wins of all time in cybersecurity and truly represents a "left of boom" moment for the industry. The capability can still be used in the future though and it would be shocking if other countries were not developing similar capabilities.

Threats to water and wastewater systems have the potential to disrupt operations and pose safety risks

Water and wastewater systems are vulnerable to a variety of cyber attacks that have the potential to disrupt operations and pose safety risks to the systems' ability to perform fundamental functions. In over half of our engagements with customers, Dragos has encountered issues with ICS/OT network accessibility from the internet.[2] Using weak or default credentials, which are often publicly available in the vendor's documentation, for OT devices increases the threat of exposure. Several recent examples demonstrate adversaries exploiting ICS/OT exposed systems.

- In November 2023, CyberAv3ngers, a self-styled hacktivist collective, executed an exploitation campaign targeting Unitronics programmable logic controllers (PLCs) across multiple sectors, including the water and wastewater sector. The campaign employed unsophisticated methods such as secure shell (SSH) brute-forcing and exploiting default configurations.[3] In December 2023, government agencies from the United States and Israel released a joint Cybersecurity Advisory linking the activity to Iranian National Revolutionary Guard (IRGC) activities targeting an Israeli company.[4] The campaign's impact was notable, causing operational disruptions such as the shutdown of a water scheme in North Mayo, Ireland, and affecting wastewater treatment facilities in the U.S. Despite the unsophisticated nature of the attacks, they underscored the potential for high-impact consequences in industrial control systems (ICS) environments, highlighting the disparity between attack sophistication and potential operational impact. This also emphasizes the urgent need for organizations with OT environments to implement fundamental security measures, adhere to critical controls, and conduct regular monitoring to mitigate risks.

- In January 2021**,** an adversary used stolen TeamViewer credentials to delete programs related to the water treatment system for a San Francisco water utility.[5] Dragos is unaware whether the

[2] https://www.dragos.com/year-in-review/
[3] https://www.dragos.com/blog/cyber-av3ngers-hacktivist-group-targeting-israel-made-ot-devices/
[4] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
[5] https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206

deleted water treatment programs were in an ICS/OT system, but had the attack been successful, San Francisco's water operations certainly would have been impacted through loss of control, availability, and safety.

- In February 2021, similar to the attack against the San Francisco water treatment facility, an adversary leveraged stolen TeamViewer credentials to access a human-machine interface (HMI) in the ICS/OT environment of an Oldsmar, Florida, water supply organization to change the water's sodium hydroxide (NaOH) level.[6] If successful, the Oldsmar water supply would have been poisoned and may have impacted the health of Oldsmar's citizens. The similarity of the San Francisco and Oldsmar attacks, including the same initial intrusion techniques, highlights how universal OT architecture within the water and wastewater sector can lower the barrier for adversaries to attack. Successful tactics, techniques and procedures (TTPs) used against one entity can be effective against others as well.

Adversaries are also targeting remote service technologies and solutions, as well as communications protocols. In 2023, Dragos observed an uptick in the water and wastewater sector in adversary actions using these types of connectivity. This highlights the importance of properly securing remote service applications and coordinating with third party vendors and contractors to do the same.

- In October 2021, in a joint advisory, the U.S. Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) stated that between 2019 and 2021, adversaries gained access to water and wastewater sector ICS/OT environments through spearphishing as an initial intrusion and then pivoting to ICS/OT environments through internet-accessible PLCs that required no authentication using remote services.[7]

- In January 2024, CyberArmyofRussia_Reborn, a known hacktivist group that has been associated with a known state actor, posted a video to their Telegram channel showing the manipulation of water tanks associated with two water authorities in Texas in the United States. Based on information in the video, it appeared that they changed the tank water level indicators, which turned on the pumps. The adversary remotely accessed the human-machine interface (HMI) via remote services, likely causing Damage to Property, Denial of Control, Manipulation of Control, and Loss of Availability.

Also notable, almost all of the activity observed by Dragos in the water and wastewater sector was indicative of reconnaissance efforts, suggesting adversaries are using tools to map out water entities' public-facing internet infrastructure for future operations.

While largely opportunistic, ransomware operators are increasingly attacking industrial organizations in several sectors, including water and wastewater. Ransomware has primarily threatened organizations' IT systems, without proper network hygiene, the connectivity between the IT and ICS/OT environments

[6] https://www.dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/
[7] https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a

often provides a pathway for adversaries to attack ICS/OT systems directly. Double extortion tactics used by ransomware operators add to the threat for water and wastewater organizations because releasing sensitive ICS/OT data and diagrams could provide other capable adversaries with valuable information they can use in campaigns with ICS/OT disruptive or destructive objectives.

- In August 2022, adversaries attacked a United Kingdom (UK) water supply company, South Staffordshire Water (SSW), using the cl0p ransomware. The ransomware operators disrupted SSW's corporate Information Technology (IT) network; however, their ability to supply clean public water was not impacted. On 16 August 2022, the ransomware operators posted pictures on its leak site of what appear to be stolen identification documents and screenshots of SSW's Human Machine Interfaces (HMIs). They claimed to have gained access to SSW's ICS/OT network and could manipulate chemical processes.[8]

III. The Public and Private Sectors Must Work Together to Make Sure Infrastructure Owners and Operators Have the Information, Tools, and Resources They Need to Protect Their Systems and Communities

The best way to help the water and wastewater sector, as well as other critical infrastructure sectors, protect against threats to their OT environments and to manage risk is for government and industry to work together, each using our unique capabilities, insights and expertise to provide real value to operators. We need to remove barriers that those operators face in accessing information, tools and equipment they need to defend their systems.

For federal agencies, such as CISA and EPA, this means focusing efforts at the strategic level, providing direction to industry regarding what to focus on protecting (i.e. what is a critically important entity/asset), what scenarios to protect against (such as the known threat scenarios to OT water systems), and provide opportunities to practice efforts while sharing knowledge. It also means investing in areas where the private sector isn't already investing and providing guidance that must come from the government. As an example, the Department of Energy's Cyber-Informed Engineering operates in an area where there is no market. It is intended to build cybersecurity resilience and principles into engineering efforts so that some of the cyber risks that we are concerned about are engineered out at a control and physics level before adversaries can exploit them. On the other hand, government resources continue to get funneled into grant programs and government initiatives that completely replicate technologies and services already available in the private sector that have been developed at lower costs with more expertise.

When it comes to regulation, the government must define and communicate what it is seeking to accomplish and prioritize outcomes. Dictating highly prescriptive controls that tell infrastructure owners how to run security in their own environments, which they know better than the government, will not reduce risk and is often counterproductive. I would recommend, instead, that the government coordinate with the private sector to use their expertise and knowledge of their systems to inform

[8] https://thecyberwire.com/newsletters/control-loop/1/4

outcome-based regulations. Regulations should also be informed by research such as the SANS Institute's 5 ICS Cybersecurity Critical Controls[9], which analyzed all known cyber threat attacks to industrial systems and identified the most effective and efficient controls against them.

We have seen this work well with models that the Federal Energy Regulatory Commission (FERC) and North American Energy Reliability Corporation (NERC) use. A regulatory agency proposes a regulation with details on what it seeks to achieve. NERC then forms a committee of members across the community to evaluate the effectiveness and feasibility of the proposed changes. This allows time for input and alignment and creates regulations that better meet the objectives. Further, models for collaboration instead of simply information sharing have begun to show value. NERC also facilities GridEx, a valuable sector-wide, large scale operational exercise that brings government, vendors, and operators together under blue sky conditions to simulate real-world scenarios. The exercise provides real, valuable insights that inform future priorities.

Another example of government successfully providing this strategic level of direction is when the Administration reached out to the Electricity Subsector Coordinating Council, the industry-CEO led group that collaborates with CISA and DOE, to coordinate on its priorities on threats to electricity ICS and OT. The Administration essentially laid out ***why*** they were concerned, including insights to cyber threats, ***what*** outcome was necessary to detect and respond to such ICS/OT cyber threats, but left the ***how*** to the private sector. The CEOs led a group to rapidly enhance the visibility across our industrial networks in the sector to detect industrial cyber threats by deploying commercial technologies, including one developed by Dragos called Neighborhood Keeper. The result is that the United States government now voluntarily receives real time insights from across the ICS and OT networks of the power companies that serve over 70% of Americans for free and at any time can identify new cyber threats and vulnerabilities.[10] This model of **why,** and **what**, but not **how** allows for the government to set and communicate straightforward priorities while allowing the expertise and innovation of the infrastructure operators to advise on how best to achieve the desired outcomes.

In another example of successful public-private sector collaboration, Dragos worked with Rockwell Automation and the U.S. government in advance of the disclosure of a novel exploit capability attributed to a state actor that affected select communication modules by Rockwell Automation deployed in industrial companies across the country. The U.S. government was able to leverage the insights from Neighborhood Keeper to determine how far wide these assets and vulnerabilities could be found, work with Dragos and Rockwell to develop detections and mitigations, deploy them in real time to the asset owners in the Neighborhood Keeper network, and simultaneously make the insights available to those who were not.[11] Another great "left of boom" example of what right can look like when the public and private sector utilize their strengths.

When the government speaks with one voice, the infrastructure community listens. However, when owners and operators receive different priorities and guidance from different agencies, it can cause

[9] https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/
[10] https://www.utilitydive.com/news/an-eye-for-an-eye-the-electric-sectors-defense-will-depend-on-federal-g/601643/
[11] https://www.dragos.com/blog/mitigating-cves-impacting-rockwell-automation-controllogix-firmware/

analysis paralysis in security teams. Agencies like CISA and EPA have tremendous opportunity to help critical infrastructure organizations prioritize security efforts to ensure they are investing in the things that truly reduce risk. For small organizations, like many water utilities, clear, relevant and aligned guidance really matters because they do not have large teams to analyze and prioritize recommendations.

Additionally, these efforts need to be properly resourced, both in the private sector and in the government. Some organizations have the resources and mechanisms to invest in cybersecurity. Many do not. There are thousands of water utilities across the country that share information technology contractors with other organizations simply to do basic information technology support. They do not have the expertise or resources for cybersecurity efforts, including those to protect operational technology. Free government assessments or further government investments in trying to develop the next greatest technology acutely miss their need. These smaller municipal and public utility infrastructure sites need direct resourcing through changes at a state and local level or resourcing from a federal level to go out and hire talent and purchase proven tools and technologies. Though we know "what" to do, the unfortunate reality is it is absolutely an economics issue.

In my role at Dragos, I see the challenges that these organizations face every day in building their OT cybersecurity programs. And so, in December, Dragos expanded our Community Defense Program to give under-resourced U.S.-based utility providers with under $100M in annual revenue free access, forever, to Dragos products and training to build their operational technology cybersecurity programs, improve their security posture, and reduce operational technology cyber risk. And yet, even with access to tens of thousands of dollars' worth of free technology and training each year most water sites will be unable to take advantage of the program. To use any technologies most of the water municipalities need basic infrastructure upgrades. Even a one-time cost of $3,000 on hardware and networking gear would be completely out of budget for these organizations and require a city council vote on the topic of cybersecurity that they do not likely understand. I have so much optimism about what we all can do together by playing to our strengths and caring enough about our communities to act using our knowledge to counter even the most sophisticated cyber threats. However, a major shift must take place in order for us to solve the underlying economic issues that would make any of it work at scale, especially in the water sector.

I. Conclusion

In conclusion, in order to help secure operational technology in the water sector, we must first understand the fundamental differences between the operational technology and information technology. The risks and threats to those systems, as well as the controls used to manage that risk, are also different across OT and IT environments. The cyber threat landscape for the OT environment has also shifted irreversibly. The same digitalization, connectivity and uniformity in OT that is enhancing efficiency and reliability for infrastructure owners and operators is also adding risk. To adequately defend water systems and other infrastructure against threats and adversaries, the community must invest in and prioritize the cybersecurity of OT and ICS networks using security controls that have demonstrated success against actual threats. Finally, the public and private sectors must work together using our

unique capabilities and expertise to ensure that water and wastewater organizations have the tools and resources they need to protect their systems. But all of this is predicated on addressing the economics and awareness of issues that exist at our local municipalities and town water systems.

I sincerely thank the subcommittee for providing me the opportunity to testify today and welcome any questions or requests for additional information.