ADDRESSING CYBERSECURITY RISKS TO THE CRITICAL PARTS OF THE UNITED STATES' ENERGY INFRASTRUCTURE

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

HEARING
BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES
UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

23 MARCH 2023, DIRKSEN SENATE OFFICE BUILDING

https://www.energy.senate.gov/hearings/2023/3/full-committee-hearing-to-examine-cybersecurity-vulnerabilities-to-the-united-state-s-energy-infrastructure

Robert M. Lee[1]

I. Background

Chairman Manchin, Ranking Member Barrasso and distinguished members of the Committee, 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. 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.

A little over five years ago I testified before this committee to discuss the industrial cybersecurity threat landscape which I noted at the time as largely unknown. My testimony focused on the critical part of critical infrastructure: the operational technology (OT) / industrial control systems (ICS). These systems are specialized computers and networks that interact with physics. As an example, a control system that opens a circuit breaker on an electric substation or a gas turbine control system that generates electricity. They are what makes critical infrastructure critical.

[1] CEO and Co-Founder of Dragos, Inc.
Bio: https://www.dragos.com/team/robert-m-lee/

For decades governments and infrastructure providers have focused on the cybersecurity of our critical infrastructure, especially the energy infrastructure. But my testimony in 2018 highlighted the fact that the industrial portion, the OT/ICS networks had largely been ignored and underinvested in. At that point in time these industrial networks that generate, transmit, and distribute electricity, manufacture medicine and consumer goods, make refineries and pipelines functional, control rail, clean and distribute water, and more were largely disconnected from other networks.

The lack of connectivity and digitization meant that cyber adversaries could not as easily reach or interact with these systems through cyber means. Thus, adversaries were largely unable to achieve their objectives on systems that they would otherwise target. However, those environments started becoming connected and digitized almost twenty years ago. That trend has only accelerated in recent years. Adversaries have paid attention to this change. They have achieved terrifying effects as a result while cybersecurity investments have lagged in comparison. In 2015 Ukraine experienced the first power outage due to a cyber attack across three regions of Ukraine. In 2016 it happened again in Ukraine with malicious software, or malware, that could be deployed at other electric transmission substations around the world. In 2017 the first ever cyber attack to target human life directly took place in a Saudi Arabian petrochemical facility where the adversary luckily made a mistake in the attack. So instead of people dying as the adversary intended, the company experienced downtime that resulted in hundreds of millions of dollars lost. Across 2018 to 2021 there were over a dozen new state actor cyber teams that started targeting industrial companies directly.[2] In 2021 an adversary compromised a water facility in Oldsmar, Florida in an attempt to change the chemicals to dangerous levels, but fortunately was caught because luckily a person at the facility noticed weird activity on the computer. When I testified in 2018, I noted that there were five state actor cyber groups that targeted industrial networks specifically. I testified that while that sounded alarming, we had time to address these issues if we worked diligently. Today there are over twenty such groups that we track and my message has more urgency.

II. The Three Points Today

My testimony today serves as an update to my testimony in 2018. I want to note what has changed over the last five years and what actions I assess we must take to continue to protect our national security and local communities. I will focus my testimony on three key points that are relevant to the Committee and this hearing's focus.

- The first is that the industrial cyber threat landscape has irreversibly shifted this past year. As a result, a heightened attention is required. It is necessary to prioritize OT/ICS networks with a focus on security controls that have demonstrated success against adversaries. We must do more than identify and implement best practices deployed in other areas such as enterprise information technology (IT).
- The second is that the government should seek to understand what is and is not working and act while taking advantage of collaborative efforts that already exist and are being

[2] https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Report-2022.pdf?hsLang=en

underutilized. This will enable the United States government and our nation's private sector to make strategic decisions about the capabilities and partnerships required for the future. Currently, there is an apprehension to call out what works and what does not work for fear of perception on picking winners and losers in the market. However, this approach means that the community has difficulty moving forward and wastes precious resources on efforts that are not as viable.

- The third is that it is important to identify what sites are critical, what risks they need to be protected against, and to properly resource these efforts. The private sector and the government must deploy resources. Most entities know what to do but policy issues impede them acting. Additionally, the federal government must be resourced and authorized correctly to secure its own infrastructure and serve as an example to private industry. Today unfortunately government agencies ask the private sector to take actions on its infrastructure that the government has not taken internally on its infrastructure.

III. Point 1: The Industrial Cyber Threat Landscape Has Irreversibly Shifted

In 2018 it was still extremely difficult to develop malicious capabilities and cyber attacks that could impact multiple industries at once. Given the heterogenous nature of industrial infrastructure there was little in common between two facilities even in the same industry. Different integrators, equipment, software, network communications, physical processes, etc. imposed great cost on infrastructure owners to manage different sites and workforce development across them. But that complexity also made it more difficult for adversaries to create attacks that caused disruption or physical destruction in a way that was repeatable across sites and different industries. For all the right reasons, the industry moved towards more homogenous infrastructure with common software packages, common network protocols, common facility designs, and more. This has brought a lot of advantages to the industry and those that depend on it, but reduced the complexity that the adversaries have to operate in while increasing the complexity of what defenders have to defend. Years ago, I often warned that I was not worried about the threats of today because our infrastructure owners and operators had focused so much on reliability and safety that it naturally helped cybersecurity. But, that one day we would get an adversary that took advantage of the homogenous infrastructure, and it would be a massive shift for the industry. In 2022 such an adversary emerged.

In 2022, during the course of Dragos's normal business operations, we were contacted by an undisclosed third party that had identified a new collection of malware. Dragos analysts used their unique ICS/OT cybersecurity expertise to analyze the capabilities and with permission partnered closely with United States government agencies. The capability was coined PIPEDREAM and was developed by a highly capable strategic state adversary.[3] PIPEDREAM is the first reusable cross-industry capability that can achieve disruptive or even destructive effects on ICS/OT equipment. Based on Dragos's assessment PIPEDREAM was initially targeted towards energy assets such as liquid natural gas and electric transmission equipment, but can work in almost all OT environments ranging from the heating, ventilation, and cooling equipment in data centers to the control systems used in next generation military equipment and weapon systems. Strategic adversaries over the years have performed high levels

[3] https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf?hsLang=en

of reconnaissance to pick the appropriate targets across the United States and to try to develop and maintain access to those targets. The addition of PIPEDREAM provides the first realistic cyber capability that can significantly disrupt critical infrastructure domestically. PIPEDREAM is not a capability you can simply patch away or otherwise prevent. Once it is in its target's networks, it is a reliable tool for an attack as it takes advantage of the native functionality and common software now deployed across infrastructure sites. This demands an effort to not just focus cybersecurity on preventing cyber attacks, but on detecting and responding to them as well.

PIPEDREAM rightfully sounds concerning but it is important to take a moment to acknowledge the victory here as well. Dragos, with its undisclosed partner, was able to work with the National Security Agency (NSA), Federal Bureau of Investigations (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and DOE to identify, analyze, and report on PIPEDREAM out 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. However, with the time that was bought it is important to ensure infrastructure owners and operators understand and mitigate the risk. However, this is not the only risk they must mitigate and the industry is often flooded with competing guidance. My next point addresses this topic.

IV. Point 2: Determining and Acting on What Does and Does Not Work

Governments around the world are appropriately apprehensive on picking winners and losers in the market. That apprehension has sometimes extended to even suggesting ideas or strategies for fear of the perception of preference. This has led to the repeated resourcing of ideas and efforts that lead to very little value while not further focusing on efforts that have shown success.

As an example, the DOE provides cutting edge research into many areas and has helped fund research with industry that has delivered unique capabilities and insights especially on innovative new energy technologies. However, it is difficult for me to name even one cybersecurity technology in the last twenty years that was developed by a national lab (i.e. not including grant programs with industry) that is still commercially viable or used across industry. The people that work at the labs are some of the finest Americans you will find with unique and much needed cybersecurity expertise. And instead of focusing those talents on strategic efforts there are usually numerous projects ongoing that overlap directly with what commercial providers have already made. There is not a lack of funding for cybersecurity technology in the private sector and yet government funding continues to go to efforts that are very often simply science projects looking for a problem to solve. Yet on the converse, there are some efforts at the national labs and DOE that are of strategic long-term importance to fundamentally shifting the cybersecurity discussion. As an example, DOE's Cybersecurity Informed Engineering operates in an area where there is no market and does so to build cybersecurity resilience and principles into engineering efforts. This translates to some of the cyber risks that we are concerned about being engineered out at a control and physics level before adversaries can exploit them. This will not solve all risks, but it shows the potential to reduce significant attack surface in a way that lets defenders focus.

As another example, when the government speaks with one voice the infrastructure community listens but when they are given competing guidance they understandably freeze. A typical power company CEO will hear from the DHS what the DHS sees as priorities for them to secure infrastructure; often straightforward guidance across two or three main areas. They are also going to hear priorities from the DOE on their straightforward guidance across two or three main efforts. They will likely also hear from every FBI field office across their service territory about their priorities, from the DOD and every base commander across their service territory about their priorities, from state regulators about their priorities, and from federal regulators about their priorities. Unfortunately, these two or three priorities are often times different across the various voices of government, causing analysis paralysis in security teams. Yet, we have seen good examples. When the Administration reached out to the Electricity Subsector Coordinating Council, the electricity CEO led group in partnership with DHS and DOE, and coordinated on its priorities the community listened. The Administration essentially laid out ***why*** they were concerned, including insights to cyber threats, ***what*** the outcome was that 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 to detect industrial cyber threats by deploying commercial technologies, including one co-developed between Dragos and the DOE called Neighborhood Keeper. The result was that the United States government now receives real time insights from across the industrial networks of the power companies that serve over 70% of Americans for free and at any time can identify new cyber threats and vulnerabilities.[4]

This model of why, 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 agreed upon outcomes. Doing it any other way has shown to be a disaster. In 2021, the DHS's Transportation Security Administration (TSA) launched a regulation called TSA-SD-2 for the interstate pipelines. The regulation came with almost no notice and no coordination across the industry or input from its experts. It sought to react to the Colonial Pipeline ransomware case. The community was not told why, despite hearing this was not just focused on Colonial Pipeline's case. It was not told what the government hoped to achieve out of the regulation, it only told operators how to achieve security with overly prescriptive regulations. Many of the security controls in the regulation were enterprise information technology security controls not appropriate for fuel and product pipeline OT environments. Following the regulation verbatim would have led to minimal security enhancements and very likely would have caused outages at pipelines as well. Fortunately, TSA listened to the community's outcry and feedback and adapted the regulation to TSA-SD-2c, which is much more directionally accurate by focusing on performance over prescriptive controls.

If the government seeks to push for future regulations it must understand why and what it is seeking to accomplish and place the priority on those outcomes. Dictating highly prescriptive controls that tell infrastructure owners how to run security in environments that they intimately know better than the government will result in failure. I would also recommend that the government seek to coordinate across government agencies to ensure that the regulatory efforts are not countering each other. At the federal level the priorities often range across multiple regulatory frameworks, where one company may operate in three or more regulated industries with little synergy between the efforts, causing an overly burdensome approach. Then, if you add in state level regulators the problem becomes even more complex as numerous states are seeking to develop their own cyber regulations that have very little to

[4] https://www.utilitydive.com/news/an-eye-for-an-eye-the-electric-sectors-defense-will-depend-on-federal-g/601643/

do with each other and will create a highly costly situation for energy companies with a mismatched network of regulations that provide little security value.

The key message is that when government partners closely with the private sector and uses their expertise, we achieve better outcomes. We have seen this through the model that the Federal Energy Regulatory Commission (FERC) and North American Energy Reliability Corporation (NERC) have used where the federal government proposes 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 for time, input, and alignment that creates regulations that better meet the objectives. Further, models for collaboration instead of simply information sharing have begun to show value. There are current efforts by the DOE and CISA to work with the electric industry to create the Electricity Threat Analysis Center (ETAC). The ETAC operates essentially as a sectorial specific spoke in CISA's overarching strategy to partner with critical infrastructure providers. The ETAC can centralize the efforts across government agencies and sharing centers such as the Electricity Information Sharing and Analysis Center (E-ISAC), and bring private sector companies and their trusted vendors to a central location to analyze and collaborate on cyber threats to the energy system.

The vendors must also be included in the discussions and held accountable to baseline requirements just like the asset owners and operators. If vendors want to play a role in the service and protection of critical infrastructure, especially its critical parts such as OT/ICS, they must be aware of their role and risks through the supply chain to the customers they serve. Right now, there are very few requirements on vendors and instead many make optional choices. As an example, at Dragos our Dragos Platform technology is deployed in critical sites from rail networks, to oil refineries, to electric transmission grids, to nuclear power plants. Optionally, and at great expense to ourselves, we decided to require 100% of our engineers and developers working on this technology to be United States citizens based in the United States; this is entirely abnormal in the world of software development due to its costs. However, it helps us better secure and control our supply chain by having all our developers in one country. The fact that I have the choice as the CEO of where I do development for the software put in nuclear power plants may not be in the best interest of national security.

Ultimately, the federal government should review its efforts and investments to ensure it eliminates duplicative or unnecessary projects and redirect resources to support strategic efforts such as Cyber Informed Engineering, the ETAC, and collaborating more fully on regulations or baselines created for the industry. These efforts should also include collaboration with the vendors and a willingness to set baselines that companies must meet to be included in the discussions. It is not a winning strategy on the topic of critical infrastructure and national security to have an expectation that everyone has exactly the same thing to offer equally and therefore should be included in every conversation on every topic out of concern of perception. Government, and especially the energy sector, need the ability to choose the right partners for the right situations regardless of perception.

V. Point 3: Identify What's Critical, Decide on Risk Scenarios, and Resource the Efforts

It is impossible to protect everything against every risk. The government must identify what is critical, what risks it should be prepared against, and ensure that the appropriate resources are able to be allocated against the challenge. Currently, there are multiple unclassified and classified lists on what is considered critical infrastructure beyond the high-level sectors. These lists often look to identify infrastructure by its size and impact for criticality or its proximity to important assets such as military bases. However, these lists are often created without full collaboration with the private sector and without clear requirements. Something is not simply critical because of its size or proximity nor is it critical for all requirements.

As an example, if the United States were to enter into conflict with China there are a set of infrastructure sites more important than others for the logistic lines and projection of force abroad. If the United States wants to launch intercontinental ballistic missiles back against an aggressor those infrastructure sites would be different. If the requirement is a crank path to restart key portions of the energy system, that would additionally be a different set of infrastructure sites. Some would be large sites but some would be very small sites not well understood by the federal government. Infrastructure owners and operators are put in an impossible situation to advise on what the key infrastructure sites they maintain are relative to unknown requirements other than "national security."

Further, protecting those sites against all cyber threats is unreasonable and extraordinarily costly. This is happening at a time where more is being demanded out of our energy system than ever before. The requirements sometimes feel as if they are: run a more reliable and safer energy system that is open to more operators than ever before while operating the system in a way it was never designed to including highly changing energy sources and technologies to make it more sustainable despite the loss of inertia and other important physical qualities of the electric system while making it more secure against all known cyber threats at as many sites as possible all while making it more affordable. In no way is my intention to be flippant, but it is not difficult to see how that is an unreasonable challenge. The energy system is becoming less resilient now than ever before because of its rapidly changing nature at a time cyber threats are paying more attention to it. It is important to help guide the community on what the requirements are so that they can advise on what is critical, while guiding them on what threat scenarios are relevant to national security so that they can advise on how to achieve the desired outcomes.

As an example, electric utilities could prepare for a combined attack by China, Russia, and Iran against substations and generation sites. But that combined threat scenario has never been seen before and to prepare against it would require significant investment that would have to be passed on to rate payers all while they are unsure if the security being invested in, against a scenario that has not been observed, would even be the right security controls when that scenario manifests. However, an electric utility that is not prepared for a Ukraine 2015 cyber attack, Ukraine 2016 cyber attack, ransomware across operations, and PIPEDREAM scenarios is behind in their efforts to counter threat scenarios that are real risks because they have happened in the industry before. Because they are real scenarios, it is easier to get buy in across the organization and to understand what the right security investments against them are, while measuring success, instead of "cyber security" being an intangible and ever increasing investment. Further, the security controls applied against known scenarios almost certainly would provide significant defense against other scenarios and unknown scenarios to include those that have not occurred yet.

If the United States government were to clarify roles and responsibilities, identify the requirements that the infrastructure needs to support, and the threat scenarios that are realistic that each industry should be prepared for, there would be a much clearer picture for infrastructure asset owners and operators on what they should do and how they can best advise and contribute their expertise.

Additionally, these efforts need to be properly resourced, both in the private sector and in the government. Many energy sites have the resources and mechanisms to invest in cybersecurity for federally important sites. Many do not. There are thousands of gas, water, and electric utilities across the country that share information technology contractors to do basic information technology support let alone cybersecurity. Free government assessments or further government investments in trying to develop the next greatest technology acutely miss the need. These smaller cooperative and public utility infrastructure sites would need direct resourcing through changes at a state level or resourcing from a federal level to go out and hire the talent and purchase the technologies they see fit. Many infrastructure sites are simply not allowed to spend money on cybersecurity without state regulator approvals which represent more than fifty different points of view on the risk and requirements. Even more so, there is an appropriate debate on whether it makes sense to have federal or national security requirements drive cost onto the energy system that local rate payers must bear. These are policy issues that, if resolved, would unleash the energy system providers to make more proactive choices.

Inside the government there are resourcing and authorities required to increase the level of cybersecurity to what the government is asking the private sector to reach. It can appear unintentionally hypocritical when asset owners and operators are held to regulations and standards that many government agencies and institutes themselves cannot meet. When the DOE resources new projects, such as distributed energy resource efforts across renewable energy sites, it very often does not include cybersecurity into the project requirements or efforts. DOE's Office of Cybersecurity, Energy Security, and Emergency Response could be resourced and authorized to ensure that a portion of the budget allocated for new energy technologies and efforts includes cybersecurity requirements to make these new sites more secure from the beginning. CISA could be more well-resourced and authorized to enforce cybersecurity requirements and efforts across federal agencies and institutions. It is difficult for the government to talk credibly on the topic of cybersecurity when its institutions have less security than most energy sites in the country.

VI. Conclusion

In conclusion, everyone has an opinion on what needs done and where, but leadership is necessary to set the actual priorities and requirements across government and the private sector. The infrastructure owner and operator community in the energy and natural resources sector has consistently shown that the majority of the players are focused on national security and not just business value creation. We must be willing to make hard choices as the threat landscape, and the energy system itself, has drastically changed. PIPEDREAM has shown that the threat landscape has irreversibly changed and that a sense of urgency is required. However, our infrastructure community has reliably shown that when empowered to do so, it will rise to the occasion and protect our communities and national security. We all are keenly aware that we live and work in the communities we serve. I would take an empowered energy sector and its partners over any state actor any day. Defense is doable.

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