THE INDUSTRIAL CYBER THREAT LANDSCAPE

THE ROLE OF THE PRIVATE SECTOR AND GOVERNMENT IN ADDRESSING CYBER THREATS TO ENERGY INFRASTRUCTURE

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

1 MARCH 2018, DIRKSEN SENATE OFFICE BUILDING

https://www.energy.senate.gov/public/index.cfm/2018/3/full-committee-hearing-to-examine-cyber-security-in-our-nations-critical-energy-infrastructure-030118

Robert M. Lee[1]

I. Background

Chairwoman Murkowski, Ranking Member Cantwell and members of the committee, thank you for providing me the opportunity to testify before you today. As a kid from a small town in Alabama with my parents who are both retired Air Force Senior Master Sergeants, it is a distinct honor to appear before you. My name is Robert Lee and I am the CEO and co-founder of Dragos, Inc. an industrial cybersecurity focused firm that takes an intelligence-driven approach to our technology and offerings and is staffed by some of the best in the community. Many of my teammates have served in the National Security Agency, military, and at the plant-floor level of the industrial environments we will be speaking about today.

I want to briefly explain my background which informs the testimony I bring before you today. I started my career at the United States Air Force Academy, was commissioned as a Cyber Warfare Operations Officer, and was then tasked out for most of my career to the National Security Agency (NSA).

While at the NSA I was tasked with building a mission to identify new nation-state groups and actors we had not previously known about. I built and led a first-of-its-kind mission focused on identifying the nation-states attempting to break into these environments. It was built on the hypothesis that we would find new threats; and we did. These were new nation-state teams performing new tradecraft during their operations. It was there I came to understand that there is a significant collection bias in the U.S. Intelligence Community and larger information security community. The community focuses and reports

[1] CEO and Co-Founder of Dragos, Inc. @RobertMLee

on the threats from where our collection exists and is blind to most of what goes on where we do not collect, such as industrial control environments.

My experiences have led me to assess that our industrial community has two strategic challenges: we do not understand the industrial threat landscape and we do not have enough trained professionals focusing on industrial control cybersecurity. For these and many other reasons I left the military and joined the private sector to tackle these issues. I built the community's first industrial control system incident response and investigations specific course at the SANS Institute and later a dedicated threat intelligence course there as well.[2,3] At SANS I have trained over 2,000 cybersecurity defenders across five continents at the world's smallest and largest companies. I learned from their points of view and their challenges.

I founded Dragos, Inc. with two of my co-workers from the NSA industrial threat discovery mission. It is at Dragos that we built the world's only intelligence-driven software technology for industrial networks to detect and respond to threats. It is also there we have the private sector community's only intelligence team fully dedicated to industrial control threats.

There were three major industrial cyber attacks over the last three years not counting the large number of adversary operations targeting critical infrastructure but not reaching the level of attacks. The Ukraine power grid cyber attack of 2015 was the first time in history a cyber attack halted grid operations, for that I was one of the lead investigators.[4] The Ukraine attack of 2016 where my firm helped identify and analyze CRASHOVERRIDE, the malicious software which was the first ever malware purpose built for disrupting electric grids.[5] And the attack in the Middle East in 2017 where my firm identified and analyzed TRISIS, the malicious software which was the first to ever specifically target human life and caused a petrochemical plant to shut down.[6]

II. The Three Points Today

Given my experience in the military and intelligence community, training the world's defenders, and leading the world's best against the world's worst, I would like to make three points today that are most relevant for this committee.

- The first, is that the industrial threat landscape is largely unknown. This demands that we seek to change this through an intelligence-driven approach that will then be used to inform our innovations, best practices, standards, and regulations.
- The second is that regulation has served a purpose in the private sector such as electric grid operators, but it is appropriate and needed to pause new regulation to allow the community to develop best practices and out-innovate our adversaries.
- The third is a recommendation for the new Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to focus on new and continued relationships between the DOE and the private sector while respecting that most of the knowledge of the threats and the innovation to counter them is occurring in the private sector. This drives a requirement for communities to work together without interfering in each's respective mission.

[2] www.sans.org/ics515

[3] www.sans.org/for578

[4] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[5] https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[6] https://dragos.com/blog/trisis/TRISIS-01.pdf

III. Point 1: The Industrial Threat Landscape is Largely Unknown

The industrial threat landscape is largely unknown. For years, the Department of Homeland Security's Industrial Control System Computer Emergency Response Team (ICS-CERT) has collected and centralized what they could to report on incidents in the private sector. Each year, media headlines highlighted the number of incidents in sectors like the electric power community. However, each year the most important metric was reported but went unnoticed. That metric stated that every single year, the number one attack vector for adversaries breaking in to industrial network was: unknown.[7]

The methods and collection the information security community has used to identify adversaries and their intrusions into corporate and business networks have not historically been available or present in the industrial networks. It is most certainly not present in the smaller co-ops and municipalities where adversaries are able to train and prepare undetected and undeterred. Industrial networks are different than the corporate and business networks of each company and require a different focus and approach.[8] Much of the collection by the U.S. Intelligence Community and the private sector has been in observing adversaries breaking into networks and patterning out and identifying their tradecraft and capabilities. This focus on intrusion analysis has led the private sector to be able to produce intelligence reports that rival and, in many cases, far exceed similar reporting in classified government settings. Simply stated, the best place to collect data relevant to cyber threats is in the networks of the targeted companies.

The information security technologies made for enterprise and corporate networks are often not appropriate for industrial networks and thus much of the community has believed that industrial threats are not common because of a limitation in this collection. Despite these limitations, some companies have done great work to identify some of the industrial threats especially when corporate networks are also being targeted. However, in the history of the information security community having purpose-built software, expertise for industrial security incident response, and threat intelligence focused on these environments is very new. In fact, it is only a few years old. As my team and others like it grow we will be faced with existing threats displaying new capabilities and brand-new threats we did not previously know existed. In other words, we will find more because we are looking now but it is also true that the focus of adversaries on industrial control environments is also growing significantly.[9]

Today my firm, Dragos, released three reports documenting our insights and lessons learned from 2017 across threats, vulnerabilities, and lessons learned in threat hunting and incident response.[10] We highlighted the CRASHOVERRIDE and TRISIS malicious software previously referenced but also noted a few very important key findings regarding the threats. First, common malware not purpose built for industrial networks is still incredibly impactful and disruptive in industrial control environments. Many of us heard of the large impacts of WannaCry and NotPetya malware on industrial environments such as the shipping and manufacturing industry that cost billions of dollars.

The report however also highlights and provides a base, census-like metric, that there are, on a very conservative estimate, at least 6,000 unique infections in industrial environments each year from common, non-targeted, malware leading to loss of revenue and in rare cases potentially unsafe conditions. However, common malware infections that spread indiscriminately are not what concerns me or most of the community. What concerns many of us most is the threat activity groups, or teams, who target

[7] https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

[8] https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

[9] www.dragos.com/yearinreview/2017

[10] Ibid.

industrial control networks. These types of campaigns against our infrastructures were rarely seen or discussed. In the Dragos annual report, the second key finding identifies that there are five such threat activity groups active this past year alone who are specifically targeting industrial control networks at infrastructure companies. There are significantly more groups that are targeting the corporate environments of infrastructure companies, but the increase in industrial specific targeting is a worrying trend. These five teams launched numerous operations that ranged from espionage to what appears to be the first stages of access required to disrupt operations.

As scary as that sounds, I want to take a moment to add an important note: the threat is far worse than people realize but not as bad as they want to imagine. My team often strives for nuance in our analysis and reporting on threats and we have observed a disservice to the community over the past decade. Even the most casual phishing email sent to a nuclear power station's corporate networks results in media headlines and inquiries about how adversaries are going to take down our infrastructure and kill people. The scenarios presented are often nonsense and full of hype and unintended misinformation. In North America we have some of the most defensible infrastructure on the planet thanks largely to our diversity and the community of people involved. Organizations ranging from the Edison Electric Institute (EEI) to NERC's Electricity Information Sharing and Analysis Center (E-ISAC) to the asset owners and operators who are doing the real defense are simply amazing and have ensured the reliability and safety of electric energy. As an example, our electric power grid and its various asset owner and operators have security infrastructure and culture of which the rest of the world is envious. The idea that a phishing email or even access into industrial networks would equate to mass chaos, disruption, and death is nonsensical and for poorly researched books and media headlines, not reality.

We as a community have only begun our journey though and there are industrial sites including those in North America whose internal teams have never even investigated the networks. I am aware of small electric co-ops, water utilities, gas pipeline facilities, oil refineries, wind farms, and manufacturing networks where not even the basics of security have been attempted although they are vital for modern civilization. The disparity across our infrastructure communities in terms of their investments and culture is a concern. As we identify the threat landscape more fully we must ensure that our technologies, best practices, standards, and regulations are informed by the industrial threat and are not simply copy and pasted insights from information technology and corporate networks as has often been the case in the past.

Equally important, we must be careful of technologies and approaches which sound too good to be true. These approaches are often referred to in the industry as buzzwords. They gain immense traction and attention when used in conversations, but security professionals widely understand their limitations and the abuse of those approaches. Blockchain, machine-speed automated response, and artificial intelligence are three such examples that are thrown around frequently as a panacea for our problems when they are simply not. Blockchain is just a ledger that does not *secure* anything, delays in response are due to vital investigations to have confidence in the actions we take not due to the need to push *machine-speed* changes, and unfortunately, we already have too much *artificial* intelligence in the security industry.

We must be measured and nuanced in how we approach the risk from cyber threats and the approach we take must be an intelligence-driven one that understands our threat landscape as well as the limitations we have in collection and analysis that hamper our understanding. Our approach must also respect that the best defense we can put forth against well-funded human adversaries is well trained and empowered human defenders operating in defensible environments with the right technology and insight and not simply the most interesting sounding.

IV. Point 2: The Role of Regulation in the Electric Power Grid

The multiple grids that make up the North American bulk electric system are different than they were fifteen years ago. Massive changes, for the better, have been made especially in the areas of implemented security controls. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are standards for Bulk Electric System asset owners and operators mandated by the Federal Energy Regulatory Commission (FERC). NERC CIP standards are often highly discussed topics, but it is undeniable that the efforts of the community to comply with these standards have made the North American Bulk Electric System the most resilient and well defended in the world. However, regulations and standards are the trailing end of best practices and only serve as a base level of security. They are not, nor would any regulation be, adequate in the face of determined adversaries. Malware and vulnerabilities are not the threat, the threat is the human adversary and we cannot regulate them away.

In fact, many regulations and standards focus on cyber hygiene and information sharing type efforts such as vulnerability management and patching. The Dragos report released today included an exhaustive look at all the industrial control system software and hardware vulnerabilities released in 2017. It identified that 64% of the vulnerability patches do not eliminate any risk because the components they were patching were already insecure to start with.[11] For 2018 we are tracking a new metric looking at the accuracy of the advisories themselves regardless of whether they reduce risk. So far in 2018 roughly 75% of the advisories released publicly had significant inaccuracies. These inaccuracies include a misunderstanding of the product, vulnerability, or the impact and risk it posed to the industrial process.

What that means is the community spends resources to address a problem that provides no benefit in addressing 64% of the time and often the industrial community is unsure if the vulnerability advisory was accurate at all. Patching is meaningful to reduce the attack surface but in industrial networks it is obviously far less meaningful than people realize. In looking at the Ukraine 2015 cyber attack, the investigation found that there were no exploits or software vulnerabilities used by the adversary in the industrial networks to disrupt the grid. In this case, they simply gained access, learned the systems and how to use them against themselves, and then used intended functionality to hijack away the system from their operators. An additional important metric in the Dragos report is that 72% of industrial control system vulnerabilities in 2017 provided no alternative mitigation guidance outside of patching, suggesting no method to reduce risk until after an update cycle. What this effectively means is the overwhelming focus for the industry is on patching away problems while it is, a majority of the time, ineffective against human threats. This is not to say that patching should not occur, but we should instead understand it does not reduce the risk nearly as much as the community would otherwise like to believe and we must take an active defense approach which means monitoring for, responding to, and learning from the threats in our environments. Regulations are not well suited for that challenge.

I have seen first-hand a regulation, check-box, mentality develop at companies subject to strong regulations. In my engagements with customers and in training the defenders of the electric system it is a common complaint I hear as well. Many resources go to satisfying regulations and trying to keep up with what regulations are coming next that a stall in innovation and security can occur. We have electric utilities today that have expressed the desire to do more in their industrial networks including deploying our technology to identify threats but are afraid to do so not knowing what regulation may come next and if their current investments will be upended by those new approaches. There are electric utilities that are

[11] www.dragos.com/yearinreview/2017

the most well protected companies in the world, there many more that are in the middle just trying to keep up with the regulations, and there are a rare few who are actually worse off as their precious resources had to be spent addressing regulation instead of the security efforts they were already doing. NERC CIP regulations have been an overall good initiative and have helped the electric community to improve its security, but we must now do something different for a period time.

I recommend for a period of three to four years that no new regulations be imposed under NERC CIP. This would allow companies to catch up with the current regulations that come out every couple of years in an unending push for more regulation. It will also allow the electric asset owner and operator community to spend a period of time innovating and thinking of new best practices informed by experience. At the end of this period DOE, FERC, NERC, and the regulated community can then identify best practices and determine if new regulations are appropriate. It is also in this time that a deep study and analysis of the threats is appropriate to ensure that our regulations are guided by lessons-learned from dealing with the threats and not general community best-practices that may not make sense for our electric community.

If this recommendation is not palatable then I would propose an alternative where the regulations are focused instead on program building, such as regulating that a company implement a threat intelligence program, instead of performance-based auditing. This would satisfy the potential desire to move regulations forward while allowing the electric community to develop their own ways forward inside of those programmatic bounds.

V. Point 3: Recommendations for DOE’s CESER

DOE’s Office of Electricity Delivery and Energy Reliability (OE) leads the DOE’s efforts to ensure a resilient, reliable, and flexible electricity system. OE accomplishes this mission through research, partnerships, facilitation, modeling and analytics, and emergency preparedness. These meaningful contributions to the electric community far exceed what regulation alone would ever accomplish. My experiences with DOE’s staff and their labs’ staff have left me impressed and those I know I am proud to call peers, colleagues, and friends. The DOE’s CESER office was the next logical step for DOE’s efforts in cybersecurity and energy security. The creation of the office is still a debated topic though. However, that decision has been made and it is important now not to cast doubt on the office’s future effectiveness but instead its role and what service it can perform for the community.

As the owner of a private sector company and as a member of the electric sector community I am always hesitant of well-intentioned government programs, grants, and efforts that ultimately are not in tune with what is already going on in the community. Such efforts can result in competition that stifles innovation, it can result in market noise, and it can result in the larger community not dividing and conquering all the various issues we have while working in tune with one another. The labs have historically pioneered discoveries in fields such as avionics, nuclear engineering, and grid reliability but the industrial cybersecurity field is a fast-moving area that I would like to see more cooperation that incorporates private sector technologies as opposed to spending years potentially replicating what already exists.

It is for these reasons that I would recommend three things to DOE’s CESER. First, provide multi-year funding and greater operational support to efforts that are prioritized to make foundational changes to the community’s risk. As an example, consequence-driven cyber-informed engineering (CCE) should be prioritized and supported. CCE will not address all cyber risks nor will it eliminate the ability for cyber threats to be effective. However, CCE will lead to systems and equipment in industrial control environments that are designed and built with an understanding of the cyber threats and risks translating to more defensible environments.[12,13] Encouraging improved product designs where efforts such as patching can be effective, and some smaller set of risks are eliminated altogether would be extremely meaningful to the community.

Second, serve as the key team focused on de-duplicating efforts in the DOE and their labs by being keenly aware of what is already taking place in the private sector. There is never malice or intentional overlap but the speed of the private sector in comparison to appropriations and grants as well as the sheer volume of innovation taking place can cause unintentional overlaps and competitive issues to emerge. DOE's CESER could, with the appropriate authorities, significantly reduce these issues.

Third, with a stated mission of focusing on addressing emerging threats realize and appreciate that the best insights and intelligence on threats in the community are inside the networks of the targeted companies. The private sector companies, like Dragos, that are already in those environments and gleaning threat intelligence can offer unique insights. Partnering with similar companies and such organizations as NERC's E-ISAC will provide the insights CESER needs without trying to recreate any efforts. Additionally, there are challenges for private sector companies to share their information with the government. Even beyond any trust issues much of the information that the government wants, and needs, is more akin to finalized intelligence assessments and not access to raw data. The private sector understandably wants to protect its raw and sensitive data but insights into the threat landscape, trends, and other types of intelligence assessments are often happily shared. There is a distinct role here for private sector security companies and the ISAC framework to act as a trusted layer between the organizations that are being targeted by adversaries and the government's authorities balanced with intelligence requirements. This can be achieved while providing security for these companies instead of just information and intelligence sharing.

It will be beneficial for CESER to work with organizations already doing the mission such as Dragos and the E-ISAC. Our insights into the threat landscape and emerging threats together is novel and currently underexplored in the larger community today. The value the private sector in concert with efforts such as DOE's CESER can provide meaningful defense to our critical infrastructures as well as those smaller infrastructures critical to our local communities.

I sincerely thank the Committee for providing me the opportunity to testify today and welcome any questions or additional information to help support the safety of our families, communities, and each other.

[12] https://www.ferc.gov/CalendarFiles/20170717080648-Assante,%20SANS%20Institute.pdf
[13] https://www.osti.gov/biblio/1341416