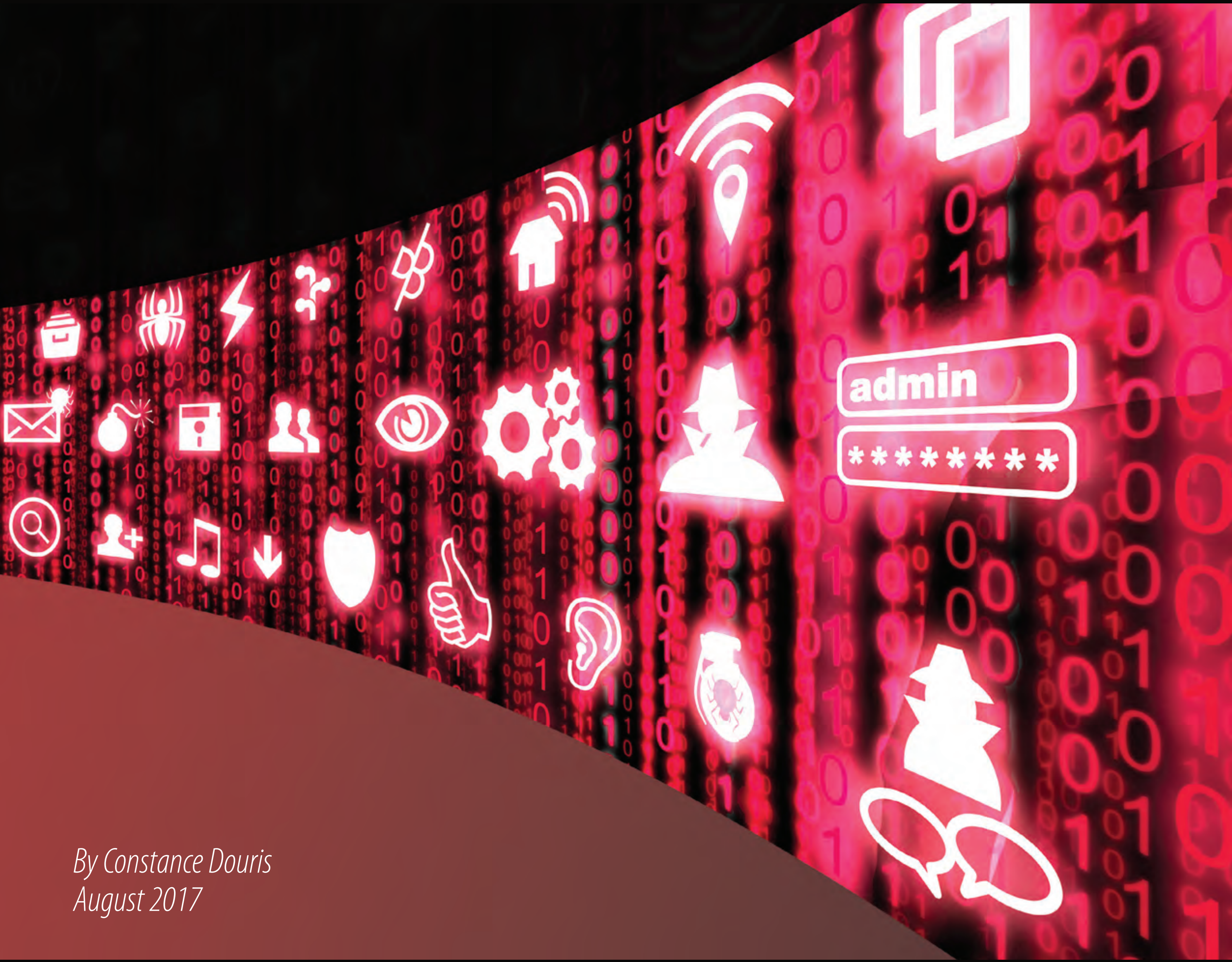
CYBER THREAT DATA SHARING NEEDS REFINEMENT



By Constance Douris
August 2017

Lexington Institute

FUTURE OF THE POWER GRID SERIES

CYBER THREAT DATA SHARING NEEDS REFINEMENT

By Constance Douris
August 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Technologies are being interconnected and integrated onto the nation's electric grid to decrease weaknesses. However, these physical and computerized elements multiply the number of access points for cyber risks, making protection of the grid challenging. If done correctly, sharing cyber threat information eliminates the chances for one cyber threat or attack to affect multiple stakeholders.

In theory, one entity identifies a cyber threat or attack and shares the collected information with public and private sector partners. The intelligence is then applied to protect these partners' networks. The intent is for data and systems to become more secure and less prone to cyberattacks when intelligence and resources are shared among many stakeholders. Without data sharing, it is almost impossible to detect, defend and contain systemic attacks early.

While sharing cyber threat data sounds easy, it is complicated by legal, operational and privacy issues. The private sector believes the government is good at collecting threat intelligence, but is hesitant to embrace it as an equal partner. Furthermore, the private sector fears it may be exposed to lawsuits for disclosing sensitive personal or business information. Released threat data could harm a company's reputation and even cause its stock price to drop. The data could also be used for regulatory actions or for law-enforcement and intelligence collection activities. Hence, the private sector is reluctant to share threat data without an incentive.

— continued

According to Agnes Kirk, Chief Information Security Officer of Washington, states are recognizing their important role of protecting critical infrastructure. At this time, there are no consistent cybersecurity controls for the distribution system, the final stage operated by utilities where electricity is delivered to customers. If a successful cyberattack on the distribution system disrupts electricity, devastating economic and security consequences could result. The distribution system needs to be protected to prevent damage to the bulk power system. Due to interconnection, taking down one or more utilities may create a ripple effect that destabilizes electricity in large areas. States need to make serious improvements to guard the grid from cyber threats.

Governors and state legislators need to develop mandates for public utilities commissions to implement strong cybersecurity controls and provide staff with necessary training. Chief information officers and chief information security officers should collaborate more with stakeholders to anticipate and prepare for emerging cyber threats. Governors could direct state information, emergency and security leaders to define roles and responsibilities in support of cybersecurity.

Currently, states in the U.S. are generally having a difficult time tailoring cyber threat intelligence to their distinctive needs. Automating the information sharing process, as California is currently pursuing, would ensure accuracy and speed of valuable and actionable data while decreasing costs. In addition, lessons learned from major cyber breaches ought to be thoroughly studied so that states are better equipped to defend their networks and respond. National Guard units are also assets that should be further developed to prepare and respond to a cyberattack on the electric grid.

INTRODUCTION

If the U.S. electric grid were to suffer a successful cyberattack, electricity could be broadly unavailable. This might have devastating economic and security consequences as electricity is needed to operate pipelines, medical facilities, telecommunications, military bases and other critical infrastructure. Thus, cyber threats that could halt electricity access need to be protected against.

In December 2015, a cyberattack interrupted Ukraine's power supply. The possibility of such an incident elsewhere in the world is possible. To protect the grid, government leaders, regulators, industry and other stakeholders need to share cyber threat data and develop requirements.[1] The 2015 Cybersecurity Information Sharing Act encourages the private sector to voluntarily report successful and unsuccessful cyberattacks to the Department of Homeland Security.[2]

Without information sharing, it is almost impossible to detect systemic attacks early enough to contain them.

In theory, sharing cyber threat data prevents one risk identified by an organization from harming another stakeholder's network.[3] Such data decreases cyber risks and enhances the overall resilience of the electric grid. Without information sharing, it is almost impossible to detect systemic attacks early enough to contain them.[4]

THE ELECTRIC GRID IS VULNERABLE TO CYBER THREATS

The electric grid is a complex infrastructure that delivers electricity. Smart grid devices are being integrated onto the grid to regulate the demand for electricity and manage the flow of information. While the smart grid aims to decrease the weaknesses of the electricity system and improve emergency response, increased interconnection and integration opens the system to more cyber risks.

Not only does the number of potential cyber threat access points increase with new devices on the grid, cyber access points further multiply because many of them are connected to one another through the internet. The U.S. electricity grid also must operate in real-time and cannot be shut down to make improvements.[5]

Some examples of components on the grid that are prone to cyberattacks include operational technologies, information technology systems and end access points. Other sections of the grid that are vulnerable to cyber threats include power line communication devices, supervisory control, intelligent electronic devices and data acquisition and energy management systems.[6]

An actual cyberattack on an electric grid was realized when Ukraine's electricity was interrupted in December 2015. A third party, widely suspected to have originated in Russia, conducted the attack which resulted in 225,000 customers losing power. Furthermore, Ukraine experienced over 6,500 cyber hacks to state institutions in November and December of 2016 alone. It is only a matter of time until another country experiences a similar attack.

The number of potential cyber threat access points increases with new devices brought onto the grid.

In 2009, U.S. officials tracked efforts by China, Russia and other countries to implant malicious software inside computers used by U.S. utilities.[7] In addition, American officials believe that a cyber campaign against the U.S. energy industry in 2014 resulted in the penetration of at least 17 companies' systems, including four utilities, where hackers stole data and gained access to private networks.[8] This means the hackers could have had the power to remotely adjust equipment settings on the grid. Due to interconnection, taking down one or more utilities may create a ripple effect that destabilizes electricity in large areas.

Recently, ESET and Dragos, two security firms, released reports about the discovery of a virus that aims to damage equipment on the electric grid. The virus is called Industroyer, also known as "Crash Override," and targets computers that control electrical substations and circuit breakers. This virus could turn off power, create rolling blackouts or physically damage grid equipment. In addition, this virus is a potential threat to all substations and circuit breakers because this equipment is largely standardized across the world.

Cybersecurity threats can be identified and defended against with more participants sharing relevant intelligence. The intent is for data and systems to become more secure and less prone to cyberattacks when information and resources are shared among many participants. Done effectively, sharing cyber threat data could reduce risks and enhance the resilience of the grid. Furthermore, threat intelligence could diminish the effects of a single cyber threat or attack by informing other partners to protect against it.

Done effectively, sharing cyber threat data could reduce risks and enhance the resilience of the grid.

CYBER THREAT INTELLIGENCE NEEDS TO BE ACTIONABLE

After stakeholders pass cyber threat information along, recipients then apply the intelligence to harden their networks and reduce the risk of malicious compromises. Data sharing also provides better situational awareness, the ability to identify, process and comprehend information on the grid. Having more knowledge about what is happening on the grid provides a better understanding of the threat landscape and attackers.

Cyber threat information could be utilized to develop a coordinated collective response to new threats. It could also reduce the chances of cascading effects across industries or sectors. With this information, stakeholders are able to reinforce resilience to cyberattacks and circulate best practices to better understand attack routes.

There are two different categories of cyber threat information: technical threat indicators and contextual threat intelligence. Technical threat indicators account for the majority of available threat information. They are specific, common and repeatable forms of data that are easy to anonymize, standardize and quickly distribute. Examples of technical threat indicators include Internet Protocol addresses, specific strings of data, file hashes and adversary techniques and procedures.

Contextual information is difficult to automate and requires human involvement. This type of intelligence includes target information, adversary courses of action and detailed data about the campaign and threat actor. This kind of information poses a risk to privacy, contractual liability and unauthorized disclosure of classified information.

Specific characteristics of threat data are necessary to ensure the intelligence is relevant and actionable for the public and private sectors. It is possible that shared cyber threat intelligence is false and could cause disruptions or damages. To prevent spreading bad information and causing harmful effects, the data must be checked for false errors and the source of the intelligence must be evaluated. Considering that threat data loses value the longer it is not used, the intelligence must be disseminated rapidly without losing quality. Thus, threat data that is needed to address present threats or vulnerabilities must be prioritized and quickly applied while other data may be less urgent.

Kiersten Todt, former executive director of a federal cybersecurity panel, expressed that "the challenge that we continue to have from the government is bulky data being distributed in a fire hose without context, without the narrative. None of this is valuable."[9] Information is valuable when it is relevant and actionable -- stakeholders need to be able to actually apply shared data specific to their networks. If the intelligence is not tailored, stakeholders would have to spend a lot of time and effort scrutinizing large amounts of data, draining resources and delaying the hardening of networks.[10]

RISKS OF DISTRIBUTING THREAT DATA

Sharing cyber threat information sounds easy, but is complicated due to legal and privacy issues.[11] The private sector is generally hesitant to share cyber threat intelligence because companies could be exposed to civil and criminal liability for disclosing sensitive personal or business material. The data could also damage a company's reputation and affect its stock price. In addition, sharing this information could be viewed as an admission of not protecting their network, and the intelligence could be used for regulatory actions or for law-enforcement and intelligence collection activities.

The 2015 Cybersecurity Information Sharing Act (CISA) provides companies with liability and other protections if all sharing requirements are followed. One requirement is removing personally identifying information. Some companies may be able to extract personal information easily from data prior to sharing, but others may need to do so manually. Unintended sharing of personally identifying information may result in the loss of protections under CISA.[12]

Some opponents of CISA question its intentions. Justin Harvey, Chief Security Officer of Fidelis Cybersecurity, declared last year that CISA was "meant to be a surveillance bill from the start," and lacked adequate privacy protections.[13] The Electronic Frontier Foundation stated that CISA does not fix any core privacy concerns.[14] For instance, the bill does not address problems related to past data breaches such as unencrypted files, poor computer architecture, servers that are not updated and staff clicking malware links. Organizations that oppose CISA include the American Civil Liberties Union, Apple, Symantec and Twitter.[15]

One way to decrease the risks of cyber threat intelligence is to share the data anonymously in a repository.[16] This might decrease the risk of a company disclosing sensitive personal or business information, relieving some private sector concerns. The stored information could also be made more valuable through utilizing analysis and aggregation to increase awareness about current and past cyber risks. The Department of Homeland Security is currently conducting a pilot that is exploring the utilization of a repository that stores voluntary information to identify cyber risks.[17]

THREAT INFORMATION SHARING IS NOT EFFECTIVE

The Department of Homeland Security and the Department of Energy manage several programs to enable cyber threat information sharing. Even though multiple programs exist, cyber threat information sharing has not been effective and is experiencing some major obstacles.

The Private Sector is Not Incentivized

One of the main challenges with cyber threat information sharing is that not everybody shares. Large organizations have the resources to do so, but smaller businesses do not. These small businesses tend to consume threat data without providing any intelligence in return. A second problem is that the government is "very good at receiving information, but not so good about sharing information back," according to Mark Weatherford, principal with security advisory firm The Chertoff Group.[18] A mechanism to motivate government to work with the private sector needs to be created.[19]

Technology industry executives and experts doubt cybersecurity information sharing will be effective because it is one-sided. Washington is focused on ensuring the private sector shares information with government, but there is not enough attention on ensuring the private sector receives quality threat data from the government. Alex Stamos, Yahoo's chief information security official, explained that his company often reports crimes to the government, but rarely receives information to identify attackers.[20] The government also classifies a lot of the data it collects, which makes it harder to share.

Large organizations have the resources to share, but smaller businesses do not. These small businesses tend to consume threat data without providing any intelligence in return.

> ***Because the government does not share valuable cyber threat data, the private sector is unlikely to share as much threat intelligence without an incentive.***

Retired General Keith Alexander, former commander of the United States Cyber Command, expressed that the four parties handling cyber issues, the Department of Homeland Security, Department of Defense, the Federal Bureau of Investigation and the intelligence community, are too "stove piped." These agencies hoard information instead of sharing it with other government agencies. According to General Alexander, "What you have is people acting independently, and with those seams, we will never defend this country."

Because the government does not share valuable cyber threat data, the private sector is unlikely to share as much threat intelligence without an incentive. Rick Howard, chief security officer of Palo Alto Networks, noted that the private sector would rather sell cyber threat data than share for free via voluntary government programs.[21] David Weinstein, New Jersey Chief Technology Officer, affirmed that the "government needs to play more of a role of incentivizing industry. If this [threat information sharing] is really going to be successful, industry needs to drive it..."[22]

Limitations of Government

General Alexander has noted that industry leaders are "dismayed" about how the government handles cybersecurity.[23] In April 2017, the National Cybersecurity and Communications Integration Center released an incident report about a sophisticated cyber campaign that used multiple malware implants.[24] A preliminary analysis found that threat actors used stolen administrative credentials and certificates and placed malware implants on critical systems. While such reports help victims take action, the campaign was found to be active since May 2016. Hence, the actors had at least an eleven-month head start by the time the report was released.

A cyberattack in June 2017 used a code known as "Eternal Blue," widely believed to have been stolen from the National Security Agency. This attack disrupted computers belonging to Russia's biggest oil company, Ukrainian banks and multinational firms. The Department of Homeland Security said it was monitoring attacks and coordinating with other countries, advising victims not to pay the extortion because access to files is not guaranteed.[25] Monitoring threats and releasing reports and notices about attacks are not sufficient protection against cyberattacks, as demonstrated by multiple incidents over the years. More effort needs to be made to find cyber threat actors and to deter them from launching an attack in the first place.

The government's lack of credibility when sharing cyber threat information is demonstrated by the Department of Homeland Security's and the Federal Bureau of Investigation's report on the hackers thought to be responsible for the Democratic National Committee intrusions in December 2016. The report was flawed, incomplete and technically inaccurate. For instance, it included several Internet Protocol addresses categorized as malicious, but further investigation found they were actually false alarms.[26]

The demand for relevant cyber threat data from private firms has created a public-private relationship that does not encourage sharing. For instance, the Cyber Information Sharing and Collaboration Program (CISCP) is located within the National Cybersecurity and Communications Integration Center of the Department of Homeland Security. CISCP allows public-private information sharing about cyber threats, incidents and vulnerabilities. However, this program has not seen much action because the private sector can pay cybersecurity firms such as FireEye, CrowdStrike and Symantec to acquire advanced intelligence gathering capabilities.[27]

Private Sector Is Able to "Cross the Last Mile"

Security experts agree that sharing threat data improves defenses. The Cyber Threat Alliance is a group of private sector companies, including Palo Alto Networks, Symantec, Intel Security, Check Point, Cisco and Fortinet, that has decided to take threat information sharing into their own hands. The alliance has published reports on ransomware and malware to strengthen cybersecurity.

Unlike the voluntary sharing for government programs, every member of the Cyber Threat Alliance is required to share information. Each affiliate must share at least 1,000 pieces of unique malicious code a day. If the minimum amount of information is not shared, the alliance holds its members accountable by sending notifications, discussing challenges and identifying issues to ensure future compliance.[28] Such accountability is currently lacking in government programs.

One benefit of private sector cyber threat information sharing is best demonstrated by its ability to "cross the last mile." The energy sector's Information Sharing and Analysis Center and the Multi-State Information Sharing and Analysis Center are helpful because they are largely dependent on existing relationships of trust within the electricity sector.[29]

However, these centers are unable to "cross the last mile" by updating networks to protect against cyber threats.[30] When threat data is received, staff needs time to read the report, identify what is relevant, formulate a response and then implement that response. This could take days, weeks or months to complete which means threat data will be almost irrelevant after so much time has passed.

Unlike information sharing and analysis centers, security vendors are able to automatically update their products to defend against cyber threats.

Unlike information sharing and analysis centers, security vendors are able to automatically update their products to defend against cyber threats. According to Howard, "We can take a new indicator of compromise, convert it into multiple prevention controls down the kill chain, and distribute it to 36,000 customers around the world in five minutes."[31] Howard also noted that other vendors have similar capabilities and cybersecurity could be boosted by pooling resources.

STATES NEED TO ENHANCE CYBERSECURITY EFFORTS

Cybersecurity efforts require staying ahead of technology, maintaining transparency and quickly sharing information. While it is impossible to fund and protect the grid from every cyber threat, efforts are being made to prevent incidents from having devastating impacts.[32]

Protect the Distribution System

At this time, cybersecurity standards exist for the bulk power system of the grid, but are lacking for the distribution system operated by utilities. This is the final stage where electricity is delivered to customers. Two exercises conducted by the financial and energy industries, Quantum Dawn 2[33] and GridEx II,[34] have demonstrated the need for improved communication and sharing of cyber threat information on the distribution system.

The Federal Energy Regulatory Commission (FERC) manages the reliability and cybersecurity standards for the bulk power system. This includes facilities and control systems necessary for operating an interconnected grid and electric energy from generation facilities needed to maintain transmission system reliability. Investor-owned utilities are typically operated under the jurisdiction of the state public utility commissions (PUCs), outside of FERC authority. Hence, cybersecurity standards exist for one part of the grid but not the other.

Utilities should be required to conduct a risk analysis to better understand their cybersecurity weaknesses.[35] This will allow for clear cybersecurity goals, informed decision-making and the identification of steps to reduce threats. Since utilities are decentralized, conducting a risk assessment for each will be challenging. For example, a utility may own multiple power plants and control centers in different states.

A centralized committee in each state tasked with aggregating and sharing threat data across the enterprise needs to be created.[36] This would streamline the state risk assessment process and serve as a central hub for threat information. Periodic cyber intrusion scenario drills conducted with the private sector could help stress test response plans and communicate protocols.

Some PUCs are reluctant to gather information about utilities' cybersecurity weaknesses because they fear that they could be held responsible if sensitive information is publicly disclosed. "There's liability for discovering vulnerabilities and not doing something about them — which is difficult, given the level of complexity and the lack of quick fixes," said Bryson Bort, chief executive officer of GRIMM. Laws need to be implemented to protect this type of data from public disclosure. Additionally, PUCs need trained staff able to assess the security postures of utilities and understand their unique risks.

After a risk analysis is conducted, PUC commissioners then need to determine whether utilities are making sufficient investments in cybersecurity and whether those assets are properly prioritized. Because the threat environment is constantly evolving, comprehensive assessments of cyber incidents on the grid need to be conducted continuously.

Lawmakers should require standard performance criteria to ensure utilities are protected from cyber threats.[37] Funding could be provided to implement the standards, but partnering with the private sector should also be encouraged to identify creative ways for cost-effective implementation. Stakeholders must be cautious when creating standards because they may take a while to develop. This means they may not be able to protect against the latest threats. In addition, distribution employees must be trained and accredited to enhance cybersecurity.

According to Agnes Kirk, Washington's Chief Information Security Officer, "States need to figure out the best way to share cyber threat information with utilities. Smaller utilities often don't have the expertise needed to understand and act on threat information. Plus, this type of intelligence is often classified, which means only a few large power utilities and government personnel have the needed clearances. Yet such intelligence is critical to defend against cyber threats. We have to get this right, and do so quickly."

Though the Federal Department of Energy and the Department of Homeland Security offer grants to fund cybersecurity efforts, such funds are limited. Utilities should seek private investors to create revenue streams to fund cybersecurity projects. Updating energy infrastructure could also result in savings that may be applied to enhance cybersecurity measures. In addition, rates could also be reasonably increased to ensure electricity delivery is secure.

Utilities Actively Protecting Against Cyber Threats

Utilities in some states are taking action to protect against cyber threats. Utilities in New Jersey are required to develop programs and procedures to identify and mitigate cyber risks, report incidents and suspicious activity, create incident response and recovery plans and provide training programs.[38]

In Pennsylvania, utilities are required to maintain physical and cybersecurity, emergency response and business continuity plans, and report cyber and physical attacks that cause more than $50,000 in damages. In Texas, the public utilities commission conducts annual security audits.

Baltimore Gas and Electric in Maryland conducts regular drills and shares information related to cyber threats it encounters with industry and government partners. Duke Energy based in North Carolina has a corporate incident response team and security professionals devoted to cybersecurity 24 hours a day. Duke Energy works closely with emergency management and law enforcement agencies on the local, state and national levels following cybersecurity incidents.[39]

Other states including Idaho, North Dakota, Rhode Island, Virginia and Texas have established state-specific efforts to assess cybersecurity infrastructure, recommend ways to enhance the resiliency of government operations and promote the growth of their cybersecurity industry and workforce.[40] Perhaps such actions could be adopted by more states to protect against cyber threats on the grid.

Develop Actionable Mandates

Governors and state legislators ought to work together to develop actionable mandates for PUCs. These commissions need to take a strong stance on cybersecurity protection, and could spur some utilities to boost cybersecurity efforts. This is because PUCs decide what percentage of profits some utilities can keep, and authorize which investment costs can be passed on to consumers.

Chief information officers and chief information security officers should collaborate more with industry, utility regulators and other government organizations to anticipate and understand emerging cyber threats that could affect the grid.[41] This would open lines of communication and allow better forecasting of future threats.

Cyber Breaches Must Be Thoroughly Studied

According to U.S. Representative John Ratcliffe, chairman of the Cybersecurity and Infrastructure Protection Subcommittee, "In the cyber domain, we are constantly learning new lessons, and it is only by incorporating that knowledge into existing programs and processes that we can continue to move towards greater collaboration and better secured networks."[42]

Once a cyber threat or attack is handled, the public and private sectors must find ways to protect themselves from future incidents. Implementing lessons learned from cyber breaches could help organizations better prepare and defend networks and respond to attacks. This would also encourage internal and external partners to engage across organizations and supply chains.[43]

Automated Information Sharing

Automating the cyber threat information process would allow states to quickly analyze and distribute intelligence in a cost-effective manner. This would enable quicker notifications to be sent and received when the grid experiences unusual activity. Automated threat information would also allow for greater situational awareness on the grid and would free staff to focus on other critical tasks such as planning, research and data analysis.[44]

Intelligence collected via an automated information sharing process could be used for other purposes, such as to identify different types of attacks. The data could also be used to notify relevant sub networks and systems and to develop an appropriate response when a cyber threat is detected. Automating cyber threat information could allow for an almost instantaneous security response, reducing outages, minimizing grid disruptions and improving recovery times.

Understanding the value of automated cyber information sharing, the California Public Utilities Commission funded the Machine to Machine Automated Threat Response (MMATR). This is part of a cooperative research and development program called California Energy Systems for the 21st Century (CES-21). MMATR will develop advanced cyber technology and tools that investor-owned utilities could use to identify and respond to threats before damage occurs to critical infrastructure. The program aims to improve warning capabilities, execute appropriate responses and identify deterrence strategies.

MMATR could be applied to existing supervisory control and data acquisition control systems to protect from cyber harm. These systems obtain measurements to estimate the operational state of the power grid and help make informed decisions with real-time indications of grid instabilities. MMATR will also explore new cybersecurity defensive technology with advanced threat analytics such as machine learning, algorithms and software analysis.[45]

According to Jamie Van Randwyck, project lead for Lawrence Livermore National Laboratory, "The CES-21 program has been a highly productive and collaborative initiative thus far. The research and development being pursued in this program has the potential to change the way utilities protect their critical assets." More public utilities commissions should consider funding automated cyber information programs in other states to support the cyber threat intelligence and response process.

NATIONAL GUARD EFFORTS TO COUNTER CYBER THREATS

The National Guard has unique authorities, responsibilities and capabilities to help defend the grid against cyber threats. The National Guard could be activated by governors for a large-scale emergency or disaster that may result from a successful cyberattack on the grid.[46] In a letter written this year to Senator Joni Ernst of Iowa, who chairs the Emerging Threats and Capabilities Subcommittee, Admiral Mike Rogers, director of the National Security Agency and commander of the U.S. Cyber Command, confirmed that the National Guard is boosting its capabilities to protect against cyber threats. States should work with their National Guard units to prepare, respond and protect the grid from cyber threats.

National Guard cyber units in California, Maryland, Wisconsin and Washington have established collaborative relationships with local utilities. In some cases, the National Guard units and utilities have conducted joint exercises. The National Guard has also been active internationally through the National Guard State Partnership Program, which matches a state with a partner nation's security forces to train on joint cyber defense efforts.[47] Cooperative cybersecurity trainings have taken place with North Dakota and Ghana, Colorado and Jordan and New Jersey and Albania to develop a reserve cyber capability and strengthen cyber defense capabilities by sharing information.[48]

A 2016 Government Accountability Office report found that the National Guard has been actively utilizing its capabilities to support civil authorities in a cyber incident.[49] However, the Department of Defense is not aware of units' capabilities because the cyber expertise of the National Guard is not monitored. The Department of Defense should track National Guard units' cyber capabilities so that organized action could be implemented in the event a successful cyberattack shuts down large parts of the grid. To better understand the options of cyber support available in the Guard, Senator Ernst has introduced a bill that would require the Department of Defense to track the National Guard's cyber expertise in an existing database.[50]

Some question the dependence on the National Guard to prepare and respond to grid cyber incidents. Michael Hamilton, a former chief information security officer for Seattle and chief executive officer at Critical Informatics, a cybersecurity firm, warned that a precedent may hinder efforts from other stakeholders. According to Hamilton, "These organizations, go 'Well, we don't have to invest in controls because the government is going to come take care of it for us.'"[51] The National Guard could participate in defending and responding to a cyberattack, but other stakeholders need to do their part too.

PRIVATE SECTOR SOLUTIONS TO AUGMENT CYBERSECURITY

Cybersecurity is one of the most serious challenges the grid faces, according to Patricia Hoffman, former assistant secretary for the Department of Energy's Office of Electricity Delivery and Energy Reliability.[52] Hoffman believes cutting edge technologies are essential to help the energy sector adapt to the evolving landscape. The research firm Zpryme estimates that U.S. utilities will spend $7.25 billion on grid cybersecurity by 2020. Hence, the global cybersecurity market for the grid will expand.

The National Institute of Standards and Technology recently released a report that identified commercially available products that increase situational awareness on the grid.[53] Situational awareness is particularly important to cybersecurity due to the unpredictability of cyber incidents. Some providers of smart grid cybersecurity include VeriSign, Raytheon, ViaSat Inc., Leidos, Kingfisher, BAE Systems and IBM.[54]

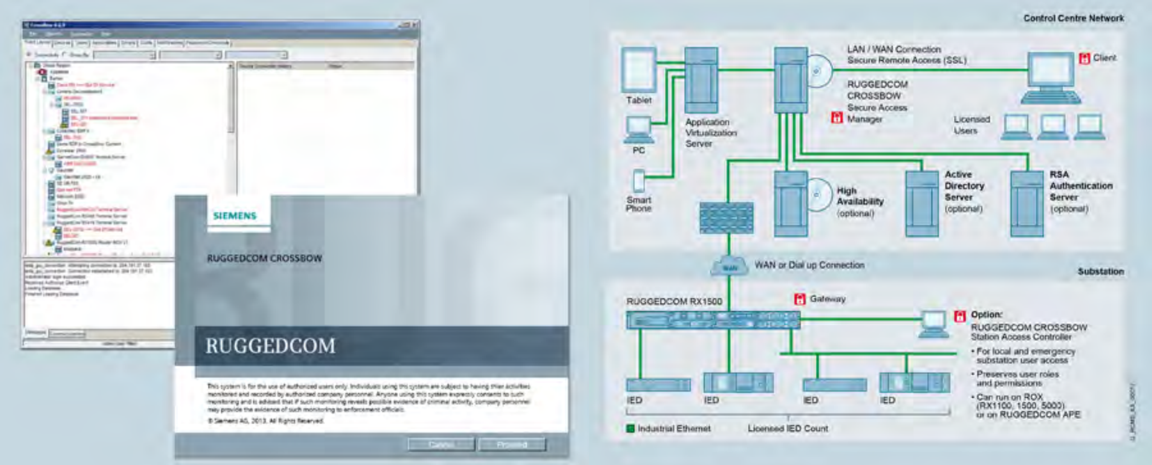
Specific products that could help with situational awareness on the grid are Siemens' Ruggedcom Crossbow, Dragos' Security CyberLens, Cisco's 2950 (Aggregator) and Belden's Tofino Security. The National Institute of Standards and Technology found that these solutions can be integrated with existing infrastructure within a utility's network to boost situational awareness.

U.S. utilities will spend $7.25 billion on grid cybersecurity by 2020, according to research firm Zpryme.

The Sierra Nevada Corporation has created Binary Armor that provides bidirectional security for communication layers on the grid by setting tailored rules for specific messages allowed to enter the network. Utilidata and Raytheon have also partnered to combine their expertise with real-time data to detect and respond to cyberattacks on the grid.[55] Massachusetts Institute of Technology, Raytheon, Boeing, BAE Systems and other companies have also created a team to launch a cybersecurity initiative aimed at keeping digital information safe from cyber threats.[56]

General Electric Renewable Energy provides cybersecurity for Invenergy's nearly-10 gigawatt fleet of wind turbines. Wurldtech will enhance Invenergy's legacy controls, upgrading and protecting the wind turbine network's security with the company's Opshield. GE and Wurldtech will also provide Invenergy's fleet with software maintenance, updates and patches.[57] The agreement is worth more than $13 million over ten years and is one of the largest cybersecurity deals to date. More private sector companies should ensure their products are safe from cyber threats.

The Defense Advanced Research Projects Agency (DARPA) has awarded several contracts to prevent and respond to cyberattacks. Vencore Labs, Inc. is developing a system that continuously executes anomaly detection algorithms to provide early warning, spoofing detection and situational awareness. Vencore Labs is developing a capability to localize



This system is for the use of authorized users only. Individuals using this system are subject to having their activities monitored and recorded by authorized company personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, company personnel may provide the evidence of such monitoring to enforcement officials.

© Siemens AG, 2013. All Rights Reserved.

SIEMENS
RUGGEDCOM CROSSBOW
RUGGEDCOM
Cancel
Proceed
Control Centre Network
Tablet
PC
Smart Phone
Application Virtualization Server
LAN / WAN Connection Secure Remote Access (SSL)
RUGGEDCOM CROSSBOW Secure Access Manager
Client
Licensed Users
High Availability (optional)
Active Directory Server (optional)
RSA Authentication Server (optional)
WAN
WAN or Dial up Connection
Substation
RUGGEDCOM RX1500
Gateway
Option:
RUGGEDCOM CROSSBOW Station Access Controller
• For local and emergency substation user access
• Preserves user roles and permissions
• Can run on ROX (RX1100, 1500, 5000) or on RUGGEDCOM APE
IED
IED
IED
IED
🟩 Industrial Ethernet
Licensed IED Count

Situational awareness provides a better understanding of the cyber threat landscape and attackers. One product that could help obtain knowledge about what is happening on the grid is Siemens' Ruggedcom Crossbow. (Published with permission from Siemens)

and characterize malicious software that has penetrated critical utility systems. This will be able to map industrial control systems, gather and analyze configuration data, determine which devices are behaving incorrectly and characterize malware to help restart operations.[58]

Raytheon is creating products that provide warnings of possible cyberattacks and identifies power grid data collection and communication issues. The company will also review how to maintain emergency communication networks after a cyberattack has occurred. In addition, collaborators at the University of California, Berkeley and Lawrence Berkeley National Laboratory have produced sensors that look for irregularities in the physical behavior of the grid and boost situational awareness to protect from a cyberattack.[59]

The private and public sectors must work together to develop effective solutions to counter cyber threats to the grid. The private sector has a track record of developing results and the electricity sector needs to continue working with such partners to prevent data loss and power outages from a cyberattack.[60] According to Scott Montgomery, vice president and chief technical strategist of Intel, the challenges cyber faces today are too large for one company to fight alone. "Cyber defense initiatives peak shortly after release and degrade quickly thereafter. No one company or entity can have a catch-all infrastructure to combat that."[61]

RESPONDING TO A CYBER INCIDENT

In the event of a cyber incident, systems connected to the Internet would need to be isolated and maybe even shut down to prevent the attack from spreading. DARPA has created a program called Rapid Attack Detection, Isolation and Characterization Systems (RADICS) to create a secure emergency network to connect power suppliers after a cyberattack.[62] Products developed as a result of RADICS could be shared with Cyber Command, Industrial Control Systems Cyber Emergency Response Team, National Guard Cyber Protection Units, the Army Corps of Engineers and commercial cybersecurity firms to boost protection of the U.S. electric grid.

Raytheon is reviewing processes for emergency communication networks to assist the rapid connection of important organizations after a successful cyberattack has occurred. An emergency network would be useful in locations where Internet infrastructure may not be working or if hackers were to embed malicious code in information technology systems belonging to utilities.

While utilities lack experience in responding to a successful cyberattack, they do have useful procedures to prepare for storms and natural disasters. When utilities expect a weather incident on the horizon, they increase the number of customer service staff to handle an influx of calls. Utilities also have preexisting arrangements with suppliers to obtain equipment in a matter of hours after a storm, and have contracts and processes in place to accept storm crews and equipment from other utilities around the country to assist with repairs. Such detailed preparation and planning also must be done in case of a cyber crisis.[63]

OTHER IMPROVEMENTS TO PROTECT THE ELECTRIC GRID

Bidirectional sharing of cyber threat information between the energy sector and the government helps determine the severity and nature of threats and assists with rapidly developing solutions. Cyber threat intelligence sharing is an important step in improving defenses, but it is not sufficient to protect the grid.

Currently, there is no proactive way to identify and find cyber criminals.

Jamil Jaffer, director of the Homeland and National Security Law Program at the George Mason University Antonin Scalia Law School, told the U.S. House of Representatives Small Business Committee in July that Americans need to have a national debate about who is in charge of providing for the grid's common defense in cyberspace, commerce and other critical sectors.[64] To avoid confusion and duplicate efforts, there needs to be clear organization as to who is responsible for what when defending against and responding to a cyberattack.

While sharing cyber threat data is a form of defending against cyber risks, an offense strategy is lacking. Currently, there is no proactive way to identify and find cyber criminals. Former Secretary of Homeland Security Michael Chertoff supports the creation of international standards to locate cybercriminals and prevent bad actors from conducting future harm.[65] International cooperation is needed to develop such standards because cyber threats affect companies and governments around the world.

The Heritage Foundation has suggested that the private sector utilize active cyber defenses of their networks.[66] If the government is unable or unwilling to threaten credible actions to deter cyberattacks or punish those who conduct them, the private sector may want to "hack-back" and take measures beyond software, firewalls and passive screening methods.

Another novel idea to identify weaknesses in the electric grid is to reward hackers that find cybersecurity exploits through a program similar to the Department of Defense's "Hack the Pentagon."[67] According to Richard Ledgett, the National Security Agency's former deputy director, "I think a bug bounty can be a good thing, if it's done well. The Department of Defense did it last year, and was pretty successful." However, there are substantial access and skill set differences between the Department of Defense hacking web applications and industrial control systems and supervisory control and data acquisition systems on the grid. Implementing such a program will likely require some physical access to the grid.

CONCLUSION

A successful cyberattack on the U.S. electric grid is possible. Russia has a well-resourced central cyber command. China is especially active in cyber as well, utilizing viruses and botnets to access targets. Iran also uses its cyber program against political enemies to collect intelligence, but is less advanced than Russia and China. Cyberattacks to the power grid are increasing in frequency, speed and sophistication, and have the potential to disrupt and destroy critical infrastructure.

Partners need to be able to communicate and share cyber threat information in a fast and consistent manner and respond to an attack before harm occurs. To do so effectively, the government needs to do a better job of sharing information and the private sector must be incentivized to share cyber threat data.

It is time for all states to take cyber protection of the grid seriously. Cybersecurity requirements need to be implemented for the distribution system of the grid operated by utilities. Public utilities commissions must require utilities in their jurisdiction to protect against cyber threats so that customer access to electricity is not at risk. States should focus on tailoring cyber threat information to fit their unique needs and automate the process to increase accuracy and speed for less cost. National Guard units in each state should also be trained to prepare, respond and protect against grid cyber threats.

If sharing cyber threat information is done effectively, it could reduce risks and enhance the overall resilience of the grid. Furthermore, threat information could reduce the effectiveness of any one cyber threat or attack by informing other partners to protect against it. U.S. policy leaders need to guard the electric grid from cyber threats to ensure that power is not shut down as it was in Ukraine.

REFERENCES

1 “Global Cyberattack Underscores Need to Strengthen U.S. Electric Grid.” *PR Newswire*, May 16, 2017. http://www.prnewswire.com/news-releases/global-cyberattack-underscores-need-to-strengthen-us-electric-grid-300458810.html (accessed May 7, 2017).

2 “Potential Risks and Rewards of Cybersecurity Information Sharing Under CISA.” *Lexology*, July 21, 2016. http://www.lexology.com/library/detail.aspx?g=9735c48c-efaa-49d6-baae-e629e63f47cb (accessed June 7, 2017).

3 Denise E. Zheng and James A. Lewis. “Cyber Threat Information Sharing.” *Center for Strategic and International Studies*, March, 2015. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf (accessed June 20, 2017).

4 “To Counter Systemic Cyber Threats, Share Information,” *CIO Journal*. Wall Street Journal, March 9, 2015. http://deloitte.wsj.com/cio/2015/03/09/to-counter-systemic-cyber-threats-share-information/ (accessed June 15, 2017).

5 “Cybersecurity of the Power Grid: A Growing Challenge.” *U.S. News*, February 24, 2017. https://www.usnews.com/news/national-news/articles/2017-02-24/cybersecurity-of-the-power-grid-a-growing-challenge (accessed June 21, 2017).

6 “Smart Grid Cyber Security Market Analysis, Development, Growth and Demand Forecast to 2025.” *Digital Journal*, June 14, 2017. http://www.digitaljournal.com/pr/3381292#ixzz4k1z1CObB (accessed June 25, 2017).

7 Juliet Eilperin and Adam Entous. “Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say.” *Washington Post*, December 31, 2016. https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.c70e9d34e8f9 (accessed January 20, 2017).

8 Rebecca Smith. “Cyberattacks Raise Alarm for U.S. Power Grid.” *Wall Street Journal*, December 30, 2016. http://www.wsj.com/articles/cyberattacks-raise-alarms-for-u-s-power-grid-1483120708 (accessed January 5, 2017).

9 Sean D. Carberry. “Why government should let industry drive cybersecurity.” *FWC*, June 30, 2017. https://fcw.com/articles/2017/06/30/todt-cyber-private-carberry.aspx (accessed July 10, 2017).

10 Dwight Davis. “Threat intelligence today.” *CSO*, May 4, 2017. http://www.csoonline.com/article/3194370/data-breach/threat-intelligence-today.html (accessed June 20, 2017).

11 Mueller, Liebert, and Heyworth. “Keeping the Lights On.” April, 2017.

12 “Potential Risks and Rewards of Cybersecurity Information Sharing Under CISA.” July 21, 2016.

13 Taylor Amerding. “Information sharing still a heavy lift.” *CSO*, October 6, 2016. http://www.csoonline.com/article/3128745/security/information-sharing-still-a-heavy-lift.html#tk.cso-infsb (accessed April 7, 2017).

14 Taylor Amerding. “Information sharing bill passes, but privacy debate goes on.” *CSO*, January 14, 2016. http://www.csoonline.com/article/3021907/security/information-sharing-bill-passes-but-privacy-debate-goes-on.html (accessed February 10, 2017).

15 Marc Jaycox. “EFF Opposes CISA as Final Vote Approaches.” *Electronic Frontier Foundation*, October 27, 2015. https://www.eff.org/deeplinks/2015/10/eff-opposes-cisa-final-vote-approaches (accessed May 21, 2017).

16 Department of Homeland Security, *Enhancing Resilience Through Cyber Incident Data Sharing and Analysis*, June 2015. https://www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015_v2.pdf (accessed June 20, 2017).

17 Matt Leonard. “DHS preps Cyber Incident Data Repository.” GCN, April 24, 2017. https://gcn.com/articles/2017/04/24/cyber-incident-data-repository.aspx (accessed (July 7, 2017).

18 Sara Sorcher. “Security pros: Cyberthreat info-sharing won’t be as effective as Congress thinks.” *The Christian Science Monitor*, June 12, 2015. https://www.csmonitor.com/World/Passcode/2015/0612/Security-pros-Cyberthreat-info-sharing-won-t-be-as-effective-as-Congress-thinks (accessed June 22, 2017).

19 Carberry, “Why government should let industry drive cybersecurity,” June 30, 2017.

20 Sara Sorcher, “Security pros: Cyberthreat info-sharing won’t be as effective as Congress thinks,” June 12, 2015.

21 Rob Wright. “Q&A: How the Cyber Threat Alliance solved threat intelligence sharing.” *TechTarget*, June 30, 2017. http://searchsecurity.techtarget.com/news/450421801/QA-How-the-Cyber-Threat-Alliance-solved-threat-intelligence-sharing (accessed July 9, 2017).

22 Carberry, “Why government should let industry drive cybersecurity,” June 30, 2017.

[23] Morgan Chalfant. "Ex-NSA head: Cybersecurity agencies don't share enough information to be successful." *The Hill*, March 2, 2017. http://thehill.com/policy/cybersecurity/322061-ex-nsa-head-agencies-too-stove-piped-to-be-successful-on-cybersecurity (accessed March 16, 2017).

[24] Department of Homeland Security, United States Computer Emergency Readiness Team, *Intrusions Affecting Multiple Victims Across Multiple Sectors*, April 27, 2017. https://www.us-cert.gov/sites/default/files/publications/IR-ALERT-MED-17-093-01C Intrusions_Affecting_Multiple_Victims_Across_Multiple_Sectors.pdf (accessed June 27, 2017).

[25] "Hackers strike across Europe, sparking widespread disruption." *CNBC*, June 27, 2017. http://www.cnbc.com/2017/06/27/hackers-strike-across-europe-sparking-widespread-disruption.html (accessed July 10, 2017).

[26] Chris Bing. "Why businesses ignore the U.S. government's information sharing programs." *Cyberscoop*, January 31, 2017. https://www.cyberscoop.com/information-sharing-cybersecurity-dhs-private-sector/ (accessed May 17, 2017).

[27] Chris Bing, "Why businesses ignore the U.S. government's information sharing programs," January 31, 2017.

[28] Rob Wright, "Q&A: How the Cyber Threat Alliance solved threat intelligence sharing," June 30, 2017.

[29] Zheng and Lewis, "Cyber Threat Information Sharing," March, 2015.

[30] Rob Wright, "Q&A: How the Cyber Threat Alliance solved threat intelligence sharing," June 30, 2017.

[31] Rob Wright, "Q&A: How the Cyber Threat Alliance solved threat intelligence sharing," June 30, 2017.

[32] "Electric industry says protecting electric grid from cyberattacks top priority." *Daily Energy Insider*, February 2, 2017. https://dailyenergyinsider.com/featured/3164-electric-industry-says-protecting-electric-grid-cyberattacks-top-priority/ (accessed May 15, 2017).

[33] "Quantum Dawn 2 A simulation to exercise cyber resilience and crisis management capabilities." *Deloitte*, October 21, 2013. http://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-quantum-dawn-2-report-102213.pdf (Accessed May 22, 2017).

[34] North American Electric Reliability Corporation, Grid Security Exercise *GridEx III Report*, March 2016. http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20After%20Action%20Report.pdf (accessed June 27, 2017).

[35] Mueller, Liebert, and Heyworth, "Keeping the Lights On," April, 2017.

[36] "Preparing Utilities to Respond to Cyber Attacks," *CIO Journal*. Wall Street Journal, October 11, 2013. http://deloitte.wsj.com/cio/2013/12/11/preparing-utilities-to-respond-to-cyber-attacks/ (accessed May 22, 2017).

[37] Cybersecurity and the North American Electric Grid: New Policy Approaches to Addressing the Threat." *Bipartisan Policy Center*, February, 2014. http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf (accessed June 20, 2017).

[38] "New Jersey utility board approves cybersecurity measures," Associated Press. *Daily Record*, May 19, 2016. http://www.dailyrecord.com/story/news/local/2016/03/19/new-jersey-utility-board-approves-cybersecurity-measures/82009708/ (accessed February 7, 2017).

[39] Bridge Tower. "Lights on: Utilities power up cyberattack preparations." *Finance and Commerce*, May 30, 2017. http://finance-commerce.com/2017/05/lights-on-utilities-power-up-cyberattack-preparations/ (accessed June 10, 2017).

[40] Francesca Spidalieri. "State Of The States On Cybersecurity." *Pell Center*, November, 2015. http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf (accessed June 20, 2017).

[41] "NIST Cyber Security Framework: 4 Steps for CIOs," *CIO Journal*. Wall Street Journal, January 14, 2015. http://deloitte.wsj.com/cio/2014/01/14/nist-cyber-security-framework-4-steps-cios-can-take-now/ (accessed January 10, 2017.

[42] Debra Flax. "DHS private sector cooperation necessary for success of nation's cybersecurity efforts." *Homeland Preparedness News*, March 10, 2017. https://homelandprepnews.com/featured/21479-dhs-private-sector-cooperation-necessary-success-nations-cybersecurity-efforts/ (accessed May 20, 2017).

[43] Kacy Zurkus. "Collaborative defense, the shift from 'what' to 'how.'" CSO, November 3, 2016. http://www.csoonline.com/article/3138544/security/collaborative-defense-the-shift-from-what-to-how.html (accessed June 7, 2017).

[44] "Lucrative Ransomware Attacks: Analysis of the Cryptowall Version 3 Threat."

[45] State of California Public Utilities Commission, *California Energy Systems for the 21st Century Proposed Research and Development Projects and Cooperative Research and Development Agreement*, November 14, 2014. https://www.pge.com/nots/rates/tariffs/tm2/pdf/ELEC_4402-E.pdf (accessed May 7, 2017).

[46] Heather Kuldell. "Ohio Taps National Guard Cyber Unit To Help Secure Elections." *Nextgov*, November 3, 2016. http://www.nextgov.com/cybersecurity/2016/11/ohio-taps-national-guard-cyber-unit-help-secure-elections/132908/ (accessed April 5, 2017).

[47] Emefa Addo Agaw. "The Major Component Missing From Trump's Executive Order on Cybersecurity." *Slate*. http://www.slate.com/articles/technology/future_tense/2017/06/trump_s_cybersecurity_executive_order_ignored_the_important_roles_state.html (accessed July 7, 2017).

[48] Department of Defense, *The State Partnership Program FY 2015 Annual Report to Congress*. http://www.nationalguard.mil/Portals/31/Documents/J-5/InternationalAffairs/StatePartnershipProgram/FY15%20SPP%20Annual%20Report.pdf (accessed June 10, 2017).

[49] U.S. Government Accountability Office, *DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises*, September 6, 2016. http://www.gao.gov/products/GAO-16-574 (accessed May 7, 2017).

[50] "Bill Notes National Guard Cyber Skills." *The National Guard Association of the U.S.*, February 7, 2017. http://www.ngaus.org/newsroom/news/bill-notes-national-guard-cyber-skills (accessed May 7, 2017).

[51] Aryn Braun, Siri Bulusu, Xiumei Dong, Katherine Lonsdorf, Patrick Martin, Steven Porter and Thomas Vogel. "Who Is Guarding the Grid?" *U.S. News*, September 23, 2016. https://www.usnews.com/news/articles/2016-09-23/is-the-energy-grid-in-danger (accessed June 6, 2017).

[52] David J. Unger. "Illinois partnership looks to build trust in grid through cybersecurity research." *Midwest Energy News*, June 12, 2017. http://midwestenergynews.com/2017/06/12/illinois-partnership-looks-to-build-trust-in-grid-through-cybersecurity-research/ (accessed July 1, 2017).

[53] National Institute for Standards and Technology, *Situational Awareness For Electric Utilities*, February, 2017. https://nccoe.nist.gov/sites/default/files/library/sp1800/es-sa-nist-sp1800-7-draft.pdf (accessed June 7, 2017).

[54] "Smart Grid Cyber Security Market Analysis, Development, Growth and Demand Forecast to 2025." *Digital Journal*, June 14, 2017. http://www.digitaljournal.com/pr/3381292#ixzz4k1z1CObB (accessed June 7, 2017).

[55] "Raytheon, Utilidata To Deliver Defense-Grade Cybersecurity For Utilities." *Raytheon*, February 8, 2017. http://investor.raytheon.com/phoenix.zhtml?c=84193&p=irol-newsArticle&ID=2244383 (accessed July 2, 2017).

[56] "MIT, Raytheon Band Together for Cybersecurity Research." *Raytheon*, March 5, 2015. http://www.raytheon.com/news/feature/mit_csail.html (accessed May 27, 2017).

[57] Joshua S. Hill. "GE Renewable Energy To Provide Cyber Security For Invenergy Wind Turbine Fleet." *Clean Technica*, May 26, 2017. https://cleantechnica.com/2017/05/26/ge-renewable-energy-provide-cyber-security-invenergy-wind-turbine-fleet/ (accessed June 7, 2017).

[58] "Vencore Labs to Assist DARPA in Protecting the Nation's Electrical Grid." *Vencore*, September 13, 2016. http://www.vencore.com/news/2016/9/12/vencore-labs-to-assist-darpa-in-protecting-the-nations-electrical-grid (accessed June 20, 2017).

[59] Peter Fairley. "Sniffing Out Grid Attacks." *IEE Spectrum*, July 22, 2016. http://spectrum.ieee.org/energy/the-smarter-grid/sniffing-out-grid-attacks_(June 10, 2017).

[60] "Preparing Utilities to Respond to Cyber Attacks," October 11, 2013.

[61] Debra Flax, "DHS private sector cooperation necessary for success of nation's cybersecurity efforts," March 10, 2017.

[62] Dr. John Everett, Defense Advanced Research Projects Agency, *Rapid Attack Detection, Isolation and Characterization Systems (RADICS)*, http://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems (accessed June 7, 2017).

[63] "Preparing Utilities to Respond to Cyber Attacks," October 11, 2013.

[64] U.S. Congress, "House Small Business Committee Hearings and Meetings Video," July 6, 2016. https://www.congress.gov/committees/video/house-small-business/hssm00/HXYa8-B-oKU (accessed June 25, 2017).

[65] David Gernon. "Cyberthreats require global response, said ex-DHS head Chertoff." *CNBC*, June 27, 2017. http://www.cnbc.com/2017/06/27/cyberthreats-require-global-response-ex-dhs-head-michael-chertoff.html (accessed June 1, 2017).

[66] Paul Rosenzweig, Steven P. Bucci, PhD, and David Inserra. "Next Steps for U.S. Cybersecurity in the TrumpAdministration: Active Cyber Defense." *The Heritage Foundation*, May 5, 2017. http://www.heritage.org/sites/default/files/2017-05/BG3188.pdf (accessed June 15, 2017).

[67] Jared Serbu. "DoD plans expansion of government's first-ever 'bug bounty.'" *Federal News Radio*, June 20, 2016. https://federalnewsradio.com/dod-reporters-notebook-jared-serbu/2016/06/dod-plans-expansion-governments-first-ever-bug-bounty/ (accessed June 10, 2017).

Future of the Power Grid Series

Supported by the Severns Family Foundation

1. *Keeping the Lights On: How Electricity Policy Must Keep Pace with Technology*, Don Soifer and Daniel Goure, July 2014

2. *Challenges and Requirements for Tomorrow's Electrical Power Grid*, J. Michael Barrett, June 2016

3. *Connecting Microgrids With Public-Private Partnerships To Meet Critical Needs,* J. Michael Barrett, September 2016

4. *California Aims To Incentivize Utilities To Adopt Third-Party Energy Resources,* Constance Douris, March 2017

5. *Balancing Smart Grid Data and Consumer Privacy,* Constance Douris, June 2017

6. *Cyber Threat Data Sharing Needs Refinement,* Constance Douris, August 2017

ABOUT THE AUTHOR

Constance Douris is Vice President of the Lexington Institute. Her current research interests include the electric grid and cyber security. Douris has been interviewed, published or quoted by various news outlets including the Associated Press, *New York Times*, *Washington Post*, and *The National Interest*. Douris has a Master and Bachelor of Arts in political science from California State University, Fullerton.

August 2017

Lexington Institute

1600 Wilson Boulevard, #203
Arlington, VA 22209

Telephone: 703-522-5828
Web: www.lexingtoninstitute.org
mail@lexingtoninstitute.org