Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector

Mission Support Center Analysis Report

Prepared by:

Mission Support Center

Idaho National Laboratory

August 2016

Disclaimer

OSTI # 1337873 **INL/EXT-16-40692**

Executive Summary

With utilities in the U.S. and around the world increasingly moving toward smart grid technology and other upgrades with inherent cyber vulnerabilities, correlative threats from malicious cyber attacks on the North American electric grid continue to grow in frequency and sophistication.[1] The potential for malicious actors to access and adversely affect physical electricity assets of U.S. electricity generation, transmission, or distribution systems via cyber means is a primary concern for utilities contributing to the bulk electric system. This paper seeks to illustrate the current cyber-physical landscape of the U.S. electric sector in the context of its vulnerabilities to cyber attacks, the likelihood of cyber attacks, and the impacts cyber events and threat actors can achieve on the power grid. In addition, this paper highlights utility perspectives, perceived challenges, and requests for assistance in addressing cyber threats to the electric sector.

There have been no reported targeted cyber attacks carried out against utilities in the U.S. that have resulted in permanent or long term damage to power system operations thus far, yet electric utilities throughout the U.S. have seen a steady rise in cyber and physical security related events that continue to raise concern. Asset owners and operators understand that the effects of a coordinated cyber and physical attack on a utility's operations would threaten electric system reliability[2]–and potentially result in large scale power outages. Utilities are routinely faced with new challenges for dealing with these cyber threats to the grid and consequently maintain a set of best practices to keep systems secure and up to date.

Among the greatest challenges is a lack of knowledge or strategy to mitigate new risks that emerge as a result of an exponential rise in complexity of modern control systems.[3] This paper compiles an open-source analysis of cyber threats and risks to the electric grid, utility best practices for prevention and response to cyber threats, and utility suggestions about how the federal government can aid utilities in combating and mitigating risks.

Among the findings of this paper, several key elements are:

- **Growth of networks and communication protocols used throughout ICS networks pose vulnerabilities** that will continue to provide attack vectors that threat actors will seek to exploit for the foreseeable future. The interoperable technologies created for a shift toward a smart grid will continue to expand the cyber attack landscape.
- **Threat actors on multiple fronts continue to seek to exploit cyber vulnerabilities in the U.S. electrical grid.** Nation-states like Russia, China, and Iran and non-state actors, including foreign terrorist and hacktivist groups, pose varying threats to the power grid. A determined, well-funded, capable threat actor with the appropriate attack vector can succeed to varying levels depending on what defenses are in place.
- **Utilities often lack full scope perspective of their cyber security posture.** Total awareness of all vulnerabilities and threats at all times is improbable, but without enough cyber security staff and/or resources utilities often lack the capabilities to identify cyber assets and fully comprehend system and network architectures necessary for conducting cyber security assessments, monitoring, and upgrades.

- Some utilities require financial assistance in creating or shaping their cyber strategy, both to meet regulatory standards and for business security. While regulatory requirements for the bulk electric system are clear about *what* compliance outcomes utilities should achieve, **utilities desire guidance about *how* to best achieve *cyber security* outcomes,** as well as how to develop active defenses capable of addressing a highly targeted cyber attack.
- **The assortment of regulatory standards and guidelines applicable to utilities regarding cyber security practices produces varied methods of adoption.** This causes some overlap and confusion in jurisdictional applicability (federal vs. state) and has produced a wide range of differing practices by utilities in meeting standards, making an evaluation of industry-wide best practices difficult.
- **Utilities expect more qualitative, timely threat intelligence from existing federal information sharing programs.** Utilities also seek clarity about the conditions of information sharing programs based on new national cyber security policy (CISA 2015).

Acknowledgements

This paper was prepared by Idaho National Laboratory for the Office of Energy Policy and Systems Analysis (EPSA) in the U.S. Department of Energy. The authors wish to recognize the counsel of Dr. Lara Pierpoint and Raisa Ledesma-Rodriguez of EPSA.

Table of Contents

Contents

1. Introduction

As the electric grid modernizes, utilities adopt new technology. However, a priority for providers is the reliable delivery of electricity—above security. Since the early 20th century, utilities have increasingly relied on automation to keep up with exponential increases in electricity demand and consumption, as well as reducing need for manpower. Utilities have steadily adopted increasing levels of system protection, automation and control capability to ensure the highest levels of reliability. As reliability levels and energy efficiencies have increased so has the demand for real time information and the expectancy of reliability. These advancing data needs and system requirements have continued to push for even broader automation and control capabilities.

Components on which utilities rely to manage daily operations were originally designed for grid efficiency, with vertically integrated utilities utilizing local generation to serve local load, and for peer utility support when needed. The electric system of today relies on an advanced transmission system, market operations, independent power producers, system operators, as well as the traditional vertically integrated utilities to ensure overall system reliability. The engineering of the power system and how the system is operated has been a very dynamic environment and in many of the new automation and control elements the potential of cyber threats was unrecognized at the time the systems were adopted. As utilities have upgraded ICS and electric grid technology to meet present-day needs, the practicality of digital automation and data transfer has become necessary. A variety of vulnerabilities have emerged, particularly related to greater accessibility as a result of advanced communication means and Internet connectivity.

Much of the publicly available information about utilities' vulnerabilities to cyber threats comes from reported cyber attacks, as well as the subsequent research exploring additional weaknesses and attack vectors for a particular system. Discovery, publication, and mitigation of cyber threats are often the work of cyber researchers and cyber security teams, acting either independently or as surveyors on behalf of a commissioning body (for example Symantec's Targeted Attacks against the Energy Sector or Ponemon's Critical Infrastructure: Security Preparedness and Maturity of 2014 for Unisys, respectively). Organizations such as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a DHS organization, also act as a governmental resource for control systems-dependent organizations such as utilities.

This paper is structured as follows: Section 1 describes the context of cyber threats to the U.S. electric grid in recent years, including known cyber incidents involving U.S. electric sector entities. Section 2 provides an overview of cyber-physical assets of the electric sector, particularly the digitization of equipment used to operate generation, transmission, and distribution systems. Section 3 discusses cyber vulnerabilities to the U.S. power system, including vulnerabilities specific to the grid and cyber security challenges. Section 4 describes cyber threats and threat actors to the electric sector. Section 5 details the current best practices of both government and industry in addressing cyber threats and improving cyber security posture. Section 6 describes the findings of this paper, including those applicable to the federal government and to industry, and Section 7 summarizes findings of the paper.

1.1. A Growing Threat

The likelihood for cyber attacks against utilities is increasing in frequency and severity of attacks. The 2015 Global State of Information Security Survey reported that power companies and utilities[i] around the world expressed a six-fold increase in the number of detected cyber incidents over the previous year.[4] The number of energy sector[ii] incidents reported to ICS-CERT is significant each year, with 79 incidents (the most reported incidents per sector) in 2014,[5] and 46 incidents (the second most reported incidents per sector) in 2015.[6] Out of the 245 total incidents reported across all sectors in FY 2014, "roughly 55% involved advanced persistent threats (APT) or sophisticated actors…The majority [38%] of incidents were categorized as having an "unknown" access vector. In these instances, the organization was confirmed to be compromised; however, forensic evidence did not point to a method used for intrusion because of a lack of detection and monitoring capabilities within the compromised network."[7] The latter point illustrates a complicating feature of cyber attacks in that discovery does not indicate removal of the threat. Similarly, in FY 2015, out of the 295 incidents reported across all sectors, roughly 37% of access vectors were stated as being unknown. The percentage of incidents originating from spear phishing incidents rose to roughly 37%, as opposed to only 17% percent in FY 2014. This indicates that the percentage of unknown access vectors stayed relatively steady between FY 2014 and FY 2015. However, the sharp increase in incidents due to spear phishing access vectors in FY 2015 indicates that the usage of spear phishing techniques appears to be on the rise across all sectors.

[i] PWC considers "power & utilities" to include electric, nuclear, and renewable (wind, solar) sources.
[ii] ICS-CERT's figures related to the energy sector include electricity, oil, and natural gas entities.

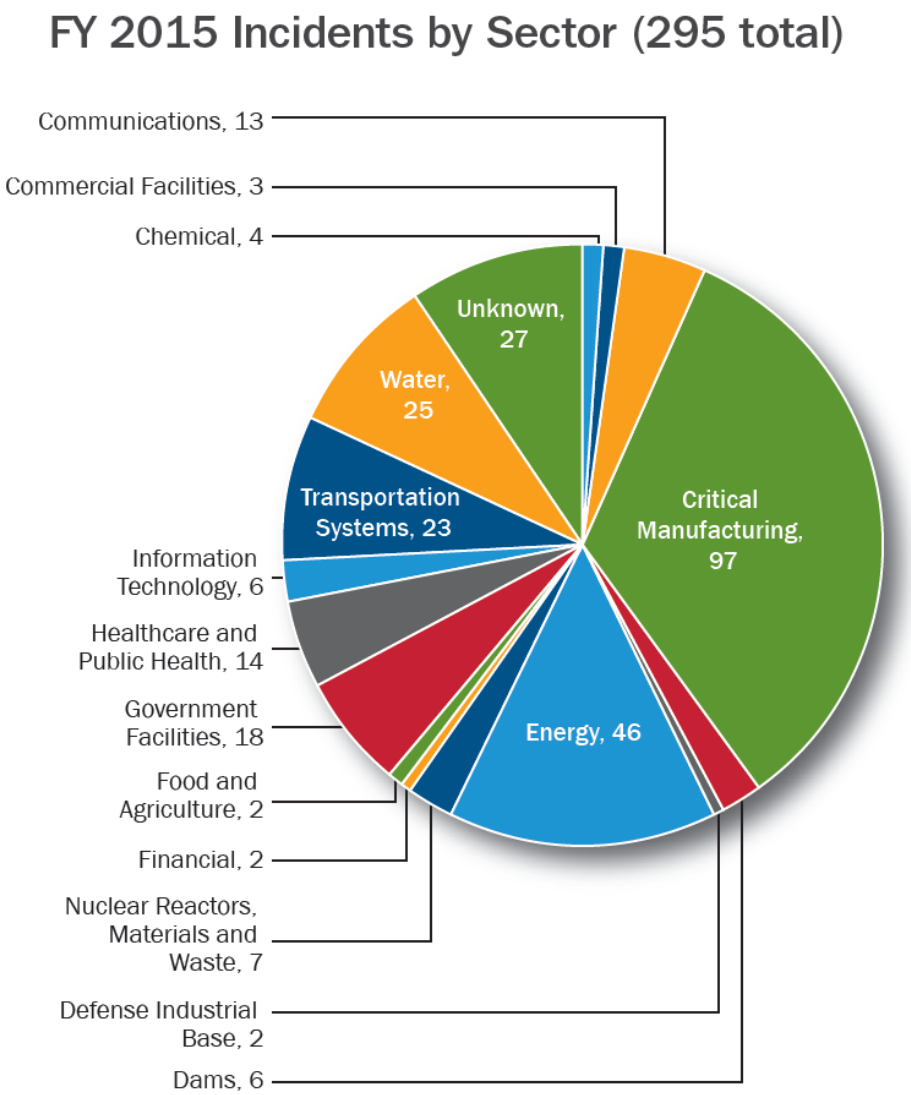

Figure 1. ICS-CERT's FY 2015 incidents reported by sector (295 total).[8] ICS-CERT notes that its established partnership with energy sector participants (to include electricity, oil, and natural gas) contributes to the number of incident reports the organization receives, in comparison to other critical infrastructure sectors.[9]

EY's Global Information Security Survey of 2013 indicated that 80 percent of power and utility companies reported an increase in threats with mobile computing, malware, and phishing being of greatest concern.[10] However, "only 11% of survey respondents said they felt their current information security measures fully meet their organization's needs, 60% are running no or informal threat assessments while 64% believe that their security strategy is not aligned with today's risk environment."[11] Lack of readiness to address current cyber threats compounds future vulnerabilities, since cyber attacks continue to grow in complexity and sophistication.

In a 2014 survey of security preparedness and maturity in critical infrastructure, the majority of respondents were not confident in their ability to upgrade security to meet current threats while also stating that they had no access to real-time alerts, threat analysis and threat prioritization.[12]

Such shortcomings may provide cyber attackers with new, or existing and unmitigated vulnerabilities to exploit. One reason for this stated lack of preparation is the unpredictability of progressively complicated, layered control systems. The increasing complexity of devices used by utilities and other critical infrastructure elements in everyday operations is paralleled by an increase in attack surfaces and vulnerabilities.[13] Because "…these unpredictable elements interact in ways so complex they can never be fully comprehended by us, let alone fully accounted for or protected,"[14] attackers may manipulate digital components to cause unintended physical consequences to real equipment,[15] such as falsifying sensor signals, causing temperature shifts to destroy electronics, over- or under-pressurizing valves, among many other possibilities in a complex control system.

1.2. Reported Cyber Attacks Involving U.S. Utilities

It is likely that many more cyber incidents occur than are reported.[16] Known attacks against the energy sector often follow a phased pattern that focuses on discovery, capture, and exfiltration of data,[17] which generally does not produce tangible or immediately detectable consequences. However, if an attacker's goal is to "degrade, disrupt, deny, [or] destroy"[18] utility operations, prior reconnaissance and established access provide launch points for destructive payloads (malware).[19] No lasting damage–physical, cyber-physical, or otherwise–to U.S. utilities as a result of a cyber attack has yet been reported publicly, but known cyber attacks and campaigns targeting U.S. electric utilities have been highly publicized.

In early 2014, ICS-CERT released information about an unnamed public utility that was compromised via remote access. Not only was the control system configured for remote access, "the software used to administer the control system assets was accessible via Internet facing hosts."[20] Intrusion activity prior and related to this threat was also discovered. Researchers also found that though the remote access point was password-protected, the password was weak.[21] Brute forcing techniques, or 'trial-and-error until solved' attempts to discover the password were found to be a threat to the access point. No long term costs or damage have been attributed to this attack, but an onsite cyber security assessment conducted by ICS-CERT as a result of the event likely resulted in recommendations for the utility's future control system administration.

Conversely, the Havex campaign uses spam email to distribute a remote access Trojan (RAT) tool to targets and in the past used watering hole attacks deployed from compromised ICS/supervisory control and data acquisition (SCADA) vendor websites.[22] Since around 2013 a group known as 'Dragonfly' and 'Energetic Bear', thought to be a state-sponsored organization is responsible for Havex[23] and targets energy sector companies (and other sectors) in the U.S. among other countries. By targeting electric grid operators, equipment vendors, and relevant software providers, the attackers were able to spread malware that "instruct infected machines to download and execute additional components."[24] Though no reports have yet emerged confirming exploit or damage of Havex in infected systems, the malware's complexity and range of access thus far could produce future effects if not properly mitigated.

Another incident to which ICS-CERT responded was found to have been ongoing since 2011 but with no detectable "attempts to damage, modify, or otherwise disrupt the victim systems' control processes."[25] The threat, known as BlackEnergy, is a Trojan-based hacking campaign that exploits

human-machine interface (HMI) software often used by utilities in grid control among other systems. While General Electric (GE), manufacturer of an HMI believed to be the target of the BlackEnergy campaign released a patch for its HMI software in response to the incident,[26] future vulnerability based on this attack vector depends in part on awareness, detection and defense in depth.[iii] The BlackEnergy malware is described as "highly modular" with functionality varying in deployment to different victims,[27] making it difficult to determine its future impact in the electricity industry. ICS-CERT published a Traffic Light Protocol (TLP) Amber-designated version of this information, a limited-release sharing mechanism by which companies affected by and/or requiring the information to mitigate a related cyber threat can receive and share the information internally on a need-to-know basis.[28]

A now-dated but well documented attack on a California independent system operator (ISO) responsible for electricity distribution across the state which occurred in 2001 highlights a lack of cyber security consideration in planned system maintenance. Taking advantage of poor security configuration, attackers compromised two web servers under development to access the ISO's network.[29] The attack was halted before attackers were able to access grid-connected systems, but took nearly three weeks to detect and was eventually assessed to be of Chinese origin. [30] The servers that exposed the utility's network were not firewalled and appear to have been an overlooked threat, the result of a time-sensitive business operations priority.

2. Cyber-physical Assets of the U.S. Electric Sector

The modern electric grid is dependent upon cyber-physical systems, "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components,"[31] to generate, move, and distribute electricity efficiently. The cyber-physical systems of the electric sector include industrial control systems (ICS), which allow digital control of the physical operations of equipment.[32] Where generation machinery such as turbines was once only mechanically operated, equipment is now mostly protected and controlled by ICS synchronously, by automation, and sometimes remotely. These technological improvements have caused the U.S. bulk electric system (BES) to be increasingly vulnerable to intrusions from cyberspace. Modernization efforts of older grid system components to incorporate new digital automation, or smart grid technologies,[33] have introduced a greater number of Internet protocol (IP) enabled access points to grid networks.

The integration of information technology (IT) and operational technology (OT) in ICS expands the cyber threat landscape by introducing several threat vectors as consequences of the greater connectivity of systems. Networks can become less secure over time, often being reconfigured to allow one-time access for a particular need or convenience and never being appropriately restored.[34] Remotely accessible equipment is further vulnerable to public discovery via unprotected networks or the Internet.[35] Each system of the U.S. power grid (generation,

[iii] "Defense in depth" is the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. Source: T. McGuiness, SANS Institute, 2001. https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525

transmission, and distribution) poses analogous and distinct vulnerabilities to the reliable delivery of electricity via cyber-physical assets as described in the sections below.

2.1. Cyber Security Risks Associated with Industrial Control Systems

ICS, "IT- and network-based systems that monitor and control sensitive processes and physical functions,"[36] are critical to performing basic operations within the electric sector, as in other sectors of critical infrastructure. BES operations are composed of multiple ICS systems (consider each power system sector, generation – transmission – distribution – and control, to have a system-of-systems[iv] with highly advanced ICS environments communicating and interdependent on other ICS environments), and each of these systems may be susceptible to similar vulnerabilities regardless of function. These vulnerabilities include:

- Various points-of-entry and paths that can be exploited by threat actors, sometimes remotely
- An ever-increasing number of new vulnerabilities introduced to ICS via system additions or integration
- Easier/broader access to systems and networks due to greater connectivity, including devices directly connected to the Internet
- Greater requirements for sensitive data collection and exchange (equipment operating status, power production and consumption, electricity pricing, etc.) among utilities, market coordinators, and customers create additional network paths and connections[37]

While common attack vectors are known to many utilities that have taken action to mitigate risks, vulnerabilities are not static and cyber assets must continuously be monitored and assessed. Regardless of a threat actor's skill or capabilities, understanding how a utility's OT environment *can* be accessed and what highest-consequence outcomes can be achieved is necessary in order to develop appropriate mitigations.

There is an ever-increasing threat of cyber attacks with consequences on ICS of the BES. The National Security Agency (NSA) reported intrusions into ICS by entities with the apparent technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[38] Such real-world capabilities have already been demonstrated: the Ukraine electric system cyber attacks occurring in December 2015 confirmed the potential for cyber attacks to inhibit and disrupt electric system operations[39] by compromising a SCADA system at host and device levels.

One foundation for the general vulnerabilities in electric sector ICS (and other critical infrastructure) lies in the integration and overlap of IT and OT networks and systems. In the past, IT and OT systems were operated separately, but as the need for greater process efficiency, productivity, safety, and regulatory compliance has increased,[40] IT interconnections with OT have become necessary to provide operator insight and control for real-time conditions in generation,

[iv] A "system-of-systems" is a collection of task-oriented systems that, when functioning together create a more complex system of greater functionality and performance than the sum of constituent systems. Source: S. Popper, S. Bankes, R. Callaway, and D. DeLaurentis, 2004. http://rs.ieee.org/component/content/article/9/77-system-of-systems.html

transmission, and distribution of electricity. Where cyber attacks in the IT domain usually focus on data acquisition, cyber attacks in the ICS domain usually focus on the destabilization of assets.[41] It is important to note that ICS environments utilize many of the same IT components, and as a result malware intended to affect IT networks can also have operational impacts within ICS environments, if introduced. Non-targeted IT-specific malware may have impacts on the cyber assets within an ICS environment and may result in an operational impact; however, a targeted ICS attack could have intent to achieve effects on an operation. In the electricity industry, this could mean the compromise or destruction of equipment used to produce and move electricity from generation to consumer. With the meshing of IT and OT domains, networks have developed new connection points, more networks by which points are connected, and even remotely connected devices. Taking advantage of the connectivity between IT and OT, an attacker may gain access to critical ICS elements to cause an operator loss of view or control, and/or directly manipulate operational performance to affect dire consequences,[42] including physical damage.

2.2. Risks across Grid Power Systems

As the U.S. power system has evolved into an ICS-enabled industry that increasingly relies on intelligent electronic devices (IEDs) using bidirectional communication to execute operations, new cyber security concerns have arisen. Issues such as cyber-hygiene, ostensibly the least difficult vulnerability to correct, and increased connectivity pose attractive modes of attack for threat actors. Despite regulation to ensure cyber security practices among bulk power[v] participants and a variety of best-practice recommendations for utilities, the operational infrastructure of the U.S. electric grid exists with an assortment of older legacy equipment at some facilities, mixed with highly connected digital assets at other facilities, and a system that is inherently difficult to defend due to the geographic distribution and thousands of unmanned remote facilities. This provides attackers opportunities to continuously target vulnerabilities in older technology, or pursue exploits in new connectivity models, or pursue a coordinated cyber-physical attack if necessary. The BES is an ideal target of malicious attacks intended to impact cyber-physical equipment because the compromise of generation and transmission facilities is generally likely to produce the greatest and most detrimental consequences.[43] This does not mean that the distribution system is immune to attack. To understand cyber-physical threats to the U.S. power grid, it is important to understand how the grid systems function individually and together, and what vulnerabilities each system poses to the overall grid. The figure below briefly illustrates the power grid systems and the division between bulk power and distribution.

[v] Bulk power includes generation and transmission of electricity.

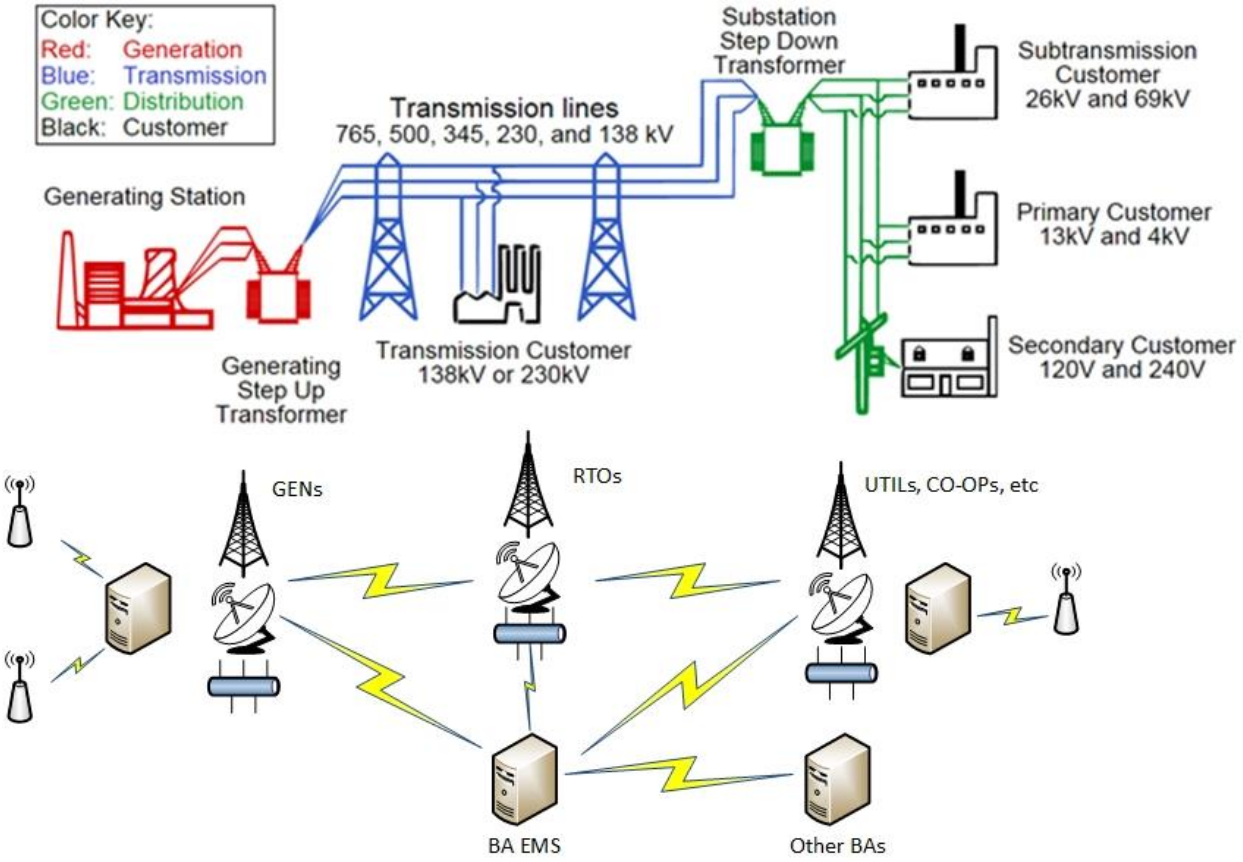

Figure 2. Delineation of Power Grid Systems.[44] The North American power grid is composed of three primary components: generation and transmission, which comprise the BES, and the distribution system. A particular facility like a substation may contain multiple voltage levels, some operating at the BES level and some that are at the distribution system level. The lower portion illustrates some of the many communications necessary among generators, regional transmission organizations, utilities, etc.

Utilities enjoy many benefits as a result of the automation, remote control, and data acquisition capabilities provided by control systems, but this connectivity also exposes sensitive operations and network assets to cyber infiltration and manipulation.[45] The addition of modern digital technology to legacy equipment never designed to be digitally connected or the replacement of analog equipment with digitally connected devices creates cyber vulnerabilities to systems that were previously immune.[46] As opposed to cyber attacks against IT systems intended to facilitate data theft or financial loss, cyber attacks against OT systems may additionally seek to cause loss, denial, or manipulation of view, control, safety, or sensors and instruments.[47] In the electricity subsector this means causing equipment malfunction or failure, physical equipment damage, power disruptions, or blackouts. Every utility has a different number and variety of cyber assets. The sheer number of grid elements means cyber security requirements between and throughout systems are difficult to identify and implement:

> "The North American bulk electric system is comprised of more than 200,000 miles of high voltage transmission lines, thousands of generation plants, and millions of digital controls. More than 1,800 entities own and operate portions of the system,

> with thousands more involved in the operation of distribution networks across North America. These entities range in size from large investor-owned utilities…to small cooperatives. The systems and facilities comprising the larger system have differing configurations, design schemes, and operational concerns."[48]

With many variables and factors determining the cyber security posture of each grid participant, it is more practical to consider cyber threats to U.S. power within electric generation, transmission, and distribution. Each area has distinct vulnerabilities to the reliable delivery of electricity, and all areas share some similar vulnerabilities. Essential system functions at risk to cyber attack include:

- Electricity supply (generation) or transfer (transmission) stability
- Equipment performance and ability to recover (backup systems)
- Communication between systems or equipment
- Operating conditions of generation, transmission, or distribution equipment
- Black start[vi] capability
- Transmission of power between generation and distribution

The following describes potential impacts to the power grid due to degradation or manipulation of such system functions.

2.2.1. Generation

Electricity supply begins with generation. A variety of fuel sources are used to produce electricity, usually via turbines. Regardless of fuel source or method, electricity generation relies on local control of output and wide-area control (Automatic Generation Control or AGC) of load and frequency.[49] Local control loops include sensors that continuously feed data to control rooms that send commands to the generator equipment (such as turbines). Consequently, production is increased or decreased to meet generation demand conditions, and system load stability is balanced across multiple generation resources. Local control loops do not depend on large scale geographically dispersed control systems and therefore the cyber attack surface is considered to be more focused on gaining access to the local control system. This can be achieved through remote access, the introduction of malware through a number of means, or pivoting through a trusted communication path in the organization's corporate networks.[50] Wide-area control depends on ICS/SCADA, and therefore an attack on AGC could have serious impacts on power stability emanating from a generation facility, though more than one attack vector related to AGC function would likely be necessary to significantly disrupt power flow.[51]

Generation control loops could be vulnerable to attacks focused on destabilizing power load that initiate equipment safety procedures (i.e., decrease in production, emergency shutdown), failure of generation equipment, or physical destruction of generation equipment. In an experiment sponsored by the Department of Homeland Security (DHS) and conducted by Idaho National Laboratory (INL) in 2007, researchers demonstrated the potential for physical damage via cyber means by hacking a simulated power plant control system to impact the physical equipment of a diesel generator.[52] The generator's protective relays were manipulated to connect the generation

[vi] A black start is the restoration of a power station without reliance upon the external power transmission system.

resource while out of sync with the connected transmission system. The greater inertia of the transmission system introduced stress on the physical rotor of the diesel generator as it was forced into sync with the system. Performing this attack rapidly over a short period of time resulted in physical damage to the generation resource from a cyber controlled device.[53]

The likelihood of a successful cyber attack that damages large utility equipment—a cyber-physical incident—depends on an adversary's ability to defeat a number of factors including utility access controls, intrusion detection capabilities, personnel awareness, and backup measures. To impact a large portion of the power grid, an attacker would likely need to gain access to and compromise multiple generation or transmission facilities simultaneously, target utility control centers, or gain entry to a system providing widespread access. Nevertheless, bulk power in the U.S. is still currently delivered throughout an interconnected, interdependent, and in many areas aging grid, one that requires significant and costly upgrades in critical electric system elements, system redundancy, and cyber security investments to be resilient to multiple, simultaneous cyber-physical events.[54]

2.2.2. Transmission

Once electricity is generated it is stepped-up in voltage and transported, often over great geographic distances, before being distributed to consumers. The major components of transmission systems are substation transformers, which step-up and step-down voltage in order to more efficiently transport electricity over long distances and deliver appropriate voltages to load, transmission towers to connect power lines, and control centers to manage the delivery of power from generation resources to the distributed system loads. These three elements are also the most at-risk to cyber attacks within transmission, but high-voltage transformers and other large equipment used to support transformer functions are the most impactful in a cyber-physical event due to replacement time and cost.[55]

Risk from loss of transformers is heightened by the lack of alternate delivery paths or lack of access to spare transformers in many transmission utilities.[56] If a transformer is damaged, generated power must be redistributed to other substations connected to the generation source, or through a spare transformer. However, most generators are only served by two or three transmission facilities.[57] The loss of one substation taking on power load from a generator may put too much stress on remaining transformers, creating grid instability. Spare transformers can ease this burden, yet most utilities do not own or have access to spare transformers capable of replacing one damaged by a cyber event.[58] Power surges due to a lack of transmission capacity could lead to cascading failures throughout the grid and long-lasting power outages. Further, while the loss of a transformer is rare, recovery without a spare can take months.[59]

Modern substations use several kinds of communication to manage local functions, the security needs of which have expanded as Ethernet-based networks that facilitate communications in substations became common in the late 1990s.[60] Transmission substations are part of the BES and some larger facilities are subject to mandatory North American Electric Reliability Corporation's

Critical Infrastructure Protection (NERC CIP)[vii] cyber security standards, making unauthorized access to substation networks difficult and likely requiring advanced skill by a threat actor. However, controllers and other devices increasingly used in substation automation are often sources of the thousand-plus ICS vulnerabilities discovered since 2010[61] that can serve as entry points to networks. Once inside the digital operations of a substation, an attacker with the necessary skills and tools could disrupt, desynchronize, or impact data communications necessary for communications and controls causing load instability.[62] Substation networks without detection capabilities to identify intrusions and malicious data injection[63] could allow an attacker to manipulate multiple substations over time without discovery. In these networks, the risk of a coordinated cyber attack powerful enough to disrupt a portion of the grid is greater.

ICS experts also note that if a threat actor can physically access a substation there is virtually no limit to potential damage: malware can be directly introduced to computers and devices, protective relays manipulated, and equipment physically destroyed.[64]

Similar to generation, cyber threats to utilities responsible for transmission depend on several variables, such as network configuration within a substation and means of communicating data, and substation and transmission tower physical security. To significantly impact transmission of power throughout the grid an attacker would also require complex means to interrupt or destroy multiple high-voltage transmission lines or transformers simultaneously. This would likely require high skill and resources as well as an ability to access and disable local equipment, since substations are usually configured so that if communications are lost the substation and all equipment will continue to operate normally.

2.2.3. Distribution

Distribution and local delivery of electricity are generally not considered part of the BES,[65] and are overseen by state public utility commissions. This means that cyber security standards and implementation of selected standards can vary in breadth of protections and backup measures for distribution utilities. Yet in some cases, cyber attacks on distribution elements can have consequences that reach the BES.[66] In December 2015, the first confirmed hack to affect a power grid occurred in Ukraine—a distribution system serving as the attack plane.[67] Attackers used malware to gain access to IT infrastructure, then hijacked the SCADA distribution management system (DMS)[68] to "cause undesirable state changes to the distribution electricity infrastructure, and attempt to delay…restoration by wiping SCADA servers after they caused the outage," while simultaneously preventing calls reporting power outages from reaching customer service centers resulting in a 3-6 hour outage.[69] The attackers demonstrated high skill level and likely conducted months of reconnaissance and planning to execute the attacks that took multiple substations offline and disabled backup power from two distribution centers simultaneously, leaving more than 230,000 customers without electricity.[70] While the Ukraine attacks were strategically executed by a sophisticated threat actor(s), the basis for the attack has been attributed to a cyber hygiene issue. According to security experts who investigated the attacks, a phishing campaign beginning in spring 2015 targeted IT personnel of power distribution companies, creating a backdoor for the

[vii] The North American Electric Reliability Corporation (NERC) produces mandatory Critical Infrastructure Protection (CIP) standards to which North American bulk power participants must comply.

attackers via Microsoft Word macros if victims opened a malicious attachment in the phishing emails.[71] This demonstrates that human error is a highly exploitable element in cyber attacks that can have serious impacts on power delivery, even outside the BES.

An attacker is more likely to gain access to substations that are not bound by NERC CIP and more likely to be lacking in basic cyber security practices and physical security protections than NERC CIP-bound substations.[72] While distribution substations are not subject to NERC CIP because they exist outside the BES and ostensibly more vulnerable, transmission substations may be equally susceptible to cyber attacks, if regulatory requirements are not implemented or enforced at the distribution level. A cyber attack on a distribution substation could involve manipulating breakers to interrupt power or compromising SCADA operations to cause load instability, but pose minimal risk to the overall grid since these effects would only have local service area impacts. However, if a threat actor can (physically) access a Distribution SCADA Master via a substation, risk is significantly greater as the SCADA Master allows access to other distribution and potentially transmission elements within the system.[73] Further, points of grid connection such as step-down transformers between the transmission and distribution systems do not always fall under NERC CIP regulation and may present cyber vulnerabilities.[74]

3. Cyber Vulnerabilities in the U.S. Electric Sector

Bulk power participants may threaten grid security if cyber-physical system equipment is not appropriately assessed when incorporated into a given system. Further, according to PricewaterhouseCoopers' 2015 *Global State of Information Security Survey*, only a little more than half of power and utility companies queried reported using vulnerability scanning tools,[75] the breadth or efficacy of which were not defined. The integration of IT and OT in ICS expands the cyber threat landscape by introducing threat vectors as direct consequences of the greater connectivity of systems. The following are vectors threat actors are most likely to exploit in order to execute cyber attacks on a power system participant.

3.1. Networks

Utilities employ networks to connect equipment, controllers, software, and systems within OT and IT environments, respectively. Because network vulnerabilities due to misconfiguration, poor administration, lack of perimeter awareness, communication shortcomings, among others are known,[76] networks are still among the most attractive entry points for threat actors. In a 2014 survey composed primarily of electric utility respondents, the use of insecure IT networks comprised 41 percent of total security incidents, the largest source of incidents reported.[77] Despite the presence of common network security measures, a determined threat actor continuously looks for potential points of entry:

> "Attackers can search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses. Attackers have exploited flaws in these network devices to gain access to target networks, redirect traffic on a network (to a malicious system masquerading as a trusted system), and to intercept and alter information while in transmission. Through such actions, the attacker can gain

> access to sensitive data, alter important information, or use one compromised machine to pose as another trusted system on the network."[78]

The communication protocols used throughout ICS networks are of additional concern. Common and long-established ICS protocols such as Modbus and DNP3 used throughout the power system have little or no security measures: lacking authentication capabilities, messages may be intercepted, spoofed,[viii] or altered, potentially causing a dangerous event in an operations environment.[79] As U.S. utilities move toward a "smart" grid, vendors of grid modernization technology have increasingly standardized their products for greater interoperability. One example of this is Ethernet-based IEC[ix] 61850, a protocol largely used in substation automation in electricity transmission and distribution, but likely to be expanded in control center use in the future.[80] Traditionally a communication protocol used in an office or IT environment, Ethernet is increasingly used by utilities throughout ICS because of its data transfer speed and low cost. However, Ethernet was not designed for use in critical operations such as power grids. ICS networks communicating via Ethernet are not isolated, dedicated circuits, and are therefore potentially more vulnerable to cyber intrusions.[81]

3.2. Communication

Electric sector ICS exist in and rely on networks to communicate data about equipment operating status, to monitor operating conditions, and to communicate changes to current equipment operations. While a utility's control systems may not be directly accessible remotely from the Internet,[82] tangentially connected devices and networks or those with a peripheral in common may provide points of ingress to the control system's network. For example, NERC created a set of cyber security reliability standards established around TCP/IP-based ("routable") connections, which provided a degree of protection in communicating with a utility's production control system network. However, serial-based connections, often used to communicate with a substation and/or remote devices such as programmable logic controllers (PLCs)or remote terminal units (RTUs), were a less secure regulatory "blind spot"[83] but still common communication protocol. Similarly, researchers recently demonstrated how vulnerabilities found in a third-party vendor's implementation of the DNP3 communication protocol could be used to access a utility's control system: "…an attacker could target a non-critical, serial-based piece of field equipment at an electrical substation and knock out visibility over all of a utility's substations. The vulnerabilities in some DNP3 implementations could allow attacks against master control systems from a field device by sending a malicious frame, or message to the control system."[84]

3.3. Devices

As components are upgraded or added to a utility's control system, keeping track of network connectivity becomes as important as keeping up technologically. As legacy equipment is updated and integrated with new technology, "The security issue, for old and new systems…[is] how they are connected to the utility's other systems, and what levels of security exist to detect and deter

[viii] Spoofing refers to the act of gaining unauthorized access to a network by sending falsified messages to a target computer IP address that appear to be sent from a trusted host.

[ix] The International Electrotechnical Commission (IEC) is a consensus-based international body that produces standards for electric and electronic products.

potential intrusions."[85] Devices communicating with or functioning as a part of a utility's control system also pose new threats to utilities and to the electric grid. Many automation components, such as PLCs function via microprocessors, contain function specific software programming, and also have management and communications capabilities over network paths.[86] Further, such devices have been the target of cyber attacks as a means of gaining access to a control system. A review of ICS-CERT Advisories at any time displays an ongoing list of ICS-related equipment vulnerabilities discovered by cyber researchers and industry professionals.[87] Such research is often conducted by cyber security experts who use the same methodologies and techniques used by cyber attackers, demonstrating literal attack vectors. In a 2012 example, a cyber researcher discovered vulnerabilities in Siemen's RuggedCom equipment, products that are widely used to communicate with remote power stations. A "back door" allowing remote access to the equipment also allowed hackers to intercept network traffic. Depending on the traffic content, such as authentication credentials, attackers could plausibly exploit such flaws to manipulate larger, connected equipment—such as a power station.[88] With the introduction of public tools such as SHODAN, a web-based search engine for identifying devices connected to the Internet, including ICS components,[89] such equipment may be discoverable, thus allowing attackers to locate and remotely probe a utility's SCADA system for weaknesses.

The growing presence of so many peripheral components and expanded interconnectedness and interdependence of systems used by utilities in conjunction with or to add capabilities to their production control systems has contributed to the changing nature of cyber attacks against the energy sector. The accessibility of ICS elements is broadened by the assortment of commercially available technology by which control systems are built. Commonly used software such as Windows or a networked input/output (I/O) device often used in the electricity industry, such as PLCs orRTUs, are individual targets of hackers; the vulnerabilities they expose translate into "dangerous remote code execution holes"[90] for utilities' control systems. Small subordinate parts such as computer chips, which "within various devices are sourced from literally everywhere,"[91] can also serve as access points to their primary systems such as SCADA. Though third party technology is a necessary part of control systems, utilities may be unaware of their control systems' supply chain vulnerabilities[92] and as a result fail to take appropriate cyber security countermeasures.

3.4. Remote Access and Mobile Devices

In order to manage geographically widespread assets, increase convenience and reduce costs, utilities increasingly rely on remotely accessible equipment and mobile devices. However, vulnerabilities stemming from unsecure access or connection to critical systems via remote tools and devices are often cited as the greatest rising source of vulnerability to cyber incidents: in a 2015 EY survey, more than half of various industry respondents including power companies and other utilities rated mobile computing use as a medium to high factor contributing to increased risk exposure.[93] Susceptibility to unauthorized access depends in part upon established controls and cyber hygiene. Strong passwords, authentication, and data encryption may seem to be obvious measures to employ when remote access to ICS networks or devices is necessary, but are often overlooked or ignored. In a 2014 incident response activity report published by ICS-CERT, a public utility's control system network was described as having been compromised as a result of weak passwords and authentication at a remote access point.[94] The same report also described

another unprotected Internet connected control system that lacked authentication controls or a firewall.[95] The shift to a smart grid will mean that utilities will add thousands of devices to their operations including new sensors, controllers, relays, meters, etc. Grid modernization technologies will likely be subject to future regulation,[96] yet maintaining a continuous cyber security perimeter is entirely the responsibility of each utility.

Remotely accessible equipment is further vulnerable to discoverability. Tools such as SHODAN, allow users to search for Internet accessible control systems, routers, building management systems, and administrative platforms throughout the world.[97] These tools leave many kinds of remotely accessible equipment in an easily searchable environment where the equipment can be identified via its IP address and in some cases easily accessed, further creating vulnerability to a cyber attack.

3.5. Third Party Services and Supply Chains

Utilities rely on vendors, system integrators, and other third party service and product providers in order to operate their power facilities. With hundreds of secondary and tertiary parties involved in the construction and maintenance of generation, transmission, and distribution, utilities often find it difficult to ensure supply chain integrity. Some vendors of ICS equipment unintentionally generate cyber security problems due to vendor maintenance policies, such as creating intentional or unintentional "backdoors" for access to devices or software, or by threatening to void equipment warranties if reconfigured from factory settings, i.e., changing passwords or installing unapproved security packages.[98]

The software supporting ICS equipment used in all segments of the power grid in IT and OT environments must also be regularly updated, though doing so sometimes requires system downtime. Scheduled outages of some facilities require approvals and coordinated operational planning activities, as well as potential financial losses associated with outages. To ensure safety and reliability, some utilities, depending on their specific operating environment, may schedule regular (although infrequent) shutdown times coordinated with maintenance windows to conduct updates, as opposed to conducting updates when vulnerabilities emerge.[99] Software can be exploited based on well-known vulnerabilities that remain unpatched, sometimes for years.[100] Most ICS operators rely on vendor-validated patches to be delivered on a regular schedule.[101] Yet some prominent vendors are slow or resistant to acknowledge vulnerabilities in their own software, even simply refusing to address vulnerabilities that exist,[102] or inadvertently serving as the distributor of malware concealed in vendor-provided web updates as demonstrated in the Havex campaign.[103] Utilities that rely on unpatched, vulnerable products may lack the skill to resolve the issues internally, or may fear voiding warranties by attempting to do so, yet must continue to use the products to avoid production downtime.

3.6. Challenges in Implementing Cyber Security

3.6.1. Lack of Cyber Security Personnel

Modern control systems such as SCADA can be expansive structures, often covering large geographic areas and requiring multiple employees to operate safely and efficiently. Yet companies continue to face challenges in designating enough or any personnel to be responsible for control system security. A congressional report published in 2013 surveyed 150 U.S. utilities, of which twenty-eight provided the number of employees each dedicated to cyber security duties: while several investor-owned utilities (IOUs) reported up to a 300% increase in number of cyber security employees over five years, federal power administration agencies responsible for major portions of the BES did not provide numbers of dedicated staff for more than one year; six federal entities reported having no employees performing primarily cyber security duties.[104] It should be noted, however, that many utilities cited information protection concerns in regards to the congressional survey and elected not to respond or respond only in part.

According to another study of critical infrastructure cyber security, 55 percent of companies surveyed responded that only one person was assigned to ICS/SCADA security; 25 percent had no one assigned.[105] This may be due in part to the fact that ICS security is a specialized field, generally with fewer practitioners than the IT security field. Utilities may lack comprehensive awareness of all control system assets online at any given time and/or a party knowledgeable of all network interconnections. This also diminishes utilities' detection capabilities for cyber intrusions, as well as unauthorized devices or connections to networks.

3.6.2. Lack of Cyber Hygiene

Control system cyber security is further impaired by poor institutional cyber hygiene such as weak or no password usage, outdated or unpatched software, and even poor physical security. Attack vectors have evolved to exploit poor personnel awareness of threats to cyber security more often than attacking hardware directly.[106] In a 2014 survey of cyber security in energy companies and financial services, "61% of respondents at energy companies said email is their biggest threat vector," and as a result, "37% of energy sector respondents reported that malware had evaded their defenses."[107] In another 2012 study of IT security in the energy and natural resources industries, phishing and infection with malicious malware, both of which are most often deployed via email, were the two most common, respectively, of the top six types of security failings found.[108] Phishing campaigns can increase vulnerabilities exponentially by making virtually all personnel points of ingress, particularly customized 'spear-phishing' attacks which can be highly effective in convincing recipients of authenticity. According to a report commissioned jointly by two House of Representative committees in 2013, many U.S. utilities reported "'daily,' 'constant,' or 'frequent' potential cyber attacks ranging from phishing to malware infection to unfriendly probes. One utility reported it was the target of approximately 10,000 attempted scans each month."[109] A successfully phished email or malware injection may provide attackers pathways to business networks and control systems. In April 2016, a Michigan utility's IT network was infected with a new type of ransomware[x] that forced the utility to shut down its accounting system and personnel

[x] Ransomware refers to a kind of virus designed to deny a victim access to the victim's digital property until the victim provides a ransom payment.

email service, as well as a customer service phone line.[110] Though the objective of ransomware cyber attacks is usually extortion, the way the virus spread through the utility's internal network after having been introduced by an employee who opened an infected email attachment[111] could affect tangentially connected systems—such as OT networks.

Cyber attackers also take advantage of the "low-hanging fruit" produced by the energy sector's delays in applying software updates and patches for problems that are several years old.[112] In early 2015, a reconnaissance malware tool known as "Trojan.Laziok" targeted energy companies via spam mail containing an exploit code embedded in an attachment. Once opened and executed, the tool allows "attackers to gather information on the compromised devices in order to decide how to proceed with the attack" at which point "additional malware payloads may then be delivered back to the compromised systems, which can cause damage to networks" and allow data exfiltration.[113] Though needing a user to open the attachment containing malicious code, the malware's success was more dependent on an old, unpatched vulnerability commonly found in the energy companies' operating system networks.

Another remote access technique easily deterred but often lacking is strong passwords for remote devices. Cyber intelligence firm IntelCrawler found many very-small-aperture terminals (VSATS), broadband satellite communications that are often used in the electricity sector to transmit data to and from remote locations, to have weak passwords—sometimes using factory default settings,[114] the details of which can often be found in manuals available online. Researchers found "thousands and thousands"[115] of systems, some of which were connected to and thus bypassing security measures of larger control systems.

4. Cyber Threats to the U.S. Electric Sector

4.1. ICS Cyber Kill Chain

Used in single exploits or in broader campaigns and in conjunction with one or more attack vectors, attack methods applied in cyber intrusions provide threat actors entry and mobility throughout a target company's business and/or operational environments. Some common attack delivery methods include phishing, introducing infected removable media, exploiting human error, introducing malware through network communication paths, and using web-based watering hole attacks.[xi] [116]

An attacker seeking to create a high impact cyber event must undertake planning and research to conduct an effective attack on a target, the complexity of which depending on the criticality of the target and thus its cyber security protections. The steps an attacker must undertake to compromise ICS can be described by the ICS Cyber Kill Chain,[117] the steps of which are listed below. The ICS Cyber Kill Chain exists as a two stage attack with multiple steps existing in each stage. The first stage is based on the cyber kill chain model developed by Lockheed Martin[118] and the second stage

[xi] A watering hole attack is a technique in which an attacker infects a website with malware with the intent that a target group of users who frequent the site will access it and at least some users will unknowingly download the malware.

is focused on achieving an ICS effect. Each step is elaborated using the example of an attacker planning to disrupt the generation facilities of one or more large utilities.

Stage 1

1) **Planning**: An attacker conducts reconnaissance to understand as much as possible about a target. This might include gathering information about ICS system(s), utility company, operator personnel, etc. A vast amount of information, often including technical details and even schematic diagrams can sometimes be easily found online. In January 2016, researchers released a list of manufacturer default passwords for over 100 ICS products, many from big-name vendors[119] found in most utility ICS, and sometimes left unchanged by operators. As previously mentioned, tools such as SHODAN may also allow an attacker to find the physical location of ICS equipment that is directly accessible from the Internet and even access web-based applications related to its control.[120]
2) **Preparation**: Having identified a suitable entry point(s), such as a utility's IT network connected with a trusted connection into an OT network for unit performance data and analysis purposes, an attacker performing network mapping and discovery would decide what tool(s) are needed to reach a target. Obtaining a foothold in a target environment is an important first step and recently, human error has proved a particularly effective target for cyber intrusions**.** According to ICS-CERT, spear phishing[xii] accounted for the most common known access vector in 2014 and 2015 (second to unknown access vectors).[121]
3) **Cyber Intrusion**: An attacker attempts to exploit a chosen attack vector(s). Methods such as phishing or watering hole attacks are often successful. Preying upon human error to gain access to networks is quick and may provide numerous opportunities, particularly if utility personnel are not trained to identify malicious activity. According to a 2014 Unisys survey of critical infrastructure companies, providing cyber security training for all employees was the lowest priority of cyber security objectives, with only six percent indicating employee training was even one of their top three priorities.[122]
4) **Management and Enablement**: After successful intrusion, an attacker may explore a network or system for connections to further exploit. Threat actors often establish multiple additional paths to ensure access in case one is detected or removed.[123]
5) **Sustainment, Entrenchment, Development, Execution**: Now an attacker can execute the means of achieving a goal such as the deployment of malware to take control of other network computers or manipulation of communications between machines. This step is critical to a threat actor's ability to effect loss, denial or manipulation of a target. It also marks a divide between activities leading to a cyber intrusion versus those leading to a cyber attack. Many companies lack effective intrusion detection and/or are unaware of this kind of activity in their systems. A 2015 SANS survey reported that 49 percent of respondents were not aware of any infiltration or infection of their control systems; 32 percent indicated that their control system networks had been infiltrated.[124] Within utilities

[xii] Spear phishing is a technique by which an attacker uses email to attempt to lure a victim to open attachment files or links that will cause the victim to download malware or provide the attacker with unauthorized access to a computer, network, or application. The victim may be carefully selected by the attacker using social engineering techniques based on the victim's access to specific items.

specifically, little more than half of those polled in PWC's 2015 survey indicated the use of intrusion detection tools, a ten percent decrease from the previous year.[125]

Stage 2

6) **Attack Development and Tuning**: With undetected freedom of movement within a target network(s), an attacker can now use findings about discovered ICS equipment to "tailor" an attack capability to achieve a desired effect.
7) **Validation**: An attacker tests the selected attack capability or capabilities. This may be conducted via simulation or in some cases, particularly a sophisticated attack carried out by a nation-state actor, an attacker may actually acquire physical ICS equipment identical to that of a target to conduct testing. Such equipment may often be easily purchased used from online retailers such as eBay, where images or descriptions may also provide useful information about how ICS equipment was last deployed and where it was in service at a utility. Security researchers recently conducted a test by purchasing a SCADA server from eBay for less than twenty dollars which contained poorly protected configuration files, diagrams, operational substation data and other sensitive information from its previous owner. The company had recently upgraded its equipment and incorrectly assumed the SCADA server had been sanitized as part of their end-of-life equipment policy before being sold.[126]
8) **ICS Attack**: The attacker activates or deploys an attack capability or capabilities (payload) to achieve a desired effect. As opposed to an attack on IT components that might result in loss of data, time, or money, an effective attack on the ICS-based OT environment of a utility could result in loss of electricity generation or transmission for a prolonged period, and an extreme consequence might be loss of life, [127] directly (power line instability electrocutes utility workers) or indirectly (hospitals lose power). While a successful attack of the latter scale would be difficult to achieve and likely require nation-state level resources, utilities are increasingly experiencing cyber attack attempts. A survey of utilities commissioned by two members of Congress in 2013 found that more than a dozen utilities reported "daily, "constant," or "frequent" cyber attack attempts, with one utility indicating that it suffered from approximately 10,000 attempts a month.[128] Assessing the intent of an originating communication is difficult and as a result many utilities would consider these thousands of cyber attack attempts as simply network scans or probes that may be initial Stage 1 reconnaissance. Whether these thousands of reconnaissance attempts are intended to result in Stage 1 attacks or progress to Stage 2 ICS attacks is unknown and as a result defenders need to leverage appropriate monitoring and response capabilities.

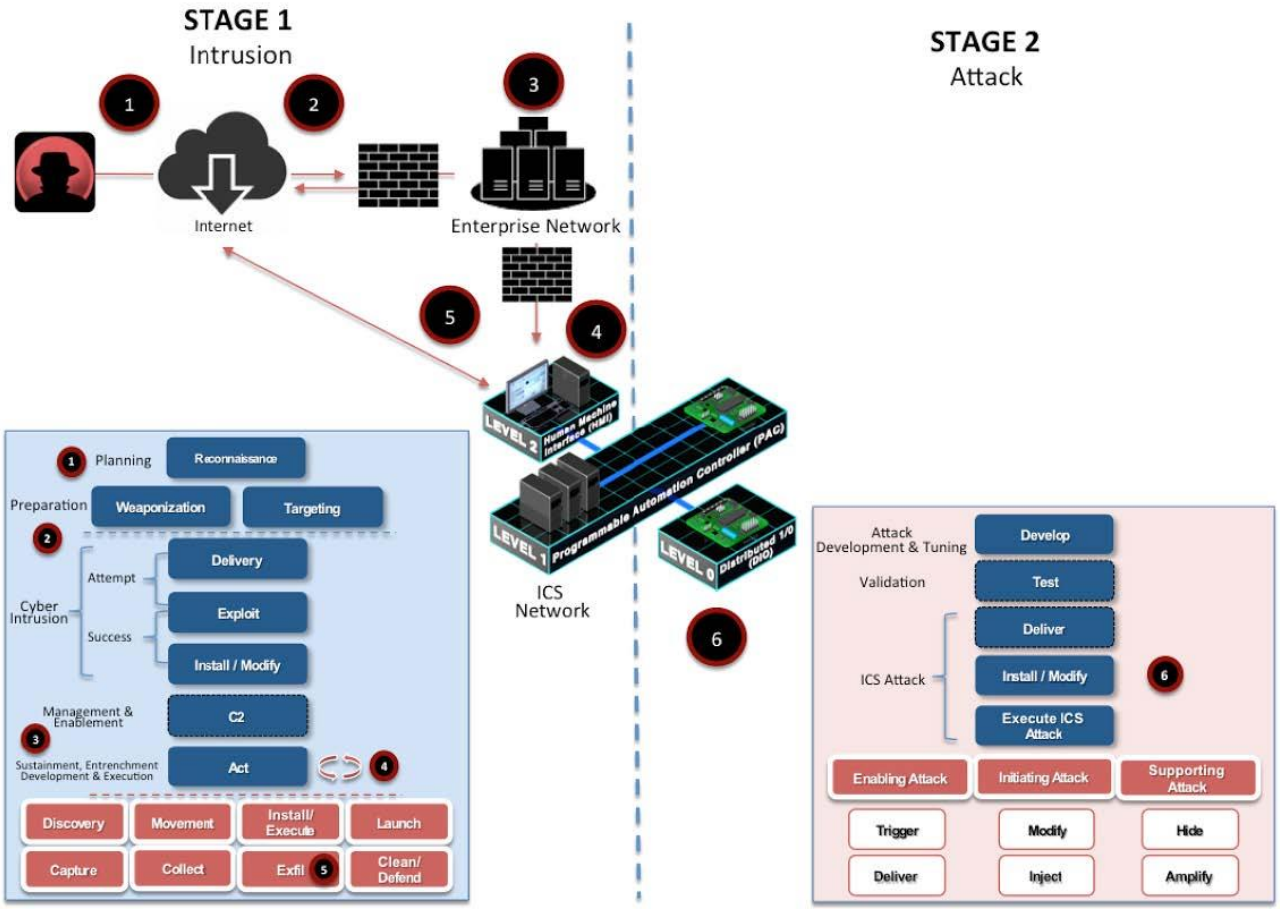

Figure 3. ICS Cyber Kill Chain -Intrusion, Preparation, and Execution.[129] An illustrative example of how a cyber attacker targets, approaches, and moves throughout networks.

4.2. Threat Actors

Attacks on ICS have become more targeted than in the past. Attackers have become more knowledgeable about how to go after industrial control systems, using attacks customized to exploit ICS. Additionally, threat actors are paying close attention not only to payload, but delivery as well,[xiii] focusing on ICS trusted relationships.

As a result, phishing attacks have increased against production engineers and those on the plant floor area, as well as watering hole attacks against sites with information for ICS engineers. Attackers are starting to trojanize ICS files and components that are available for updating firmware and finding ways to replace them in the supply chain in order to get malware over the firewall and into production environments.[130]

[xiii] A cyber "payload" refers to malicious software or computer viruses that produce a harmful effect(s) in a target system to which a payload is delivered. The "delivery" of a payload refers to the vector, or path by which an attacker introduces the payload to a target.

A number of threat actors on multiple fronts continue to seek to exploit cyber vulnerabilities in the U.S. electrical grid. Nation-states and non-state actors including foreign terrorist groups and criminal organizations all pose a threat to the power grid, albeit at different levels.

> ***"Politically motivated cyber attacks are now a growing reality, and foreign actors are reconnoitering and developing access to U.S. critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile. In addition, those conducting cyber espionage are targeting U.S. government, military, and commercial networks on a daily basis."***[131]
>
> ***-James Clapper, Director of National Intelligence***

Nation-states such as Russia and China seek to exploit grid vulnerabilities to serve strategic objectives in wartime, and are growing capabilities to strike at U.S. critical infrastructure. Countries like Iran and North Korea have undertaken offensive cyber operations, aiming their attacks at disruption or asymmetric effects in terms of national, economic, and civil security. Non-state actors target grid facilities for not only the asymmetric efforts, but also to make political statements and challenge perceptions of governance and stability.[132]

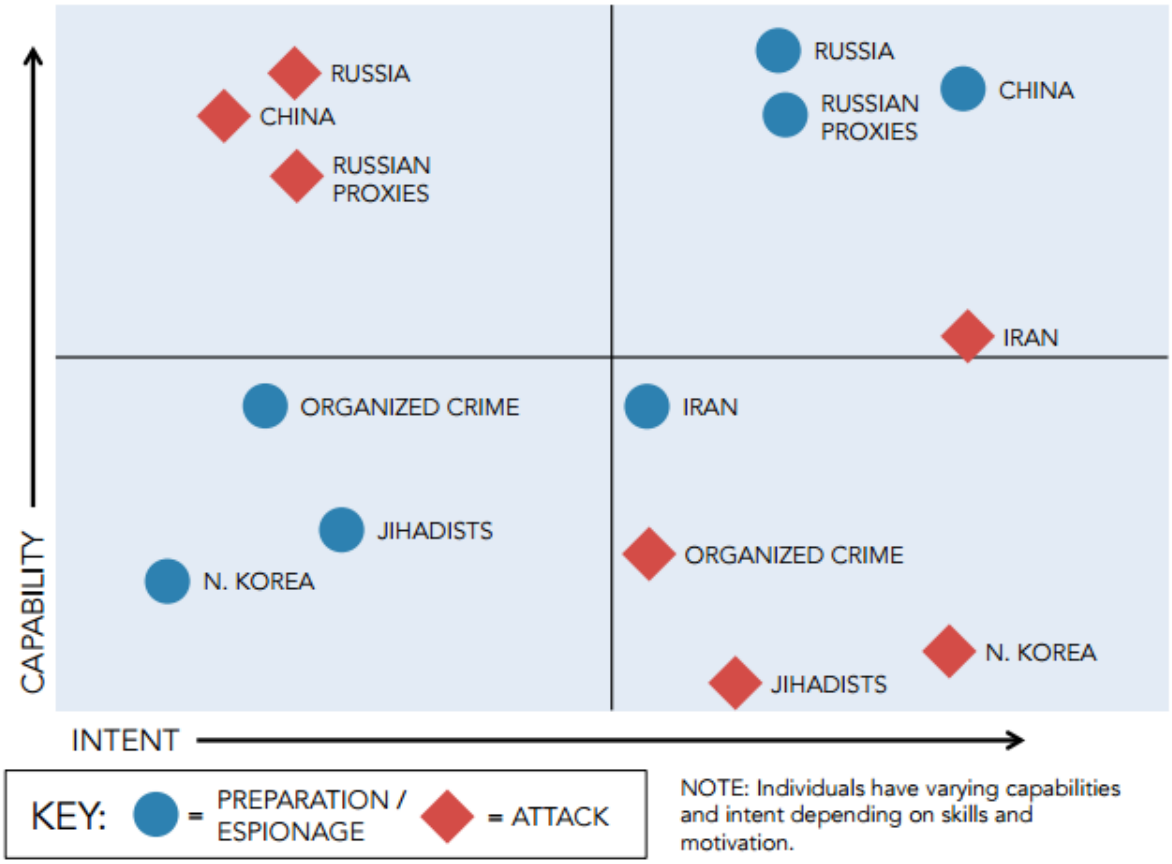

Figure 3. Intents and Capability of Threat Actors.[133] The skill necessary to plan for versus execute a cyber attack differs, even within the same group. High skill is also not always

indicative of greater intent to attack. For example, national actors may benefit greatly from cyber intrusions to an adversary nation, but a cyber attack might mean an act of war.

4.2.1. Russia

Russia possesses a substantial and well-resourced central cyber command. Past cyber intrusions on U.S. governmental organizations including the State Department, Department of Defense, and the White House have been attributed to Russian state-sponsored hackers.[134] In 2007, Russia conducted cyber attacks on Estonia's critical technology infrastructure, flooding government, financial and media sectors with Distributed Denial of Service (DDoS) attacks.[135] In 2009, it was reported that Russia and China had both made attempts to penetrate the U.S. power grid, using software programs to map U.S. infrastructure and potentially disrupt the system.[136]

In late December 2015, in the most comprehensive cyber attack on a power system to date, sophisticated actors, widely suspected of working on behalf of the Russian government,[137] targeted the Ukrainian energy sector using multiple cyber tools, including the malware BlackEnergy to gain initial, unauthorized access to power company networks. This malware was discovered on Ukrainian networks as early as May 2014.[138]

4.2.2. China

China has been an extremely active, advanced cyber actor for some time now – particularly in regards to economic espionage against U.S. companies – though they often use blunt force cyber tools (such as network scanners, viruses, and botnets) to access targets.[139] China's multiple intrusions into U.S. ICS/SCADA and smart grid tools may be aimed more at intellectual property theft and gathering intelligence to bolster their own infrastructure, but it is likely that they are also using these intrusions to develop capabilities to attack the BES, as well. For example, one of the People's Liberation Army Unit 61398 military personnel charged with stealing U.S. economic secrets in May 2014 was linked to UglyGorilla, a hacker pseudonym responsible for cyber intrusions of a Northeastern U.S. utility since beginning at least in 2012.[140]

Like Russia, China is unlikely motivated to execute a cyber attack resulting in widespread damage to the U.S. power grid due to the political consequences such a hostile act would likely guarantee. However, nation-state threat actors will undoubtedly continue to probe energy sector participants' networks and remotely accessible assets in order to learn about U.S. critical infrastructure.[141]

4.2.3. Iran

Iran uses its cyber program as a tool against political foes and for collecting intelligence, and has proven itself a highly motivated, although somewhat less sophisticated cyber actor compared to Russia and China. A 2016 U.S. federal indictment attributed a 2013 incident involving multiple remote intrusions of a control computer of the Bowman Dam in Rye, New York to private computer security teams operating on behalf of Iran's Islamic Revolutionary Guard.[142] From 2012 to 2013, Iran went after U.S. online banking sites, hitting them with

DDoS attacks. Overall, Iran and government-sponsored cyber-organizations throughout the country are continuing to expand their ability to conduct a major cyber attack.[143]

4.2.4. North Korea

Although less sophisticated,[144] the Democratic People's Republic of Korea (DPRK) has proven its intent to conduct cyber attacks are somewhat unpredictable, as in the 2014 Sony breach. The DPRK primarily focuses its cyber operations on intelligence collection rather than destruction, mainly directed at South Korea.[145] At the very least, the DPRK has a demonstrated interest in cyber warfare as a way to confront South Korean and U.S. capabilities.[146]

4.2.5. Terrorists

Terrorist groups such as ISIS have ambitious attack aims when it comes to cyber. While attempts to "take down" the U.S. power grid have been non-threatening to this point, pro-terrorist groups represent a highly visible threat, and ISIS has proven to be one of the most significant drivers of hacktivist activity throughout 2015.[147] However, though terrorist groups such as ISIS may have high motivation to disrupt or damage the power grid, they do not currently possess the sophisticated tools or skill necessary to execute a cyber attack that could have a widespread or significant impact to the power system.[148]

4.2.6. Hacktivists

Hacktivists – or ideologically motivated hackers – pose another cyber threat difficult to plan against. Groups such as Anonymous typically attack corporations and government agencies by exposing classified data or bombarding their systems with DDoS attacks. The National Security Agency stated that Anonymous might be able to cause a limited power blackout, and some federal officials believe Anonymous is headed in a more disruptive direction beyond attacking corporations and government websites.[149]

5. Government and Industry Risk Mitigation Practices

5.1. Federal and State Government Regulations and Guidelines

A variety of federal and state cyber security regulations and recommendations exist to guide U.S. utilities in how best to incorporate cyber security into general risk management practices. NERC is currently the only regulatory body with mandatory standards, though these apply compulsorily only to designated BES participants.[150] It should be noted that FERC designated NERC to develop these mandatory standards and to enforce them. Therefore, FERC also has oversight and power of enforcement. Broadly, the NERC CIP Version 6 standards include ten categories intended to establish CIP controls: BES Cyber System Categorization, security management controls, personnel and training, electronic security perimeters, physical security of BES Cyber Systems, system security management, incident reporting and response planning, recovery plans for BES Cyber Systems, Configuration Change Management and Vulnerability Assessments, and Information Protection.[151] Additionally, a framework, consisting of standards, guidelines, and practices,—although voluntary—is represented in the National Institute of Standards and

Technology's (NIST) *Cybersecurity Framework* and provides protocols designed for organizations of any size to implement cyber security practices.[152] Whereas NERC standards resemble a checklist of cyber security requirements, the NIST *Framework* is a process by which organizations may inventory their cyber security posture and make necessary adjustments based on findings.

Drawing from NERC standards, the National Association of Regulatory Utility Commissioners (NARUC) encouraged state utility commissions to adopt general NERC CIP principles and to make cyber security monitoring and evaluation a high priority for regulated utilities.[153] NARUC also encourages utility commissions to work with relevant organizations, such as the Department of Energy (DoE), Department of Defense (DoD), FERC, Edison Electric Institute (EEI), and NIST, on cyber security issues as well as training and education opportunities.[154] Some state public utility commissions, including those of Pennsylvania, Texas, and Missouri, independently require utilities under their jurisdiction to meet specific cyber security standards for non-BES facilities that are not subject to the NERC standards. These additional state level requirements include requirements such as possessing secure meter technology or emergency response plans in the event of a cyber incident, or making mandatory otherwise optional federal standards such as NERC CIP.[155] While mandatory requirements protect assets critical to energy transmission such as those of the U.S. BES, some utilities worry that "standards can lead to a focus on compliance at the expense of an overarching cybersecurity strategy,"[156] perhaps even impeding practical cyber security measures that might occur organically from a business operations or risk management perspective. NERC CIP Version 6 has taken steps to address some of these ongoing concerns, however states are still taking specific actions to protect the distribution system facilities that fall outside of the scope of NERC.

5.2. Industry Adoption of Regulations and Guidelines

Presently, utilities may perform system assessments to minimize the attack surface of generation facilities and identify potential attack vectors available to threat actors. For bulk power participants such as generation facilities, assessments must be conducted to satisfy the regulatory requirements of the NERC CIP standards related to Cyber Security (CIP-002, CIP-003, CIP-004,[157] CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, CIP-011).[158] Only bulk power utilities and applicable distribution facilities are required to meet these regulatory standards, though these entities make up a growing majority of the U.S. power grid. These standards contain a set of requirements detailing *what* utilities need to do, but *how* this is achieved is a utility's decision.

Beyond those bound to regulatory standards, utilities also perform assessments of cyber assets to protect against financial loss and for liability reasons. For example, INL's Consequence-Driven Cyber-Informed Engineering (CCE) process, a pilot program to help utilities assess and mitigate cyber vulnerabilities to operations, includes a system-of-systems breakdown of a utility's operations.[159] This allows analysts and engineers to view systems from logical, physical, functional, and communications perspectives, identifying potential system vulnerabilities. In generation, it is common to find a multiple-plant utility with different fuel sources at each location using combinations of vendor equipment at each plant for reliability or operability. However, if more than one plant uses the same configuration of equipment and with the same access controls, all plants are at risk if a cyber attacker discovers a way to compromise the equipment.

Mitigations to prevent failures throughout the transmission system exist, such as distributed high-voltage direct current (DC) interconnects that were designed to prevent widespread power outages.[160] The Federal Energy Regulatory Commission (FERC) and NERC regulate transmission, but regulators do not describe how utilities should achieve cyber security requirements,[161] or rate which strategies are more or less effective than others. Contingency strategies are developed by utilities to gauge the effects of a loss of individual elements, and a loss of facilities, by conducting transmission planning studies that identify critical transmission assets. The capability to perform this level of analysis at a regional or national grid scale becomes very challenging.[162] This electric system modeling and contingency analysis capability is critical to develop a wide area national grid view that can examine impactful system conditions (sustained power outages, for a large area or population).

5.3. Industry Best Practices and Ongoing Challenges

Many utilities understand the importance of cyber security and have developed or are developing a baseline for technical practices. In particular, the upgrade to the smart grid in the U.S. has required utilities to implement new technical practices to protect a vulnerable combination of communication, IT, and OT as well as protect customer privacy.[163] Smart grid software architecture developed or aided in development by utilities, such as the Secure Common Operating Environment (SCOE), has been used to mesh cyber security with smart grid technologies.[164] Furthermore, the smart grid upgrade will not only require robust cyber security, but will need to integrate physical security—that which provides protection to personnel, hardware, programs, networks, and data from unauthorized physical manipulation[165]—as well. In this domain, some utilities have begun securing supply chains to reduce vulnerability in vendor supplied equipment.[166]

To supplement technical and physical best practices, utilities are also increasingly participating in public and private partnerships, developing and using integrated frameworks, reorganizing how cyber threats are dealt with in utilities' workforce structure, and determining the organization level responsible for addressing cyber threats and overseeing the utility cyber security division.[167] For example, the Electricity Sub-Sector Coordinating Council Charter (ESCC)—a voluntary organization that was created to facilitate dialogue and information sharing about cyber threats, vulnerabilities, incidents and protective measures (in addition to other issues of interest to the sub-sector) among participants[168]—allows the electricity sub-sector to engage with participants and federal government about cyber threats, resiliency, and preparedness among other issues. Such practices suggest that utilities are becoming more responsive to cyber threats and making efforts to integrate approaches to security.

5.3.1. Technical Practices

There are a variety of specific technical and administrative cyber security best practices that utilities are implementing. These technical practices include network firewalls, antivirus software, application control software, encryption of communication data, securing smart grid technology upgrades, intrusion detection systems, etc.[169] Many of these practices were initially adapted IT security plans and were applied to electric utility software that controls a utility's physical OT. Much of the OT currently used by utilities was not designed with cyber security in mind, putting

the responsibility on utilities and partners to come up with innovative practices and solutions to protect the electric grid.[170] This reinforces the need for utilities to apply administrative practices to enhance technical and physical cyber security practices.

The first lines of defense utilities use to protect IT systems from malicious cyber activity are network firewalls. Firewalls must not only be able to block external threats, but must also block and control traffic to distinct internal zones of the network and separate the network into separate "trust" zones.[171] Boundaries for these trust zones are particularly important for utility networks that combine IT and OT systems. Non-existent or easily penetrated internal firewall boundaries allow a potential hacker easy access to any part of a utility's assets.[172] Some firewalls are now making use of a system known as deep packet inspection (DPI) to inspect network traffic traveling to and from control and automated systems and blocking inappropriate traffic.[173] DPI firewalls apply more detailed inspection to network traffic, rather than simply implementing a traditional black/white list method.[xiv] More specifically, DPI firewalls can be used to separate malicious data messages from benign ones. This is particularly useful in SCADA systems where malicious data messages need to be differentiated from routine control messages.[174]

Like most cyber security conscious businesses, many utilities implement some sort of antivirus software on networked computers to prevent traditional malicious cyber attacks. One alternative to traditional antivirus software that many utilities are starting to implement or consider is the use of secure application control software,[175] if supportable in an ICS environment. Application control software allows for a variety of trusted applications to be run in a critical infrastructure system. All other higher risk or dangerous applications are simply blocked and are not allowed to be executed in the system. This is in contrast to simply blacklisting known threats and allowing unknowns. In addition to increasing utility cyber security, utilities have found that some types of application control software can also reduce the number of required patching cycles and maintain regulatory security standards for utility systems.[176]

Another common practice many utilities have adopted is data encryption, particularly encryption of communication data. Encryption has long been used in IT systems to prevent undesirable third parties from intercepting and reading data messages. Some utilities currently use encryption software to encrypt SCADA communications to prevent hackers from collecting information on control processes for the electric grid.[177] Encryption is particularly important to utilities for protecting the privacy of smart meter communication data.[178] The emergence of smart grid metering technology in North America and around the world has made encryption of communication data an even higher priority for electric utilities. To ensure proper encryption, cryptographic protocols are already being developed, such as the IEEE[xv] P1711, to encrypt information transmitted from utility substations.[179] A recent survey shows that many utilities are moving toward implementation of encryption for substations. Of the utilities surveyed, 41% claim

[xiv] Blacklisting in the context of cyber security is a practice in which a host establishes a list of entities to be denied access, privileges, and/or recognition by the host and host services. Whitelisting is a similar practice in reverse, in which a host establishes a list of entities approved for access, privileges, and/or recognition; those not included in a whitelist will be denied.

[xv] The Institute of Electrical and Electronics Engineers (IEEE) is a professional association that produces publications and standards related to electrical engineering, computer engineering, information technology, and telecommunications.

to use encrypted protocols with the majority having encrypted protocols active in communication from the substation to the control station, as opposed to substation to substation or within the substation.[180]

As utilities in the U.S. begin to upgrade to an advanced metering infrastructure (AMI) technology smart grid, the security of this technology must also be kept up to date. With AMI technology comes inherent risks that can leave the smart grid vulnerable. The smart grid integrates a combination of OT, IT, and communication systems that comprise and connect the smart grid. This combination of technologies produces a variety of vulnerabilities to the smart grid with more device interconnections and bidirectional information flows which increase the likelihood of data breaches, and a broader digital surface to attack.[181] Utilities are addressing these security risks using a number of practices. San Diego Gas & Electric Company (SDG&E) cites three major foci for protecting the smart grid, namely "physical security, cyber security, and customer privacy."[182] To execute these foci, SDG&E established multiple-step physical security procedures including badging for authorized personnel to transmission facilities, 24-hour monitoring by on-site and remotely by security personnel,[183] using a dedicated cyber security lab to deploy and maintain new grid technology, and establishing an Office of Customer Privacy (OCP) to develop and maintain privacy and policy goals.[184] To protect the cyber-related aspects of the smart grid, Southern California Edison (SCE) has proposed smart grid software architecture, called the smart grid "Secure Common Operating Environment (SCOE)." The SCOE software builds on collaboration between SCE and a NIST architecture team and was designed to aid in the integration of smart grid systems and cyber security. This is the same NIST architecture team that developed a "NIST Smart Grid Conceptual Model" as a baseline for smart grid cyber security.[185] A major component of this architecture is ensuring secure communication between smart grid meters as well as other devices with the utility.

In terms of researching and developing new technology, some utilities are teaming with technology companies to enhance smart grid security, such as Sacramento Municipal Utility District (SMUD), which has teamed with Applied Communication Sciences (ACS) to enhance the security of AMI networks.[186] This partnership led to the development of an "Intrusion Detection System" for wireless radio frequency intrusion detection to the smart meter network, which was implemented in the spring of 2013. Although work remains to be done on this project, SMUD has reported that cyber security has been boosted by this system and that it has created some new security capabilities as well.[187] In July 2015, a partnership including Booz Allen Hamilton, Siemens, and Power Analytics was announced as the planning and development team for a series of future microgrid projects on behalf of New York utilities. Each company will contribute technical expertise or hardware to the projects: real-time patented microgrid technology (Power Analytics), technical architecture (Siemens), and cyber and physical security knowledge to reduce cyber vulnerabilities (Booz Allen Hamilton).[188] The partnership is unique in its application to microgrids, local electrical systems separate from the larger grid, and will identify if and how scale affects susceptibility of electrical grids to cyber incidents.

5.3.2. Employee Training for Cyber Hygiene

Cyber attackers may target utility employees with deceptive techniques such as spear phishing to gain access or information. According to Ponemon's 2014 *Critical Infrastructure* report, employee

use of personally owned devices accounted for 32% of specific security incidents reported by the critical infrastructure companies surveyed, second only to the use of insecure networks.[189] Some utilities conduct training to educate and even test employees' cyber and physical security awareness. For example, the New York Power Authority (NYPA) briefs its employees "on specific cyber risks and threats and on preemptive strategies," such as avoiding use of USB sticks or similar peripherals distributed at a conference or other public places on company equipment.[190] Some utilities require employees to undergo online training, the efficacy of which is later assessed by an internal mock exercise. While technological redundancies are generally recommended, cyber security training including physical security has been adopted by utilities to mitigate the risks posed by their employees.[191]

5.3.3. Supply Chain Security

When upgrading and retrofitting components of the electric grid, it is important to ensure that this equipment is purchased from a reputable vendor with reliable products. Many utilities are now taking the time to ensure that purchased equipment comes from a reliable vendor and that hardware or software is free of major security flaws. Some utilities such as SMUD are considering working with vendors to ensure that hardware and software security is a high priority, even going as far as designating an officer to work with business lines and evaluate security risks.[192] As utilities upgrade to a smart grid, it has become necessary to ensure vendors selling metering technology implement necessary security precautions such as meter encryption, firmware management, etc.[193]

One method that will soon be used to decrease cyber security risk to both hardware and software are standards certifying that a product purchased from a vendor was designed securely. Based on standards currently being implemented in the IT industry, some organizations have been pushing the development of vendor certification standards for securing electric grid control system products, such as the International Society of Automation (ISA), which proposed a set of standards known as ISA99. Use of standards such as these have already been implemented for IT industry purposes to certify computer software product security under the "Common Criteria for Information Technology Security Evaluation 155" and have significantly helped in bolstering the cyber security of network IT systems.[194] In response to this push, FERC, as of July 2016, has ordered NERC to develop a set of supply chain security standards.[195] This FERC order is an essential first step in the development of standards for shoring up vulnerabilities in vendor purchased technology and improving the overall cyber security of the affected hardware and software.

5.3.4. Industry Administrative Practices

In addition to specific technical and physical practices, individual utilities across the United States are developing administrative methods to protect against cyber attacks on their IT and OT systems. These include utility cooperative security projects, structuring of utility cyber response programs, integration of physical and cyber security, and other practices to mitigate cyber risks.

Utility partnerships have been organized for the purpose of comparing cyber security practices, ensuring best practices are up to date, and supporting cyber security research. The partnerships are created between utilities and other organizations including technology companies, equipment

vendors, state and federal government organizations, as well as other utilities. Cyber security research is a key outcome for many cooperative agreements between utilities. One cyber security progressive organization, the Edison Electric Institute, has created a "Threat Scenario Project" with the intent to bring together different groups allowing cyber security professionals to evaluate areas of improvement for utility security.[196] Another utility, Pacific Gas & Electric (PG&E), recently conducted its first enterprise-wide cyber and physical security exercise in collaboration with Booz Allen Hamilton, after participating in the NERC GridEx II event.[197] Additionally, utilities such as PG&E have provided funding to universities to boost research and interest in cyber security. PG&E has provided an $80,000 grant to California Polytechnic State University's Cyber security Center to create collaboration among academia, private utility companies, and government defense agencies.[198] Other utilities have teamed with state governments. For example, Hawaiian Electric has joined a group led by the state of Hawaii and several federal government agencies to predict and prevent cyber threats and risks to the Oahu electric grid.[199] The partnering of U.S. utilities with a wide variety of organizations and institutions has given many utilities an advantage in boosting grid cyber security by obtaining a wide range of information and expertise in developing secure technology and software.

In addition, utilities are improving the way they respond to cyber threats through collaborative practices in operations planning within each utility. One organization-wide approach for identifying, evaluating, and mitigating cyber threats is the development and use of a framework. With the involvement of business, operations, engineering, and cyber staff, the process by which critical systems of a utility or other infrastructure entity could be compromised is examined in phases, to include the planning necessary to execute an attack and mapping of an "ICS Kill Chain," or steps necessary for an attacker to achieve a cyber attack goal.[200] This helps utilities identify critical operations assets and upgrade or implement new cyber security practices if additional vulnerabilities are discovered.

Some utilities are also reorganizing the way in which cyber threats are dealt with in each company's workforce structure to combat them more effectively. Recently, some utilities have been moving toward incorporating physical security into their cyber security centers to create a "centralized operations center" organized under a Chief Information Security Officer (CISO) responsible for cyber security.[201] This centralized operations center generally works toward meshing IT with physical OT. Other utilities such as the Salt River Project have their cyber security risk management program located in the IT Security department and reporting directly to the Chief Financial Executive of the financial business unit.[202]

Some utilities suffer from a lack of ground level cyber expertise. According to a recent survey, 37% of utilities surveyed make cyber security decisions at the executive level, 47% at the management level, and only 16% by professional staff.[203] Another recent survey states that only 15% of cyber security senior management at utilities actually have a direct line of reporting to the company's Board of Directors.[204] This is particularly troubling considering the number of utilities that make cyber security decisions at the executive level. If those responsible for developing and implementing cyber security practices within an entity lack direct communication with individuals who oversee the entity as a whole, it is less likely that changes to or new cyber security policies will be adopted at the same pace that new vulnerabilities and threat actors emerge. Among a minority of utilities whose security line of effort passes through each level of company hierarchy,

the Board of Directors of Xcel Energy is regularly provided updates on cyber security from the company's cyber security program. The executives of Xcel also actively work to improve cyber security in industry and government, with their CEO being a member of an industry subcommittee recommended by the National Infrastructure Advisory Council (NIAC), which provides information and advice to the President of the U.S.[205]

6. Findings and Identified Needs

6.1. Opportunities for Further Federal Government Engagement

Beyond the best practices that utilities currently have in place, many U.S. utilities have stated that there are specific areas in which the federal government could engage to aid utilities in protecting the electric grid from cyber threats. These areas include increased protection of information shared between utilities and the government, protection from liability based on this information, federal initiative in prosecuting cyber attackers,[206] and federal grants and oversight for upgrading and insuring cyber security systems.[207]

6.1.1. Information Sharing

In terms of dealing with electric grid cyber security threats, the effectiveness of the relationship between the federal government and utilities is largely dependent on the sharing of threat intelligence between the two entities. The confidentiality of the information shared between these entities is a primary concern for utilities as well as the government. It therefore comes as no surprise that many organizations, such as the Edison Electric Institute, are calling for federal legislation that would provide greater safeguard of information that utilities share with federal government agencies.[208] Businesses fear general public disclosure as well as use of shared information for regulatory activities that could in turn lead to penalties. For smaller utilities such as those at the municipal level, civil lawsuits that arise as a result of sharing information about a cyber incident with the government can be costly.[209] Between 2011 and 2015, broad measures were proposed to Congress that would limit liability for cyber incidents and protect infrastructure owners from criminal and civil legal action for punitive damages, if the owner was in compliance with suitable cyber security practices,[210] but no laws were passed as a direct result of these efforts.

Currently, the Protected Critical Infrastructure Information (PCII) Program exists to facilitate the secure sharing of voluntarily provided information between infrastructure owners and operators, such as utilities, and the government to identify and mitigate vulnerabilities.[211] PCII protects shared owner and operator data from being used in regulatory actions, civil litigation, Freedom of Information Act (FOIA) disclosures, and state disclosure laws, but PCII data is also highly controlled and only accessible by trained and certified federal, state, and local government employees and contractors.[212] The lack of a bidirectional information flow may delay other utilities' efforts to remedy connected or similar vulnerabilities in a timely manner.

Some efforts have also been made by federal government agencies to work with private utilities to process and disseminate utility and government held information, the effective sharing of which can be hindered by slow-moving declassification procedures. One such effort was the

establishment of the Electricity Information Sharing and Analysis Center (E-ISAC) in 1998, which coordinates operations with the Department of Homeland Security and the Department of Energy to distribute declassified cyber threat information to utilities.[213] Currently, the E-ISAC is a group within NERC and because NERC is also responsible for standards development and enforcement, some utilities have been reluctant to share potentially non-regulatory conforming information with E-ISAC.[214] In recent years the E-ISAC has established and communicated many policy components in an effort to eliminate this concern from utilities. The establishment of the E-ISAC does not fully reconcile the inaccessibility of information due to classification or a lack of utility personnel with security clearances, therefore utilities may find benefit in achieving greater access to federally held information related to cyber security. Currently, only some federal information sharing programs are equipped to share classified information with critical infrastructure sector participants, and depend on participants' eligibility for and holding of an active clearance. Without the required security clearances, many utilities are unable to quickly access important government-controlled information in the event of a cyber emergency.[215] These programs, such as DHS's Cyber Information Sharing and Collaboration Program (CISCP), also have additional requirements in order to receive classified information such as having Cooperative Research and Development Agreements (CRADA) in place with participants.[216] In October 2015, the Cybersecurity Information Sharing Act of 2015 (CISA 2015) was passed, providing greater liability protections to utilities that voluntarily share cyber threat information with the government and aims to facilitate better real-time sharing of threat information with participating entities.[217] The Department of Homeland Security will serve as the distributor and repository for cyber security information shared among utilities and government agencies, but because the bill including CISA 2015 only passed into law in December 2015, the efficacy of CISA 2015 to utilities in addressing cyber threats is yet unknown.

6.1.2. Industry Concerns about the Quality of Information Sharing Programs

When asked about current federal engagement or policies related to the electricity sector, utilities often express concern about penalties associated with information sharing.[218] Newer legislation such as CISA 2015 has garnered support from utilities that see it as a facilitator of more meaningful cyber security information sharing while maintaining a balance between liability and privacy protections.[219] The federal government should respond adaptively to utility concerns, taking into account utility concerns about sharing minimal information or meeting minimum regulatory standards for the sake of compliance rather than cyber security. However, as CISA 2015 is implemented and other information sharing mechanisms are created, the government should be aware of and prepared to allay confusion regarding which sharing programs contain or exclude liability protections and limitations.[220]

6.1.3. Providing Resources for Industry Cyber Upgrades

Another proposition put forth by utilities is the conferring of federal grants and low-interest loans for upgrading existing and investing in new cyber security systems, as well as government acknowledgement of correct action when investing in and insuring these cyber security systems. Many utilities and businesses have found some difficulty in keeping cyber security up to governmental standards as this can be costly in most instances. Therefore, added financial incentives to upgrade cyber systems and equipment may encourage utilities to better conform to

standards and cooperate more effectively with government agencies. More specifically, federal grants and loans could be used to offset costs of developing emergency response plans that coordinate with the government, as well as vulnerability assessments of existing cyber systems.[221] Aid from DOE has already been granted to some utilities such as SMUD, which received $127.5 million to invest in smart grid security programs.[222] However, many utilities will require additional funding as smart grid and other technology progresses.

Some utilities have also asked for oversight in the upgrading of utility cyber security systems and the updating of cyber insurance policies. In particular, DOE could work directly with utilities and industry suppliers to assess cyber security investments by developing metrics for evaluation of these investments. Additionally, DOE or other government agencies could provide funding to cyber security research efforts in industry, with a specific focus on evaluating new investments in cyber security and the relative effectiveness of these investments in protecting utilities against cyber attacks.[223] Additionally, federal support would likely benefit vendors and manufacturers of technologies requiring embedded or applied cyber security measures, since third party equipment and software is necessary in utility operations. As utility OT equipment is upgraded, the federal government could also be a key resource in providing or updating cyber insurance policies. Currently, OT systems are often overlooked in most cyber insurance policies and physical damage to an OT system is often not covered.[224] As OT cyber attacks are only likely to become more common in the future, a pertinent approach would be for the federal government to help develop cyber insurance policies that take into account new cyber security upgrades and insure against damage to utility OT systems.

6.1.4. Implementing Specific Regulatory Requirements

Some utilities also require assistance in creating or shaping their cyber strategy, both to meet regulatory standards and for business security. The government should also consider ways to assist utilities in requests to upgrade cyber security systems—this might include grants for physical equipment additions or upgrades, cyber research funding, or assistance in acquiring or upgrading cyber insurance policies.

NERC addresses emerging cyber threats in iterations of NERC CIP, but to truly aid bulk power participants, more attention should be paid to existing implementations instead of simply handing down a checklist of items. Regulatory "blind spots," such as a lack of guidance for serial-based communications commonly found in utility operations,[225] may be better understood in the future by greater interchange with utilities about systems planning and organization. Feedback from utilities should be incorporated, where possible, in newer versions of NERC CIP and other cyber security standards used in the power industry.

6.1.5. Jurisdictional Challenges

Because the distribution system is not federally regulated, the implementation of cyber security practices largely depends on each state government's individual guidance. For this reason, the impact of a cyber attack on a distribution system may vary between states, depending on where state regulatory lines are drawn around securing distribution transformers and other equipment. The impact of a cyber attack is also dependent on the size of the utility and the utility's

corresponding cyber security budget. Over the next few decades the emergence of the smart grid is likely to blur the lines of jurisdiction between transmission and distribution systems.[226] Unless regulation or other best-practice guidance is implemented across distribution systems, the risk of cyber attacks with greater consequences to power delivery, such as the 2015 attacks in Ukraine, may become more prevalent in the U.S.

6.1.6. Legal Challenges

Federal authorities need to more solidly define what constitutes a cyber attack/crime, and establish countermeasures. Establishing clear legal terms defining what constitutes a cyber attack and outlining what responses the government will take against threat actors is essential for cyber defense/deterrence. This will demonstrate to utilities, vendors, and other electric sector participants that positive efforts to improve cyber security posture are supported by law.

A federal program intended to help utilities deter cyber attackers by providing a swifter legal process and eventual prosecution of perpetrators is currently in development. "Current law prohibits businesses from doing anything more than attempting to defend their networks with firewalls and other security software, and collecting information on attacks"[227]—capabilities that many utilities are only now adopting or expanding to meet current threats. With growing cyber threats to critical infrastructure particularly in mind, in 2012 the Department of Justice's National Security Division created the National Security Cyber Specialists Network (NSCS), an organization of federal agents and prosecutors with experience in cyber security-related technology, crime, and law, to improve protocols for providing assistance to entities such as utilities[228] in identifying and apprehending cyber attackers. However, this is dependent on a utility having the capability to detect and capture data about cyber intrusions that can then be provided to law enforcement. Further, a successful joint federal-industry effort would require law enforcement to be familiar with and prepared to engage with companies to build prosecutions within guidelines covering information sharing, privacy and civil liberties.[229] If organizations such as NSCS are tasked to work with the energy sector, it will likely be some time before the latter is prepared to provide the data necessary for effective judicial actions to take place. With the increasing number of cyber attacks on critical infrastructure elements, federal organizations could easily become overwhelmed by the sheer volume of utilities' requests for assistance.

6.2. Opportunities for Improving Electric Sector Industry Cyber Security

6.2.1. Develop and Adopt Tools

Preparing for the coming smart grid provides utilities with an opportunity to incorporate new and existing cyber security tools into operations when upgrading technology. A long-established application, intrusion detection is a recurrent shortcoming reported by utilities in recent surveys regarding cyber security posture.[230] The absence of intrusion detection systems (IDS) and monitoring in IT and OT networks[231] means utilities cannot obtain forensic data related to cyber intrusions and attacks. All utilities should have intrusion detection and monitoring tools in place, even as a minimum cyber security procedure. Organizations have varying monitoring conditions

and nearly all utilities will require different IDS specifications, therefore development of customizable IDS that utilities can easily integrate into existing networks is a practical measure.

Increased attribution capabilities will aid in deterring threat actors, who largely rely on anonymity. Threat actors consistently adapt to every defensive measure employed at a private, local, and national level. It is essential that government and private research and intelligence entities continue to widen their analysis of cyber threat actors and attack vectors. Further, utilities should keep abreast of vulnerability and threat trends throughout the electric sector and ICS in order to efficiently maintain defenses. This can be achieved in part by monitoring information security vulnerability databases, such as the Common Vulnerabilities and Exposures (CVE) database maintained by the MITRE Corporation,[232] or ICS-CERT's Advisories that provides information about security issues, vulnerabilities and exploits,[233] and by conducting vulnerability assessments. Vulnerability assessments may illuminate overlooked hazards associated with remote and mobile connectivity, but are valueless if not conducted regularly as personnel turnover, network changes, and new device connections are established and new vulnerabilities are discovered.

6.2.2. Continue to Foster and Establish Industry Partnerships

Partnerships between utilities, vendors, and academic institutions allow electric sector stakeholders to develop equipment and practices to improve cyber security strategies. Utilities should welcome research opportunities and collaborative exercises to strengthen overall cyber security posture, for instance leveraging the technical expertise of vendors when planning future microgrid projects as in the case of New York utilities,[234] or participating in security exercise events such as GridEx.[235] Relationships among electric sector stakeholders should also seek to create greater communication between utilities and vendors about equipment security. Such mechanisms should enable feedback about utility cyber security needs and regulatory requirements to equipment vendors. Collaborative efforts are particularly important as the grid modernizes and utilities incorporate a new generation of "smart" technology into critical operations. Partnerships such as that of the Sacramento Municipal Authority (SMUD) and Applied Communication Sciences (ACS) to research and develop cyber security tools for the former's smart meter network[236] can generate practical cyber security measures and help vendors produce more effective equipment in support of utility operations.

6.2.3. Identify and Implement Effective Cyber Hygiene Practices

The array of federal and state cyber security regulations and recommendations that exist to guide U.S. utilities in how best to incorporate cyber security into general risk management practices is diverse. Cyber hygiene practices of U.S. utilities, either in response to mandatory standards or for general business and operations security, are similarly varied, yet most utilities that experience cyber intrusions or attacks are compromised via the same threat vectors—phishing and malware.[237] Future research about cyber hygiene practices among utilities used to combat or mitigate cyber threats should provide the electric sector with perspective of the cyber threat landscape, and should initiate the incorporation of cyber hygiene practices in utilities where they are not already used, such as better device and network passwords, IT and OT network segregation and monitoring, and personnel training. Given the constant, even daily number of cyber intrusions reported by some utilities,[238] the industry should seek a more comprehensive understanding of which hygiene techniques are and are not effective against common, prevailing cyber threats.

6.2.4. Remain Flexible Throughout Regulatory Update Process

The shift to a smart grid will mean that utilities will add thousands of devices to their operations including new sensors, controllers, relays, meters, etc.[239] Further, cyber security is unlikely to be the top priority for new electricity subs-sector participants, such as distributed energy resource (DER) stakeholders, that will introduce additional digital complexity to power systems. This will mean several new policies, as well as changes to existing ones. Grid participants should prepare for the impending changes and take an active role in grid modernization and technology regulation. Despite current (and future) regulation and best-practice recommendations, older equipment and new connectivity models are still vulnerable to attack.[240] Utilities should still conform to regulations and apply best practices, but be aware and ready for the fact that if a targeted attack happens, they will be penetrated. Utilities, organizations, and the government must have policies in place to be ready to respond and react to successful attacks.

7. Conclusions

In the coming years, cyber threats to utilities are likely to grow in number and sophistication. ICS attacks are becoming increasingly more targeted and sophisticated, with trusted communications networks, remote access, mobile devices, vendors, and supply chains are the most likely routes of ingress. An advanced threat actor with the appropriate attack vector will get in regardless of what defenses are in place. This does not mean that a cascading attack on the U.S. BES is imminent. However, the definitions of what constitute cyber warfare or cyber crime are blurry at best, and attribution can be nearly impossible at times, which serves to encourage threat actors' motivations. Nation-states and non-state actors alike can only improve their cyber attack capabilities. Therefore, with the evolvement of the smart grid creating even more vulnerabilities, we should be prepared to see threat actors trying to duplicate or surpass the capabilities that have been demonstrated in Ukraine.

The impact of a cyber attack can be severe for utility companies, vendors, and the public. This report does not suggest a cyber-apocalypse is going to occur. However, there is no mitigating effort that can be 100% effective. A defense mechanism that works today may not be effective tomorrow – the ways and means of cyber attacks constantly change. It is critical all energy sector participants remain aware of changes in cyber security and continue to work to prevent potential vulnerabilities in the systems they manage.

Recognizing this, many U.S. utilities have taken the initiative to prevent and mitigate cyber threats through the development and implementation of a set of best practices. In spite of these best practices, utilities will continue to require help from the federal government in maintaining cyber preparedness, obtaining threat information, and combating cyber threats as they are occurring. Based on the significance of critical infrastructure sectors such as energy in broader national security strategy, it is in the interest of the federal government to ensure updates to current cyber security regulations to address evolving and emerging threats. To fulfill the federal vision for energy sector security and resilience,[241] increasing cooperation between government and energy sector members is likely necessary. The best practices of utilities for dealing with emerging cyber threats may be significantly enhanced by aid from the federal government in a number of

meaningful ways, possibly through the enactment of new legislation and federal programs. However, utilities must demonstrate commitment to cyber security beyond business risk practices by continuously evaluating and implementing practical measures such as cyber hygiene and intrusion detection mechanisms.

Establishing cyber security for the bulk power grid can be both expensive and time consuming. However, every effort to prevent, track, and respond to attacks is key to maintaining cyber security in this increasingly critical field.

8. Appendix A: Glossary

Alternating current (AC). An electric current in which the flow of electric charge periodically reverses direction. AC is the form in which electricity is delivered to businesses and homes.

Advanced Persistent Threat (APT). A network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.

Automatic Generation Control (AGC). A system for adjusting the power output of multiple generators at different power plants, in response to changes in the load.

Advanced metering infrastructure (AMI). Advanced metering systems comprise state-of-the-art electronic/digital hardware and software, which combine interval data measurement with continuously available remote communications. These systems enable measurement of detailed, time-based information and frequent collection and transmittal of such information to various parties.

Authentication. Allowing access to resources in an information system.

Black start. A black start is the restoration of a power station without reliance upon the external power transmission system. Black start capabilities are often provided by small co-located diesel generators which are used to start larger generators, which in turn start the main power station generators.

Bulk electric system (BES). A large interconnected electrical system made up of generation and transmission facilities and their control systems. A BES does not include facilities used in the local distribution of electric energy.

Blacklisting. A reverse practice of Whitelisting, in Blacklisting a host establishes a list of entities to be denied access, privileges, and/or recognition by the host and host services.

Configuration. Step in system design; for example, selecting functional units, assigning their locations, and defining their interconnections.

Cyber attack. An attempt to infiltrate information technology systems, computer networks, or individual computers with a malicious intent to steal information, cause damage, or destroy specific targets within the system.

Direct current (DC). An electric current in which the flow of electric charge is unidirectional. High-voltage DC current is used to transmit electricity over long distances.

Distributed control system (DCS). In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit.

Distributed Denial of Service (DDoS). The prevention of authorized access to multiple system resources or the delaying of system operations and functions.

Distributed Network Protocol (DNP3). A set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Deep packet inspection (DPI). A network surveillance technology that enables operators to scan Internet traffic in real time and make automated decisions about what to do with it.

Encryption. Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

Ethernet. The most widely used local area network (LAN) technology. The Ethernet access method is used to connect computers in a company or home network as well as to connect a single computer to a modem for Internet access. Ethernet uses cables to connect computers; Wi-Fi is its wireless counterpart, and both technologies are used together.

Exploit. A piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.

Firewall. An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall).

Human-machine interface (HMI). The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.

Input/Output (I/O). A general term for the equipment that is used to communicate with a computer as well as the data involved in the communications.

Industrial control system (ICS). A general term that includes several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), Programmable Logic Controllers (PLC) and others often found in industrial and critical infrastructure sectors. An ICS consists of combinations of control components that act together to achieve an industrial objective.

Information and Communications Technology (ICT). A general term that includes any communication device or application, encompassing: radio, television, cellphones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them. Alternatively, this term refers to technology that allows users to transmit and receive information and data as well as manipulate, store, and retrieve this information.

Intrusion detection system (IDS). A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intelligent electronic device (IED). Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source.

Internet protocol (IP). The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables Internetworking, and essentially establishes the Internet.

Information technology (IT). The application of computers to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise.

Malware. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Malware includes viruses, worms, and Trojans.

Modbus. A serial communications designed for use with programmable logic controllers (PLCs). Modbus protocol itself provides no security against unauthorized commands or interception of data.

Operational technology (OT). Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Patching. The act of applying updated software to an existing program or computer system to improve, support, or repair it. This includes mitigating cyber vulnerabilities.

Payload. Malicious software or a computer virus that produces a harmful effect(s) in a target system to which a payload is delivered. The "delivery" of a payload refers to the vector, or path by which an attacker introduces the payload to a target.

Phishing. A technique by which an attacker uses email to attempt to lure victims to disclose personal information, open attachment files or links that will cause the victim to download malware, or provide the attacker with unauthorized access to a computer, network, or application.

Programmable logic controller (PLC). A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, communication, and data and file processing.

Protocol. A set of rules to enable, implement and control some type of association (e.g., communication) between systems.

Ransomware. A kind of virus designed to deny a victim access to the victim's digital property until the victim provides a ransom payment.

Remote access Trojan (RAT). A malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment.

Remote terminal unit (RTU). A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment.

Risk. The potential for loss, damage, or destruction of a specified asset.

Supervisory control and data acquisition (SCADA). A generic term for computerized systems that are capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution systems. SCADA was designed for the unique communication challenges posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.

SHODAN. An open source web-based search engine for identifying devices connected to the Internet, including ICS components.

Smart grid. An electrical grid which includes a variety of digital elements including smart meters, smart appliances, renewable energy resources, and energy efficiency resources. Smart grids rely on bidirectional communication among control, devices, and equipment.

Spear phishing. A more specifically-targeting technique related to phishing, by which an attacker uses email to attempt to lure a victim to open attachment files or links that will cause the victim to download malware or provide the attacker with unauthorized access to a computer, network, or application. The victim may be carefully selected by the attacker using social engineering techniques based on the victim's access to specific items.

Spoofing. The act of gaining unauthorized access to a network by sending falsified messages to a target computer IP address that appear to be sent from a trusted host.

Substation. A part of an electrical generation, transmission, or distribution system. Substations transform voltage from high to low, or the reverse, or perform any of several other important functions such as reactive power compensation and overcurrent/overload protection.

System-of-system. A collection of task-oriented systems that, when functioning together create a more complex system of greater functionality and performance than the sum of constituent systems.

TCP/IP. The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network.

Threat. An entity that can cause damage to a specified asset through the exploitation of a vulnerability.

Traffic Light Protocol (TLP). A set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).

Transformer. An electrical device that transfers electrical energy between two or more circuits through electromagnetic induction. Transformers are used to increase or decrease the alternating voltages in electric power applications.

Trojan. A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Universal Serial Bus (USB). An external bus standard that supports data transfer rates of 12 Mbps. USB peripherals, such as storage sticks allow quick, mobile transfer of data to other devices with USB ports.

Very-small-aperture terminal (VSAT). Small two-way satellites often used in the electricity sector to transmit data via broadband Internet to and from remote locations such as power grid substations.

Vulnerability. Weaknesses or security gaps that can be exploited by malicious entities to gain access to an asset.

Watering hole attack. A technique in which an attacker infects a website with malware with the intent that a target group of users who frequent the site will access it, and that at least some users will unknowingly download the malware.

Whitelisting. A reverse practice of Blacklisting, in which a host establishes a list of entities approved for access, privileges, and/or recognition; those not included in a whitelist will be denied.

9. Appendix B: Acronyms & Initialisms

Applied Communication Sciences (ACS)

Chief Information Security Officer (CISO)

Common Vulnerabilities and Exposures (CVE)

Consequence-driven Cyber-informed Engineering Process (CCE)

Critical Infrastructure Protection (CIP)

Cybersecurity Information Sharing Act of 2015 (CISA 2015)

Democratic People's Republic of Korea (DPRK)

Department of Defense (DoD)

Department of Energy (DoE)

Department of Homeland Security (DHS)

Department of Justice (DoJ)

Edison Electric Institute (EEI)

Electricity Information Sharing and Analysis Center (E-ISAC)

Federal Energy Regulatory Commission (FERC)

Freedom of Information Act (FOIA)

Idaho National Laboratory (INL)

Independent system operator (ISO)

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

Institute of Electrical and Electronics Engineers (IEEE)

International Electrotechnical Commission (IEC)

International Society of Automation (ISA)

Investor-owned utility (IOU)

National Association of Regulatory Utility Commissioners (NARUC)

National Infrastructure Advisory Council (NIAC)

National Institute of Standards and Technology (NIST)

National Security Agency (NSA)

National Security Cyber Specialists (NSCS)

North American Electric Reliability Corporation (NERC)

New York Power Authority (NYPA)

Office of Customer Privacy (OCP)

Pacific Gas & Electric (PG&E)

Protected Critical Infrastructure Information Program (PCII)

Sacramento Municipal Utility District (SMUD)

San Diego Gas & Electric Company (SDG&E)

Southern California Edison (SCE)

References

1. Daughtery, Will, "Lloyd's Report Highlights Risk of Cyberattacks on National Power Grid," Data Privacy Monitor, May 23, 2015, accessed December 17, 2015, www.dataprivacymonitor.com.

2. "Frequently Asked Questions about Cyber Security and the Electric Power Industry," Edison Electric Institute, October 2014, accessed September 24, 2015.

3. Assante, Michael, Tim Roxey, and Andy Bochman, "The Case for Simplicity in Energy Infrastructure," Center for Strategic & International Studies, October 2015, accessed December 22, 2015.

4. "Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015," PWC, September 30, 2014, accessed September 30, 2015.

5. "ICS-CERT Monitor September 2014—February 2015," ICS-CERT, March 11, 2015, accessed November 9, 2015.

6. "NCCIC/ICS-CERT 2015 Year in Review," NCCIC and ICS-CERT, April 19, 2016, accessed July 21, 2016.

7. "ICS-CERT Monitor September 2014—February 2015," ICS-CERT, March 11, 2015, accessed November 9, 2015.

8. "NCCIC/ICS-CERT 2015 Year in Review," NCCIC and ICS-CERT, April 19, 2016, accessed July 21, 2016.

9. "ICS-CERT Monitor September 2014—February 2015," ICS-CERT, March 11, 2015, accessed November 9, 2015.

10. "Plug In: EY's Latest Insights for Power & Utilities," EY, February 2014, accessed October 26, 2015.

11. "Plug In: EY's Latest Insights for Power & Utilities," EY, February 2014, accessed October 26, 2015.

12. "Critical Infrastructure: Security Preparedness and Maturity," Ponemon Institute: Unisys, July 2014, accessed September 30, 2015.

13. Assante, Michael, Tim Roxey, and Andy Bochman, ”The Case for Simplicity in Energy Infrastructure,” Center for Strategic & International Studies, October 2015, accessed December 22, 2015.

14. Assante, Michael, Tim Roxey, and Andy Bochman, ”The Case for Simplicity in Energy Infrastructure,” Center for Strategic & International Studies, October 2015, accessed December 22, 2015.

15. Vinton, Kate, “Hacking Gets Physical: Utilities At Risk For Cyber Attack,” Forbes, July 10, 2014, accessed December 22, 2015, www.forbes.com.

16. “ICS-CERT Monitor September 2014—February 2015,” ICS-CERT, March 11, 2015, accessed November 9, 2015.

17. Wueest, Candid, “Targeted Attacks Against the Energy Sector,” Symantec, January 13, 2014, accessed October 8, 2015.

18. Hayden, General (Ret). Michael, Remarks of Hayden to Bipartisan Policy Center, "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat," 1225 Eye St. NW, Washington, D.C., 28 February 28, 2014.

19. Wueest, Candid, “Targeted Attacks Against the Energy Sector,” Symantec, January 13, 2014, accessed October 8, 2015.

20. “ICS-CERT Monitor January 2014—April 2014,” ICS-CERT, May 16, 2015, accessed November 9, 2015.

21. “ICS-CERT Monitor January 2014—April 2014,” ICS-CERT, May 16, 2015, accessed November 9, 2015.

22. Kovacs, Eduard, "Attackers Using Havex RAT Against Industrial Control Systems,” Securityweek, June 24, 2014, accessed November 10, 2015, www.securityweek.com.

23. "Dragonfly: Western Energy Companies Under Sabotage Threat" Symantec Security Response, June 20, 2014, accessed November 9, 2015, www.symantec.com/connect/blogs.

24. Kovacs, Eduard, "Attackers Using Havex RAT Against Industrial Control Systems,” Securityweek, June 24, 2014, accessed November 10, 2015, www.securityweek.com.

25. "Alert (ICS-ALERT-14-281-01B) Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)," ICS related alert issued 10 December 2014, accessed November 9, 2015, https://www/ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

26. Overton, Thomas, “DHS Issues New Alert on ICS Malware,” Power Magazine, November 5, 2014, accessed November 10, 2015, www.powermag.com.

27. “BlackEnergy Threatens U.S. infrastructure,” Government Security News, September 11,

2014, accessed November 9, 2015, www.gsnmagazine.com.

28. "Alert (ICS-ALERT-14-281-01B) Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)," ICS related alert issued 10 December 2014, accessed November 9, 2015, https://www/ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

29. Wueest, Candid, "Targeted Attacks Against the Energy Sector," Symantec, January 13, 2014, accessed October 8, 2015.

30. Morain, Dan, "Hackers Victimize Cal-ISO," Los Angeles Times, June 9, 2001, accessed November 11, 2015, www.latimes.com.

31. "Cyber-Physical Systems (CPS)," National Science Foundation's Cyber-Physical Systems Research Guidelines, accessed May 6, 2016, http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286&org=NSF&sel_org=NSF&from=fund.

32. Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, "NIST 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, May 2015, accessed May 1, 2016.

33. McLarty III, Thomas F., and Thomas J. Ridge; Project Chairs, "Securing the U.S. Electrical Grid," Center for the Study of The Presidency & Congress, October 2014, accessed February 16, 2016.

34. "The Critical Security Control for Effective Cyber Defense Version 5.0," Council on Cyber Security, February 2014, accessed May 2, 2016.

35. "ICS-CERT Monitor January 2014—April 2014," ICS-CERT, May 16, 2015, accessed November 9, 2015.

36. "Challenges in Securing the Electricity Grid: Statement of Gregory C. Wilshusen," U.S. Government Accountability Office: Testimony before the Committee on Energy and Natural Resources, U.S. Senate Director Information Security Issues, July 17, 2012, accessed February 17, 2016.

37. Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn, "NIST 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, May 2015, accessed May 1, 2016.

38. Campbell, Richard J., "Cybersecurity Issues for the Bulk Power System," Congressional Research Service, June 10, 2015, accessed February 15, 2016.

39. Zetter, Kim, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed February 15, 2016, www.wired.com.

40. “Industrial Control System (ICS) Security,” Corero Network Security, 2014, accessed February 22, 2016.

41. Weiss, Joseph, Protecting Industrial Control Systems from Electronic Threats (New York, N.Y: Momentum Press, 2010), 36-37.

42. “Industrial Control System (ICS) Security,” Corero Network Security, 2014, accessed February 22, 2016.

43. “High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,” U.S. Department of Energy and North American Electric Reliability Corporation, June 2010, accessed February 16, 2016.

44. “Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations,” U.S.—Canada Power System Outage Task Force, April 2004, accessed March 14, 2016.

45. “Strategy for Securing Control Systems,” ICS-CERT, October 2009, accessed February 15, 2016.

46. “Strategy for Securing Control Systems,” ICS-CERT, October 2009, accessed February 15, 2016.

47. Assante, Michael J., and Robert M. Lee, “The Industrial Control System Cyber Kill Chain,” SANS Institute, October 2015, accessed February 24, 2016.

48. “High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,” U.S. Department of Energy and North American Electric Reliability Corporation, June 2010, accessed February 16, 2016.

49. Govindarasu, Manimaran, Adam Hahn, Peter Sauer, Cyber-Physical Systems Security for Smart Grid, Power Systems Engineering Research Center, February 2012, accessed February 25, 2016.

50. Govindarasu, Manimaran, Adam Hahn, Peter Sauer, Cyber-Physical Systems Security for Smart Grid, Power Systems Engineering Research Center, February 2012, accessed February 25, 2016.

51. Govindarasu, Manimaran, Adam Hahn, Peter Sauer, Cyber-Physical Systems Security for Smart Grid, Power Systems Engineering Research Center, February 2012, accessed February 25, 2016.

52. "Mouse Click Could Plunge City into Darkness, Experts Say,” CNN, September 27, 2007, accessed March 1, 2016, www.cnn.com.

53. "Mouse Click Could Plunge City into Darkness, Experts Say," CNN, September 27, 2007, accessed March 1, 2016, www.cnn.com.

54. "Interview with Manimaran Govindarasu" IEEE Smartgrid, July 2012, accessed February 24, 2016, www.smartgrid.ieeee.org.

55. Parfomak, Paul W., "Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations," Congressional Research Service, June 17, 2014, accessed May 4, 2016.

56. Smith, Rebecca, "Transformers Expose Limits in Securing Power Grid," Wall Street Journal, 4 March 2014, accessed May 4, 2016, www.wsj.com.

57. Hurley Jr., Daniel C., James F.X. Payne, Mary T. Anderson, "Risk Mitigation in the Electric Power Sector: Serious Attention Needed," Armed Forces Communication and Electronics Association 2012, accessed February 25, 2016.

58. Tong, Scott, "Utility Companies to Stockpile $8 Million Spare Parts in Case of Disaster" Marketplace, April 8, 2016, accessed May 4, 2016, www.marketplace.org.

59. Gonzalez, Rick, "Spare Transformers: Why, How Many, and How to Compute it All?," Excel Engineering, May 2, 2012, accessed May 4, 2016, www.exceleng.net.

60. Lee, Robert M., "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS ICS Security Blog, January 8, 2016, accessed March 2, 2016, www.ics.sans.org/blog.

61. Lee, Robert M., "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS ICS Security Blog, January 8, 2016, accessed March 2, 2016, www.ics.sans.org/blog.

62. Sridhar, Siddharth, Adam Hahn, Manimaran Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," IEEE 100 (2012): 215, accessed February 25, 2016.

63. Sridhar, Siddharth, Adam Hahn, Manimaran Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," IEEE 100 (2012): 215, accessed February 25, 2016.

64. Lee, Robert M., "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS ICS Security Blog, January 8, 2016, accessed March 2, 2016, www.ics.sans.org/blog.

65. "Frequently Asked Questions," North American Electric Reliability Corporation, August 2013, accessed December 16, 2015, http://www.nerc.com/AboutNERC/Documents/NERC%20FAQs%20AUG13.pdf.

66. "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat," Bipartisan Policy Center, February 2014, accessed March 3, 2016.

67. Zetter, Kim, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed February 15, 2016, www.wired.com.

68. Lee, Robert M., Michael J. Assante, Tim Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," SANS Institute & the Electricity Information Sharing and Analysis Center, March 18, 2016, accessed May 11, 2016.

69. Assante, Michael J., "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," SANS ICS Security Blog, January 9, 2016, accessed February 23, 2016, www.ics.sans.org/blog.

70. Zetter, Kim, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed February 15, 2016, www.wired.com.

71. Zetter, Kim, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, accessed February 15, 2016, www.wired.com.

72. Lee, Robert M., "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS ICS Security Blog, January 8, 2016, accessed March 2, 2016, www.ics.sans.org/blog.

73. Lee, Robert M., "ICS Cross-Industry Learning: Cyber-Attacks on Electric Transmission and Distribution (Part One)," SANS ICS Security Blog, January 8, 2016, accessed March 2, 2016, www.ics.sans.org/blog.

74. Campbell, Richard J., "Cybersecurity Issues for the Bulk Power System," Congressional Research Service, June 10, 2015, accessed February 15, 2016.

75. "Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015," PWC, September 30, 2014, accessed September 30, 2015.

76. Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, Adam Hahn, "NIST 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, May 2015, accessed May 1, 2016.

77. "Critical Infrastructure: Security Preparedness and Maturity," Ponemon Institute: Unisys, July 2014, accessed September 30, 2015.

78. "Vulnerability Analysis of Energy Delivery Control Systems," Idaho National Laboratory, September 2011, accessed February 16, 2016.

79. Robinson, Michael, "The SCADA Threat Landscape," BCS, September 2013, accessed February 22, 2016.

80. "SCADA over IP-based LAN-WAN Connections," ABB, 2011, https://library.e.abb.com/public/09e2909e92d2ce8ac1257863004e7da0/SCADA%20application%20flyer_small.pdf.

81. Weiss, Joseph, Protecting Industrial Control Systems from Electronic Threats (New York, N.Y: Momentum Press, 2010), 36-37.

82. "Access to the Control System LAN," ICS-CERT, accessed November 9, 2015, https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities.

83. Mimoso, Michael, "Electric Utility Cybersecurity Regulations Have a Problem," Threat Post, January 24, 2014, accessed November 9, 2015, www.threatpost.com.

84. Mimoso, Michael, "Electric Utility Cybersecurity Regulations Have a Problem," Threat Post, January 24, 2014, accessed November 9, 2015, www.threatpost.com.

85. Campbell, Richard J., "Cybersecurity Issues for the Bulk Power System," Congressional Research Service, June 10, 2015, accessed February 15, 2016.

86. "IEEE Smart Grid Cybersecurity Round Up," IEEE Smart Grid, accessed November 9, 2015, http://smartgrid.ieee.org/resources/interviews/363-ieee-smart-grid-cyber-security-round-up?highlight=WyJjeWJlciIsInNlY3VyaXR5IiwiY3liZXIgc2VjdXJpdHkiXQ==.

87. "ICS-CERT Advisories" ICS-CERT, accessed November 5, 2015, https://ics-cert.us-cert.gov/advisories.

88. "Energy at Risk: A Study of IT Security in the Energy and Natural Resources Industry," KPMG Global Energy, 2013, accessed October 1, 2015.

89. O'Harrow Jr., Robert, "Cyber search engine Shodan exposes industrial control systems to new risks," Washington Post, June 3, 2012, accessed November 10, 2015, www.washingtonpost.com.

90. Storm, Darlene, "Hackers exploit SCADA holes to take full control of critical infrastructure," Computerworld, January 15, 2014, accessed November 11, 2015, www.computerworld.com.

91. "IEEE Smart Grid Cybersecurity Round Up," IEEE Smart Grid, accessed November 9, 2015, http://smartgrid.ieee.org/resources/interviews/363-ieee-smart-grid-cyber-security-round-up?highlight=WyJjeWJlciIsInNlY3VyaXR5IiwiY3liZXIgc2VjdXJpdHkiXQ==.

92. Rosenbush, Stephen, and Rachael King, "Utilities Race to Protect Electric Grid Before 'Disaster Strikes'," Deloitte CIO Journal, February 19, 2013, accessed October 22, 2015, www.wsj.com.

93. "Creating Trust in the Digital World: EY's Global Information Security Survey 2015," EY, October 2015, accessed May 5, 2016.

94. "ICS-CERT Monitor January 2014—April 2014," ICS-CERT, May 16, 2015, accessed November 9, 2015.

95. “ICS-CERT Monitor January 2014—April 2014,” ICS-CERT, May 16, 2015, accessed November 9, 2015.

96. Contos, Brian, "Five More Reasons ICS Security is Fragile,” Darkmatters, March 22, 2015, accessed February 26, 2016, www.darkmatters.norsecorp.com.

97. “Shodan,” accessed May 4, 2016, https://www.shodan.io/.

98. "Interview with Manimaran Govindarasu," IEEE Smartgrid, July 2012, accessed February 24, 2016, www.smartgrid.ieeee.org.

99. Pasquali, Dana, "Validation among Insecurities,” Control Engineering, April 22, 2015, accessed May 4, 2016, www.controleng.com.

100. Khandelwal, Swati, "18-year-old Unpatched Vulnerability Affects All Versions of Microsoft Windows,” The Hacker News, April 13, 2015, accessed February 26, 2016, www.thehackernews.com.

101. Harp, Derek, Bengt Gregory-Brown, “The State of Security in Control Systems Today,” SANS Institute, June 2015, accessed February 22, 2016.

102. "Experts: Despite Warnings, Slow Progress Securing Industrial Systems" The Security Ledger, January 16, 2014, accessed February 26, 2016, www.securityledger.com.

103. Kovacs, Eduard, "Attackers Using Havex RAT Against Industrial Control Systems,” Securityweek, June 24, 2014, accessed November 10, 2015, www.securityweek.com.

104. Staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA), “Electric Grid Vulnerability: Industry Responses Reveal Security Gaps,” U.S. House of Representatives, May 21, 2013, accessed October 9, 2015.

105. “Critical Infrastructure: Security Preparedness and Maturity,” Ponemon Institute: Unisys, July 2014, accessed September 30, 2015.

106. Stollery, Mark “Cyber Security-the Best Weapon Remains Good Information Security Hygiene,” Computer Weekly, March 2013, accessed May 20, 2016, www.computerweekly.com.

107. “Energy Companies and Financial Services Firms Remain Vulnerable to Data-Breaching Malware,” ThreatTrack Security, April 2014, accessed November 9, 2015.

108. “Energy at Risk: A Study of IT Security in the Energy and Natural Resources Industry,” KPMG Global Energy, 2013, accessed October 1, 2015.

109. Staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA), “Electric

Grid Vulnerability: Industry Responses Reveal Security Gaps," U.S. House of Representatives, May 21, 2013, accessed October 9, 2015.

110. Lacy, Eric, "BWL in Limbo from Cyberattack," Lansing State Journal, April 27, 2016, accessed May 9, 2016, www.lansingstatejournal.com.

111. Lacy, Eric, "BWL in Limbo from Cyberattack," Lansing State Journal, April 27, 2016, accessed May 9, 2016, www.lansingstatejournal.com.

112. Bonderud, Douglas, "New Malware Attacks Hunt for Cracks in Energy Sector Defenses," Security Intelligence, April 3, 2015, accessed October 8, 2015, www.securityintelligence.com.

113. Santillan, Maritza "Global Energy Sector Targeted in Reconnaissance Malware Attacks," Tripwire, March 31, 2015, www.tripwire.com, accessed November 11, 2015.

114. Storm, Darlene, "Hackers exploit SCADA holes to take full control of critical infrastructure," Computerworld, January 15, 2014, www.computerworld.com, accessed November 11, 2015.

115. Storm, Darlene, "Hackers exploit SCADA holes to take full control of critical infrastructure," Computerworld, January 15, 2014, www.computerworld.com, accessed November 11, 2015.

116. Mateski, Mark, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, and Jason Frye, "Cyber Threat Metrics," Sandia National Laboratories, September 2011, accessed February 16, 2016.

117. Assante, Michael J., Robert M. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed February 24, 2016.

118. "Cyber Kill Chain," Lockheed Martin, accessed May 4, 2016, http://cyber.lockheedmartin.com/solutions/cyber-kill-chain.

119. Higgins, Kelly J., "Researchers Out Default Passwords Packaged With ICS/SCADA Wares," DarkReading, January 4, 2016, accessed February 25, 2016, www.darkreading.com.

120. "Industrial Control Systems," Shodan, accessed May 4, 2016 https://www.shodan.io/explore/category/industrial-control-systems.

121. "ICS-CERT Year in Review 2014" ICS-CERT, May 16, 2015, accessed February 12, 2016.

122. "Critical Infrastructure: Security Preparedness and Maturity," Ponemon Institute: Unisys, July 2014, accessed September 30, 2015.

123. Assante, Michael J., Robert M. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed February 24, 2016.

124. Harp, Derek, Bengt Gregory-Brown, “The State of Security in Control Systems Today,” SANS Institute, June 2015, accessed February 22, 2016.

125. “Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015,” PWC, September 30, 2014, accessed September 30, 2015.

125. Contos, Brian, "Five More Reasons ICS Security is Fragile,” Darkmatters, March 22, 2015, accessed February 26, 2016, www.darkmatters.norsecorp.com.

126. “ICS-CERT Monitor November—December 2015,” ICS-CERT, May 16, 2015, accessed February 12, 2016.

127. “Industrial Control System (ICS) Security,” Corero Network Security, 2014, accessed February 22, 2016.

128. Staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA), “Electric Grid Vulnerability: Industry Responses Reveal Security Gaps,” U.S. House of Representatives, May 21, 2013, accessed October 9, 2015.

129. Lee, Robert M., Michael J. Assante, Tim Conway, “SANS ICS Defense Use Case 3.v1.1” SANS Institute, April 23, 2015, accessed May 6, 2016.

130. Assante, Mike, “The Six Most Dangerous New Attack Techniques and What's Coming Next,” RSA Conference, May 7, 2015, RSAConference.com.

131. “Worldwide Cyber Threats,” Office of the Director of National Intelligence, House Permanent Select Committee on Intelligence, September 10, 2015.

132. McLarty III, Thomas F., Thomas J. Ridge; Project Chairs, “Securing the U.S. Electrical Grid,” Center for the Study of The Presidency & Congress, October 2014, accessed February 16, 2016.

133. McLarty III, Thomas F., Thomas J. Ridge; Project Chairs, “Securing the U.S. Electrical Grid,” Center for the Study of The Presidency & Congress, October 2014, accessed February 16, 2016.

134. “US should be More Worried about Russia’s Cyber Capabilities,” ValueWalk, October 2, 2015, accessed May 20, 2016, www.valuewalk.com.

135. Davis, Joshua, “Hackers Take Down the Most Wired Country in Europe,” Wired, August 21, 2007, accessed May 4, 2016, www.wired.com.

136. Gorman, Siobhan, “Electricity Grid in U.S. Penetrated by Spies,” Wall Street Journal, April 8, 2009, accessed 22 February 2015, www.wsj.com.

137. “Hackers Caused Power Cut in Western Ukraine,” BBC, January 12, 2016, accessed March 9, 2016, www.bbc.com.

138. “2015 Global Threat Report,” Crowdstrike Intelligence Threat Team, June 10, 2015, accessed February 18, 2016, www.crowdstrike.com.

139. Cyber Behavior: Concepts, Methodologies, Tools, and Applications (Hershey, P.A.: IGI Global, 2014), 795, Information Resources Management Association, ed.

140. Riley, Michael, and Jordan Robertson, “UglyGorilla Hack of U.S. Utility Exposes Cyberwar Threat,” Bloomberg Business, June 13, 2014, accessed March 8, 2016, www.bloomberg.com.

141. Riley, Michael, and Jordan Robertson, “UglyGorilla Hack of U.S. Utility Exposes Cyberwar Threat,” Bloomberg Business, June 13, 2014, accessed March 8, 2016, www.bloomberg.com.

142. “United States of America v. Fathi et. Al,” U.S. District Court Southern District of New York, 2016, accessed March 28, 2016, https://www.justice.gov/opa/file/834996/download.

143. McLarty III, Thomas F., Thomas J. Ridge; Project Chairs, “Securing the U.S. Electrical Grid,” Center for the Study of The Presidency & Congress, October 2014, accessed February 16, 2016.

144. “Solutions 2016: Cybersecurity,” Heritage Foundation, 2016, accessed March 8, 2016, www.solutions.heritage.org.

145. “2015 Global Threat Report,” Crowdstrike Intelligence Threat Team, June 10, 2015, accessed February 18, 2016, www.crowdstrike.com.

146. Beach-Westmoreland, Nathaniel, “If North Korea Did Hack Sony, It’s a Whole New Kind of Cyberterrorism,” Wired, December 23, 2014, accessed March 8, 2016, www.wired.com.

147. “2015 Global Threat Report,” Crowdstrike Intelligence Threat Team, June 10, 2015, accessed February 18, 2016, www.crowdstrike.com.

148. Pagliery, Jose, “ISIS is Attacking the U.S. Energy Grid (and Failing),” CNN Money, October 16, 2015, accessed May 20, 2016, www.money.cnn.com.

149. McLarty III, Thomas F., Thomas J. Ridge; Project Chairs, “Securing the U.S. Electrical Grid,” Center for the Study of The Presidency & Congress, October 2014, accessed February 16, 2016.

150. "Frequently Asked Questions,” North American Electric Reliability Corporation, August 2013, accessed December 16, 2015, http://www.nerc.com/AboutNERC/Documents/NERC%20FAQs%20AUG13.pdf.

151. “CIP Standards,” NERC Reliability Standards, accessed December 17, 2015, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

152. “Framework for Improving Critical Infrastructure Cybersecurity Version 1.0,” National Institute of Standards and Technology, February 12, 2014, accessed December 17, 2015.

153. “Resolution Regarding Cybersecurity,” National Association of Regulatory Commissioners, February 17, 2010, accessed December 17, 2015.

154. “Resolution Regarding Cybersecurity Awareness and Initiatives,” National Association of Regulatory Commissioners, July 24, 2013, accessed December 17, 2015.

155. “Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat,” Bipartisan Policy Center, February 2014, accessed September 23, 2016.

156. “Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat,” Bipartisan Policy Center, February 2014, accessed September 23, 2016.

157. "Invensys Critical Infrastructure & Security NERC CIP Compliance Checklist," Schneider Electric, April 2015, http://software.schneider-electric.com/pdf/service-profile/critical-infrastructure-and-security-nerc-cip-compliance-checklist/.

158. “CIP Standards,” NERC Reliability Standards, accessed December 17, 2015, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

159. “Consequence-driven Cyber-informed Engineering Process,” Idaho National Laboratory, 2015 (unpublished), accessed May 4, 2016.

160. "Here's What Chinese Hackers Can Actually Do to the US Power Grid," Business Insider, November 23, 2014, accessed February 26, 2016, www.businessinsider.com.

161. Thomas F. McLarty III, Thomas J. Ridge; Project Chairs, “Securing the U.S. Electrical Grid,” Center for the Study of The Presidency & Congress, October 2014, accessed February 16, 2016.

162. Hurley Jr., Daniel C., James F.X. Payne, and Mary T. Anderson, “Risk Mitigation in the Electric Power Sector: Serious Attention Needed,” Armed Forces Communication and Electronics Association, 2012, accessed February 25, 2016.

163. “Mitigating Cyber-Security Risk of Smart-Grid AMI,” Oracle, 2012, accessed September 25, 2015.

164. “Southern California Edison Smart Grid Strategy & Roadmap,” Southern California Edison 2010, accessed September 30, 2015.

165. “Physical Security,” Techtarget, accessed February 15, 2016, http://searchsecurity.techtarget.com/definition/physical-security.

166. “Comments of the Electric Trade Association in Response to NIST’s Request for Information on ‘Developing a Framework to Improve Critical Infrastructure Cyber security,’” Sacramento Municipal Utility District, April 8, 2013.

167. “Best Practices for Cyber Security in the Electric Power Sector” IBM, 2012, accessed September 24, 2015.

168. “Electricity Sub-Sector Coordinating Council Charter,” Electricity Sub-Sector Coordinating Council, 2013, accessed July 21, 2016.

169. “Protecting Our Critical Utilities with Integrated Control Systems,” Motorola, 2012, accessed September 29, 2015.

170. Gauci, Adam, Didier Giarratano, and Sandeep Pathania, “A Framework for Developing and Evaluating Utility Substation Cyber Security,” Schneider Electric, 2014, accessed October 26, 2015.

171. “Siemens: Cyber Security,” Siemens AG, 2015, accessed October 26, 2015.

172. Rosenbush, Stephen, Rachael King, "Utilities Race to Protect Electric Grid Before ‘Disaster Strikes’,” Deloitte CIO Journal, February 19, 2013, accessed October 22, 2015, www.wsj.com.

173. “Belden, Schneider Electric Pair on Cybersecurity Firewall,” Electric Light & Power, January 28, 2014.

174. Byres, Eric, “SCADA Security & Deep Packet Inspection,” March 29, 2012, accessed October 26, 2015, www.tofinosecurity.com.

175. Cornell, Scott, “Cyber Security for the Electric Grid,” Faronics Blog, September 26, 2012, accessed October 26, 2015, www.faronics.com.

176. “S&C Enhances Security of Smart Grid Controls with McAfee Solutions,” S&C Electric Company News Center, May 9, 2012, accessed October 26, 2015, www.sandc.com.

177. Ozturk, Metin, and Philip Aubin, “SCADA Security: Challenges and Solutions,” June 2011, accessed October 26, 2015.

178. “Understanding the Facts: Edison Electric Institute’s Positions on Radio Frequency, Cyber Security and Data Privacy,” Pepco, accessed October 26, 2015, www.pepcoholdings.com.

179. Hurd, Steven, Rhett Smith, and Garrett Leischner, “Tutorial: Security in Electric Utility Control Systems,” IEEE, 2008, accessed October 26, 2015.

180. “Encryption of Substation Communication Protocols on the Rise in North American Electric Utilities,” Newton-Evans Research Company, Inc., February 26, 2014.

181. “Mitigating Cyber-Security Risk of Smart-Grid AMI,” Oracle, 2012, accessed September 25, 2015.

182. “Grid and Cyber Security Strategy,” San Diego Gas & Electric Company, 2015, accessed September 30, 2015.

183. “Written Procedures and Compliance Plan: FERC Standards of Conduct for Transmission Providers,” San Diego Gas & Electric Company, February 11, 2014, accessed December 15, 2015.

184. “Securing Your Energy," San Diego Gas & Electric Company, accessed 15 December 2015, http://www.sdge.com/smartgrid/securing-your-energy.

185. “Southern California Edison Smart Grid Strategy & Roadmap,” Southern California Edison 2010, accessed September 30, 2015.

186. Hawk, Carol, and Akhlesh Kaushiva, “Cyber security and the Smarter Grid,” The Electricity Journal (2014): 89-90.

187. Hawk, Carol, and Akhlesh Kaushiva, “Cyber security and the Smarter Grid,” The Electricity Journal (2014): 89-90.

188. “Booz Allen, Siemens and Power Analytics Partner with New York Communities to Win 16 NY Prize Microgrid Projects,” Booz Allen Hamilton, McLean, VA, July 9, 2015.

189. “Critical Infrastructure: Security Preparedness and Maturity,” Ponemon Institute: Unisys, July 2014, accessed September 30, 2015.

190. Clamp, Alice, “Cyber and Physical Security: Evolving Threats and Defense Mechanisms,” American Public Power Association, August 30, 2014, accessed December 16, 2015, www.publicpower.org.

191. Wieck, Angie, “Cyber-security Professionals Say Employees are Biggest Threat to Network Security,” Dickinson Press, September 27, 2015, accessed December 16, 2015, www.thedickinsonpress.com.

192. “Comments of the Electric Trade Association in Response to NIST’s Request for Information on ‘Developing a Framework to Improve Critical Infrastructure Cyber security,’” Sacramento Municipal Utility District, April 8, 2013.

193. Henderson, Cam, and Behzad Hosseini, “UE 262 Information Technology: Direct Testimony and Exhibits of Cam Henderson, Behzad Hosseini,” Portland General Electric Company, February 15, 2013, accessed October 8, 2015.

194. Rivaldo, Alan, "Report on Electric Grid Cybersecruity in Texas," Public Utility Commission of Texas, November 2012, accessed September 29, 2015.

195. "FERC Directs Development of Standards for Supply Chain Cyber Controls," Federal Energy Regulatory Commission (FERC), July 21, 2016.

196. "Frequently Asked Questions about Cyber security and the Electric Power Industry," Edison Electric Institute, October 2014, accessed September 24, 2015.

197. "Pacific Gas and Electric Company (PG&E) Grid Security Exercise Support," Booz Allen Hamilton, Tysons Corner, Virginia, 2015.

198. Hewes, Amy, "PG&E Provides Support for the Cal Poly Cyber security Center," Cal Poly University News, December 13, 2013.

199. "Hawaii Creates Cyber security Post to Tighten Ties with Federal Government," State of Hawaii: Office of Information Management & Technology, February 12, 2014.

200. Assante, Michael J., Robert M. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015, accessed December 22, 2015.

201. "Best Practices for Cyber Security in the Electric Power Sector" IBM, 2012, accessed September 24, 2015.

202. "Comments of the Salt River Project Request for Information on 'Developing a Framework to Improve Critical Infrastructure Cyber security'," Salt River Project, April 8, 2013.

203. "2012 Utility Cyber Security Survey," ViaSat, January 2013, accessed September 25, 2015.

204. Nicol, Fraser, "Securing Utilities against Cyber Attack," EY, 2013, accessed September 25, 2015.

205. "Xcel Energy Response to NIST RFI," Xcel Energy, 2013.

206. "Appropriately Limiting Public Power Liability for Cyber Incidents," American Public Power Association, February 2015, accessed November 12, 2015.

207. "Incentives to Adopt Improved Cybersecurity Practices," Department of Water and Power of the City of Los Angeles, Los Angeles, CA, April 29, 2013.

208. "Frequently Asked Questions about Cyber security and the Electric Power Industry," Edison Electric Institute, October 2014, accessed September 24, 2015.

209. "Appropriately Limiting Public Power Liability for Cyber Incidents," American Public Power Association, February 2015, accessed November 12, 2015.

210. “Appropriately Limiting Public Power Liability for Cyber Incidents,” American Public Power Association, February 2015, accessed November 12, 2015.

211. “Protected Critical Infrastructure Information (PCII) Program," Department of Homeland Security, accessed December 22, 2015, http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program.

212. “Protected Critical Infrastructure Information (PCII) Program," Department of Homeland Security, accessed December 22, 2015, http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program.

213. “Comments of the Electric Trade Association in Response to NIST’s Request for Information on ‘Developing a Framework to Improve Critical Infrastructure Cyber security,’” Sacramento Municipal Utility District, April 8, 2013.

214. “Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat,” Bipartisan Policy Center, February 2014, accessed September 23, 2015.

215. “ICS-CERT Monitor January 2014—April 2014,” ICS-CERT, May 16, 2015, accessed November 9, 2015.

216. “Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015,” The Office of the Director of National Intelligence, The Department of Homeland Security, The Department of Defense, The Department of Justice, accessed May 20, 2016.

217. “S.754 - Cybersecurity Information Sharing Act of 2015,” United States Congress, accessed March 15, 2016, https://www.congress.gov/bill/114th-congress/senate-bill/754.

218. “Frequently Asked Questions about Cyber security and the Electric Power Industry,” Edison Electric Institute, October 2014, accessed September 24, 2015.

219. “The Electric Power Sector Supports S. 754, the Cybersecurity Information Sharing Act (CISA) and Opposes Weakening Amendments,” National Rural Electric Cooperative Association, October 13, 2015, accessed March 17, 2016.

220. DeJesus, Joel, “New Grid Security Measures for 2016,” Public Utilities Fortnightly, February 2016, accessed March 17, 2016.

221. “Incentives to Adopt Improved Cybersecurity Practices,” Department of Water and Power of the City of Los Angeles, Los Angeles, CA, April 29, 2013.

222. Parks, Jim, “Smart Grid Implementation at the Sacramento Municipal Utility District” (presented at the CPUC Smart Grid Workshop, San Francisco, CA, March 18, 2010).

223. “Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat,” Bipartisan Policy Center, February 2014, accessed September 23, 2015.

224. “Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid,” Lloyd’s, accessed September 24, 2015.

225. Mimoso, Michael, "Electric Utility Cybersecurity Regulations Have a Problem,” Threat Post, January 24, 2014, accessed November 9, 2015, www.threatpost.com.

226. “Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat,” Bipartisan Policy Center, February 2014, accessed September 23, 2015.

227. Bucci, Steven P., Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation, April 21, 2013, accessed November 12, 2015, www.heritage.org.

228. Bucci, Steven P., Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation, April 21, 2013, accessed November 12, 2015, www.heritage.org.

229. Horwitz, Sari, "Justice Department trains prosecutors to combat cyber-espionage,” Washington Post, July 25, 2012, accessed November 12, 2015, www.washingtonpost.com.

230. “Critical Infrastructure: Security Preparedness and Maturity,” Ponemon Institute: Unisys, July 2014, accessed September 30, 2015.

231. “ICS-CERT Monitor September 2014—February 2015,” ICS-CERT, March 11, 2015, accessed November 9, 2015.

232. "Common Vulnerabilities and Exposures,” accessed May 6, 2016, https://www.cve.mitre.org/cve/index.html.

233. "ICS-CERT Advisories,” ICS-CERT, accessed May 6, 2016, https://ics-cert.us-cert.gov/advisories.

234. “Booz Allen, Siemens and Power Analytics Partner with New York Communities to Win 16 NY Prize Microgrid Projects,” Booz Allen Hamilton, McLean, VA, July 9, 2015.

235. “Pacific Gas and Electric Company (PG&E) Grid Security Exercise Support,” Booz Allen Hamilton, Tysons Corner, Virginia, 2015.

236. Hawk, Carol, and Akhlesh Kaushiva, “Cyber Security and the Smarter Grid,” The Electricity Journal (2014): 89-90.

237. “Energy Companies and Financial Services Firms Remain Vulnerable to Data-Breaching Malware,” ThreatTrack Security, April 2014, accessed November 9, 2015.

238. Staff of Congressmen Edward J. Markey (D-MA) and Henry Waxman (D-CA), “Electric Grid Vulnerability: Industry Responses Reveal Security Gaps,” U.S. House of Representatives, May 21, 2013, accessed October 9, 2015.

239. Contos, Brian, "Five More Reasons ICS Security is Fragile,” Darkmatters, March 22, 2015, accessed February 26, 2016, www.darkmatters.norsecorp.com.

240. Glenn/Wright, “US Electric Utilities Cyber Security Threat Analysis,” Idaho National Laboratory, March 2016, accessed March 20, 2016.

241. “Energy Sector-Specific Plan 2015,” Department of Homeland Security, accessed February 15, 2016.