NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBER SECURITY FOR CRITICAL ENERGY INFRASTRUCTURE

by

Jason F. Clemente

September 2018

Thesis Advisor:	Scott E. Jasper
Second Reader:	Erik J. Dahl

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE CYBER SECURITY FOR CRITICAL ENERGY INFRASTRUCTURE			**5. FUNDING NUMBERS**
6. AUTHOR(S) Jason F. Clemente			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The United States power grid is a logical target for a major cyber attack because it connects all of the nation's critical infrastructures with electricity. Attackers consistently exploit vulnerabilities of the bulk power system and are close to being able to disrupt electrical distribution. We live in a world that is interconnected, from personal online banking to government infrastructure; consequently, network security and defense are needed to safeguard the digital information and controls for these systems. The cyber attack topic has developed into a national interest because high-profile network breaches have introduced fear that computer network hacks and other security-related attacks have the potential to jeopardize the integrity of the nation's critical infrastructure. The national and economic security of the United States depends on a reliable, functioning critical infrastructure. A comprehensive understanding of the effects of a massive power failure may help promote changes in the way cyber security is run on our most important critical infrastructure: the national power grid. This study investigates the robustness of the power grid's network system, the collaboration between public and private sectors against cyber threats, and mitigation requirements in areas of weakened controls such as program planning and management, access controls, application software development, and system software and service continuity controls.

14. SUBJECT TERMS cyber security, cyber attack, critical infrastructure, power grid, homeland security, NIPP, NICC			**15. NUMBER OF PAGES** 91
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

CYBER SECURITY FOR CRITICAL ENERGY INFRASTRUCTURE

Jason F. Clemente
Lieutenant, United States Navy
BS, San Diego State University, 2012

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2018

Approved by: Scott E. Jasper
Advisor

Erik J. Dahl
Second Reader

Mohammed M. Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States power grid is a logical target for a major cyber attack because it connects all of the nation’s critical infrastructures with electricity. Attackers consistently exploit vulnerabilities of the bulk power system and are close to being able to disrupt electrical distribution. We live in a world that is interconnected, from personal online banking to government infrastructure; consequently, network security and defense are needed to safeguard the digital information and controls for these systems. The cyber attack topic has developed into a national interest because high-profile network breaches have introduced fear that computer network hacks and other security-related attacks have the potential to jeopardize the integrity of the nation’s critical infrastructure. The national and economic security of the United States depends on a reliable, functioning critical infrastructure. A comprehensive understanding of the effects of a massive power failure may help promote changes in the way cyber security is run on our most important critical infrastructure: the national power grid. This study investigates the robustness of the power grid’s network system, the collaboration between public and private sectors against cyber threats, and mitigation requirements in areas of weakened controls such as program planning and management, access controls, application software development, and system software and service continuity controls.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

CIP	critical infrastructure protection
CISCP	Cyber Information Sharing and Collaboration Program
CRISP	Cybersecurity Risk Information Sharing Program
DHS	Department of Homeland Security
DOS	denial-of-service
EMS	emergency management system
ESP	electronic security perimeter
FERC	Federal Energy Regulatory Commission
HIPPA	Health Insurance Portability and Accountability Act
HMI	human machine interface
ICS	industrial control system
ICS-CERT	Industrial Control System-Computer Emergency Response Team
ICT	information and communication technology
IOT	internet of things
ISAO	information sharing and analysis organization
ISM	industrial, scientific, and medical
IT	information technology
MIS	management information system
MITM	man-in-the-middle
NERC	North American Electric Reliability Corporation
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
NSTAC	National Security Telecommunications Advisory Committee
OE	Office of Electricity
OEM	original equipment manufacturer
PII	personal identifiable information
PKI	public key infrastructure
PLC	programmable logic controller
PPD-21	Presidential Policy Directive-21

PPP	public private partnership
RF	radio frequency
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SMB	server message block
SME	subject matter expert
UPS	uninterruptable power supply
VBA	Visual Basic for Applications
VPN	virtual private network
WSN	wireless sensor network

ACKNOWLEDGMENTS

Foremost, I would like to express great appreciation to my advisor, Professor Scott Jasper, for his full support of my graduate study and thesis research. His encouragement, patience, and expertise kept me driving forward through the entire thesis development processes. He sets the educational standard high for all educators and scholars. I am thankful he was my thesis advisor. I am also humbled and grateful for Professor Eric Dahl's expert and professional guidance in developing this thesis. Additionally, special thanks to my academic associate, Professor Carolyn Halladay, the entire Naval Postgraduate School (NPS) Graduate Writing Center staff, and Aileen Houston with the NPS Thesis Processing Office.

Furthermore, nobody is more important to me in completing this thesis than my entire family. I cannot express how grateful I am to my parents-in-law, Scot and Margaret Bradley, for their unrelenting encouragement. I am also thankful for the constant support I received from my brothers-in-law, Keegan Bradley and Collin Bradley. I cannot forget to thank all my close friends who have gone through this journey with me.

I am extremely grateful to my parents, Godofredo and Guadalupe Clemente, and my brother, Alexander Clemente, for their love, prayers, and care to educate and prepare me for the road ahead throughout my life. My father and mother have sacrificed a lot for me and were always by my side whenever I needed it. I attribute much of my success to them. Thanks for being the best parents a child could ever ask for.

Finally, with all my love I would like to thank my wife, Breana Clemente. She has been my life support throughout my entire Naval career. Without her as the cornerstone in my life, I may not have made it through my graduate education. I am especially grateful for her support, love, and encouragement through this demanding part of my life. I cannot imagine a better wife and best friend than her.

THIS PAGE INTENTIONALLY LEFT BLANK

I. ENHANCING ELECTRICAL GRID CYBER SECURITY

The United States' power grid is a logical target for a major cyber-attack because it connects all the nation's critical infrastructures with electricity. Attackers consistently exploit vulnerabilities of the bulk power system and are close to being able to disrupt electrical distribution system. How can the United States better protect its cyber networks to prevent an attack on the electrical grid by aggressive and dangerous hackers?

A. SIGNIFICANCE OF THE RESEARCH

We live in a world that is interconnected, from personal online banking to government infrastructure, which consequently requires network security and defense to safeguard the digital information and controls for these systems. The cyber-attack topic has developed into a national interest because high-profile network breaches have created fear that computer network hacks and other security related attacks have the potential to jeopardize the integrity of the nation's critical infrastructure. The United States requires a functional and resolute critical infrastructure to cultivate its economic and political strength.[1]

The most important asset within the nation's 16 critical infrastructure lineup is the national power grid. The Department of Homeland Security (DHS) refers to the energy sector as the "backbone of our nation's economy, security, and health."[2] Without electrical power, just about everything from emergency services equipment to residential lighting, in our information-age reliant society will not work.[3] Parts of the U.S. electrical network are aging past a century, comprised of power plants averaging 30 years old. The massive and outdated electrical grid is a sprawling machine constructed of millions of equipment pieces,

[1] "Reducing Cyber Risk to Critical Infrastructure: NIST Framework Department of Energy," Department of Energy, accessed August 25, 2018, https://www.energy.gov/oe/cybersecurity-critical-energy-infrastructure/reducing-cyber-risk-critical-infrastructure-nist.

[2] "What Is Critical Infrastructure?" Department of Homeland Security, accessed December 7, 2017, https://www.dhs.gov/what-critical-infrastructure.

[3] Sans Institute, "Can Hackers Turn Your Lights Off? The Vulnerability of the U.S. Power Grid to Electronic Attack," (Institute InfoSec Reading Room, SANS Institute, 2001), https://www.sans.org/reading-room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack-606.

many that require replacement or overhaul.[4] Obsolete equipment that are now interconnected to complex automated systems have the potential to leave an entire electrical grid vulnerable to hackers. If hackers were to remotely shut off decrepit but critical electrical transformers at three strategically located substations in the Northeastern part of the United States during a winter when energy demand peaks, power would likely have to be routed from nearby states.[5] The intentional act of shutting off important electrical transmission and distribution equipment can cause a domino effect by creating cascading power outages across multiples cities or states.

Rogue actors attempt to gain information on U.S. stealth aircraft, GPS satellites, and military operations. It would be irresponsible to assume they are not showing the same interest in the United States' critical energy infrastructure. People in developed countries tend to take the value of electricity for granted because it is something that is expected to work. "Despite its great importance in our daily lives, most of us rarely stop to think what life would be without electricity," and the interdependencies it has on other critical infrastructures, like powering the pumps in the potable water system or powering the heavy machinery that extracts natural gas from the Earth's surface.[6] Although the potential repercussions of an attack on the electrical grid are severe, most people do not consider this issue pressing because there is no precedent of an irreparable failure. However, the emergence of innovative and rapidly evolving threats as the nation moves to complex automated networked systems is enough reason to be wary.

To provide a glimpse of what a mass electrical outage can cause, in September 2011 approximately five million electrical customers throughout the Southwest United States and parts of Northern Mexico on a hot summer weekday had their daily routine interrupted at precisely 3:38 pm PST. Trains stopped, freeways and roads were gridlocked without any

[4] Katie Bo Williams and Cory Bennett, "Why a Power Grid Attack Is a Nightmare Scenario," *The Hill*, last modified June 30, 2016, http://thehill.com/policy/cybersecurity/281494-why-a-power-grid-attack-is-a-nightmare-scenario.

[5] Harold Shapiro, *America's Energy Future* (Washington, DC: National Academy of Sciences, 2009), 256, https://www.nap.edu/read/12091/chapter/1#ii.

[6] Mary Bellis, "What Is Electricity?" ThoughtCo, last modified February 28, 2018, https://www.thoughtco.com/what-is-electricity-4019643.

working traffic signals, courts and universities shut down for the day, water supplies became contaminated, and emergency services and hospitals ran on limited generator power. Though the cause was not a deliberate act, the widespread blackout continued until the next morning, leaving multiple geographic regions in complete darkness throughout the evening. Power to the San Diego metropolitan area was out for close to a day; although the major result was inconvenience, a deliberate lengthy and widespread outage could have many more severe and even deadly consequences.

The power grid has been physically susceptible for decades. We have just recently begun to recognize and comprehend the gravity of an evolving hazard to the power grid's cyber security framework. As the power grid becomes more reliant on data sharing and computers, it can respond to the fluctuations in power demands and link a variety of energy sources together. However, there is a high potential that the automated functions used in these grids could be manipulated by hackers who manage to break into the electrical grid computer systems.[7] The United States cannot have a normally functioning society without a resilient cyber security program protecting our nation's power grid. Without linking the grid to an operable and safe network, it will continue to be vulnerable to disruptions.

B. LITERATURE REVIEW

Much of the modern world has transferred from an analog to a digital mode of operating critical infrastructure.[8] The shift in technology has brought out new hazards and threats provoking intellectual discussions among energy sector think tanks, subject matter experts (SME), and scholars. These widespread discussions have led to a myriad of ideas, new and enhanced practices and standards, and sparked hypothetical scenarios and their consequences that were not possible just a few decades ago.[9] This literature review will

[7] Manimaran Govindarasu and Adam Hahn, "Cybersecurity of the Power Grid: A Growing Challenge," U.S. News and World Report, last modified February 24, 2017, https://www.usnews.com/news/national-news/articles/2017-02-24/cybersecurity-of-the-power-grid-a-growing-challenge.

[8] "Consulting for Critical Infrastructure," Cytek, accessed August 27, 2018, https://www.cytek.com/consulting-for-critical-infrastructure/.

[9]Aranyaand Chakrabortty et al., *Digital Grid: Transforming the Electric Power Grid into an Innovation Engine for the United States*, arXiv:1705.01925 (North Carolina: North Carolina State University, 2017), http://arxiv.org/abs/1705.01925.

examine literature pertinent to cyber security safeguards in the energy sector. This thesis will delineate the critical infrastructure of the energy sector into three fundamental cyber security elements: (1) security system robustness; (2) joint public and private collaboration; (3) available options to mitigate risk.

1. Cyber Security Robustness

The prolific data breaches in recent months and the exhaustive efforts by cyber security professionals to stop them is a stark reminder to have a robust cyber security system. The Director of National Intelligence stated in 2009 testimony before the Congress, "the growing connectivity between information systems, the internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, energy pipelines, financial networks, and electrical power."[10] High-tech information technology (IT) systems, with the direct involvement of operators, regulate the U.S. power grid's entire electrical production process from generation, transmission, and distribution, most commonly referred to as industrial control systems (ICS).[11] The National Institute of Standards and Technology (NIST) defines industrial control systems as "combinations of control components that act together to achieve an industrial objective."[12] The United States' critical infrastructure is heavily reliant on ICS to manage utility industrial operation.[13] It is just as important to defend industrial control systems as it is to protect the physical assets in the power grid.

[10] *Examining the Cyber Threat to Critical Infrastructure and the American Economy: Hearing Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security*, *House of Representatives*, 112th Cong. 1 (2009), https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72221/pdf/CHRG-112hhrg72221.pdf.

[11] "Industrial Control System," Trend Micro USA, accessed August 25, 2018, https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system.

[12] "Industrial Control System," CSRC, accessed August 25, 2018, https://csrc.nist.gov/Glossary/?term=4752.

[13] Lendvay, Ronald, "Shadows of Stuxnet: Recommendations for U.S. Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack" (master's thesis, Naval Postgraduate School, 2016), 138, https://calhoun.nps.edu/bitstream/handle/10945/48548/16Mar_Lendvay_Ronald.pdf?sequence=1&isAllowed=y.

The nations outermost cyber security defenses are no match to hackers. A 2014 report released by the Committee of Homeland Security and Government Affairs revealed figures that clearly show the federal government's inability to successfully mitigate the 48,000 times government systems were targeted that year.[14] The statistics are more concerning in the privately-owned electrical utility realm with only 40 percent of all cyber-attacks ever being discovered, with even less of those publicly disclosed.[15] If laws or moral obligation do not require companies to reveal they have been hacked, they most likely will not; revealing flawed information that can smear a company's reputation is bad business that will ward off customers. This ultimately creates an uninformed public and hinders the success rate for solutions. The holes that allow penetration into the system are often the result of outdated software and failures to install updated programs and/or patches. These types of controllable shortcomings pose a great risk to our power grid critical infrastructure.

Adversaries, without a doubt, have infiltrated the woefully insecure networks and systems that manage industrial equipment that keep our lights on. However, the United States is not yet on the verge of declaring our first cyber-war, which could result in blackouts, mass chaos, and cascading effects to other critical infrastructures.[16] Sandworm, a Russian-connected computer hacking group, was responsible for the December 2015 Kiev, Ukraine, blackout--the first of its kind in the world because it was a cyber-attack induced outage.[17] The antagonists deliberately conducted a similar attack, taking down a transmission station, the following year. The hacker's actions were sophisticated, which demonstrated they had comprehensive information about the electrical grid's management system and how to manipulate it.[18]

[14] National Cybersecurity and Communications Integration Center Act, 113th Cong (2014), https://www.congress.gov/congressional-report/113th-congress/senate-report/240/1.

[15] Ibid.

[16] James Zirin, "Are We on the Brink of a Cyber-War?" Huffington Post, last modified April 26, 2010, https://www.huffingtonpost.com/james-d-zirin/are-we-on-the-brink-of-a_b_475237.html.

[17] Andrea Peterson, "Hackers Caused a Blackout for the First Time, Researchers Say," The Washington Post," last modified January 5, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/?noredirect=on&utm_term=.17f8269a82ae.

[18] Ibid.

Some scholars caution against comparing Ukraine's Soviet era power grid to the United States' behemoth of interconnected systems that make up its power grid, because "America's power grid infrastructure is substantially more complex than Ukraine's."[19] Assuming the cyber-attacks in Ukraine is an impossible scenario in the United States is far-fetched, but it would certainly pose a prodigious challenge to those who dare. The U.S. power grid is an intricate web comprised of hundreds of electric utility companies, all with the same objective to produce power and provide it to their customers.[20] Electrical companies manage electricity in their own geographical locations; though separate entities, each are interconnected via power lines, transmission systems, generation facilities, and systems that reduce the possibility of a blackout and mitigate the aftermath in the event of a blackout.[21] Hurricanes Harvey and Katrina are evidence of the tenacity of the electrical grids' employees to restore power in a practical amount of time after catastrophic events.[22] Cyber security professionals can learn to respond to cyber-attacks with the identical steadfast dedication that emergency responders put forth during restoration efforts after a natural disaster. Additionally, while it is challenging to successfully take a few menial pieces of equipment offline, it is exponentially more arduous to shut down all operations of an entire electrical company let alone a multitude of them.[23]

[19] Robert Lee and Sergio Caltagirone, "Dragonfly 2.0: Hackers Don't Control America's Power Grid," Fortune, last modified September 11, 2017, http://fortune.com/2017/09/11/dragonfly-2-0-symantec-hackers-power-grid/.

[20] "United States Utility Company List by State," BEST, accessed August 27, 2018, http://www.bestenergynews.com/solar/utility_co/utility_companies.php.

[21] "U.S. Electric System Is Made up of Interconnections and Balancing Authorities," U.S. Energy Information Administration (EIA)," last modified July 20, 2016, https://www.eia.gov/todayinenergy/detail.php?id=27152.

[22] "UPDATED: Electric Utilities Make Headway on Harvey Outage Restorations," Electric Light and Power, last modified August 28, 2017, https://www.elp.com/articles/2017/08/harvey-causes-300-000-power-outages-at-peak.html.

[23] Ibid.

2. Public and Private Sector Collaboration

If the public and private electric companies collaborate with one another, they will have an advantage over cyber threats and will have the capacity to defend against them.[24] About 85 percent of the United States' energy infrastructure is owned and operated by the private sector; however, the entire sector, including entities run by the government, face the same challenges against cyber threats.[25] Therefore, company stakeholders must understand that it is imperative to have a robust cyber security program to prevent probable threats. The government and privately-owned companies have their own strengths and weaknesses to combatting cyber criminals. For example, the U.S. government has far more resources than their private counterparts to determine the origin of an attack. The federal government has working relationships with law enforcement agencies with large databases, they have the means and authority to analyze foreign intelligence, and access to their own highly sensitive systems that no private utility could ever have access to.[26] For these reasons, the public sector is "better positioned to investigate and prosecute cyber criminals."[27]

The country's health and welfare depend on a well-guarded and resilient critical infrastructure made up of the most vital physical and cyber assets. "The National Infrastructure Protection Plan (NIPP) established a partner framework that enables federal, state, regional, local, tribal, territorial, and international governments to collaborate among their private sector associates."[28] According to DHS, this partner framework improves all aspects of infrastructure from development and communication to risk assessment and

[24] Arnav Jagasia, "A Look into Public Private Partnerships for Cybersecurity," Public Policy, last modified April 18, 2017, https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for.

[25] Federal Emergency Management Agency, *Critical Infrastructure Long-Term Trends and Drivers and Their Implications for Emergency Management* (Washington, DC: FEMA, 2011), https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf.

[26] Ibid.

[27] Ibid.

[28] Department of Homeland Security, *NIPP 2013 Partnering for Critical Infrastructure Security and* Resilience (Washington, DC: DHS 2013), https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

response.[29] A partnership of all energy sector stakeholders will make implementing cyber security and resilience activities throughout the country seamless yet robust.

3. Mitigating Options

Modern electrical systems are built to operate in the most extreme weather environments and are able to quickly restore to normal operations after gale force winds, raging wildfires, lightning strikes, snow storms, and a variety of system failures. [30] Apart from the standard features incorporated into the electrical systems physical design, which withstand the wrath of mother nature, they are also built with sophisticated technological safeguards to protect against unpredictable actors.[31] Just as the methods and techniques of modern hackers evolve, so must the protections and responses of the systems evolve.

If the United States fell victim to an attack similar to the level of sophistication used in the Ukraine cyber-attack, the capability to operate the power grid in a manual state without the digital overlay and automated controls would be difficult, but achievable.[32] In addition, to prepare for a cyber-attack, the United States electricity sector participates in the largest biennial power grid security exercise called GridEx, which is "designed to execute the electricity sector's crisis response to simulated coordinated cyber security and physical security threats and incidents, to strengthen utilities' crisis response functions, and to provide input for lessons learned."[33]

Lastly, the Energy Policy Modernization Act of 2015 is designed to defend our national energy grid from terrorist cyber-attacks. The bipartisan act supported by both Senate Majority Leader Mitch McConnell and Senate Minority Leader Harry Reid is proof

[29] Ibid.

[30] James Zucchetto, *Terrorism and the Electric Power Delivery System* (Washington, DC: The National Academies Press, 2012), 55, https://www.nap.edu/read/12050/chapter/8.

[31] Ibid.

[32] Robert Knake, "A Cyberattack on the U.S. Power Grid," Council on Foreign Relations, last modified April 3, 2017, https://www.cfr.org/report/cyberattack-us-power-grid.

[33] "GridEx III Showcases Steady Improvements on Participation, Coordination," Transmission & Distribution World, last modified April 4, 2016, https://www.tdworld.com/transmission/gridex-iii-showcases-steady-improvements-participation-coordination.

of the United States' determination to keep hackers away from our power grid.[34] The Act provides faster and more effective responses when threats arise, authorizes additional cyber security research, and erects stronger cyber security defenses. Additionally, the bill grants the energy secretary emergency authority in the event of a cyber-attack on the electrical grid. If the United States can manage to mitigate the aftermath of a cyber-attack, the nation will position itself to be able to seamlessly restore power. However, the Act falls short of an actual true energy reform by continuing and expanding the government knows best model, which has a history of failure.

C. POTENTIAL EXPLANATIONS AND HYPOTHESES

The following elements will be discussed in the chapters that follow because of their importance to cyber security safeguards. The first element is the robustness of the power grid's network systems that requires improvement. The number of cyber-attack related cases targeting all U.S. critical infrastructures and their industrial systems have surged since 2010.[35] Per a 2015 report produced by Department of Homeland Security Industrial Control Systems Computer Emergency Response Team (ICS-CERT), the energy sector faced a grueling 20 percent spike in targeted attacks in under a decade.[36]

The second element of collaboration between the public and private sectors also requires improvement. Cyber-attacks are inevitable, but the nation will continue to use computerized systems. Even with the obvious cyber and physical security threats to U.S. critical infrastructure, there is an indistinct divide in the working relationship between the private and public sectors.[37] A massive proportion of the energy sector and assets

[34] Energy Policy Modernization Act, 114th Cong. (2015) https://www.govtrack.us/congress/votes/114-2016/s54.

[35] "Cyber Security Solutions for Critical Infrastructure and Industrial Control Systems," FireEye, last modified 2017, https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/pf/ms/sb-critical-infrastructure.pdf.

[36] Ibid.

[37] David Hall, "Why Public-Private Partnerships Don't Work," Public Services International, (February 2015): 56, Public Services International, http://www.world-psi.org/sites/default/files/rapport_eng_56pages_a4_lr.pdf.

important to national security are owned and operated by private organizations.[38] Accordingly, due to the great influence private organizations have in the electrical sector, they must "promote cooperation among public and private entities that cultivates cohesive, interdependent agreements and communication, which is crucial to preserving critical infrastructure security and resilience."[39]

The third element of mitigation need improvement largely due to weakened computer control system vulnerabilities. The weakened controls include "entity wide security program planning and management, access controls, application software development and change controls, and segregation of duties, system software controls, and service continuity controls."[40]

To better protect our cyber infrastructure to prevent a major power grid attack, three things must be done: there must be a higher level of situational awareness against adversarial threats, tougher security standards and measures must be in place to combat cyber threats and vulnerabilities, and lessons applied from analysis of malicious physical and cyber security incidents against the electrical grid.

It will never be an easy task to defend the American power grid from cyber-attacks because of the size and scope of the grid.[41] Chris Martin and Will Wade claim the grid is composed of a myriad of computerized and physical equipment linking almost all standing structures in the United States. Additionally, because the electrical grid must continually be operational, providing the exact quantity of electricity where it is needed during every second of the day means it is something that cannot be taken offline to repair or upgrade for extended periods of time. The pace of the technology used to operate the equipment is

[38] "Electricity 101," Department of Energy, accessed August 27, 2018, https://www.energy.gov/oe/information-center/educational-resources/electricity-101.

[39] "Critical Infrastructure Sector Partnerships," Department of Homeland Security, accessed December 8, 2017, https://www.dhs.gov/critical-infrastructure-sector-partnerships.

[40] Anthony Coresman, and Justin Cordesman, *Cyber-Threats* (Santa Barbara, CA: Praeger, 2001), 200, ABC-CLIO.

[41] Chris Martin and Will Wade, "America's Power Grid," Bloomberg, last modified March 14, 2016, https://www.bloomberg.com/quicktake/u-s-electrical-grid..

developing more rapidly than the grid infrastructure itself, making it challenging to meet security standards.

A vast area that needs attention is cyber security literacy. Many cyber security breaches can be traced to phishing attacks, in which corporate employees click on fake links to allow hackers to install malware on their computer network. Many government and private employees access sensitive servers every day and these people may have insufficient training on how to protect the network they are using. Regardless how much security administrators strengthen a network, it can all be brought down by network users inadvertently clicking on a link from an unknown sender.

Security standards allow power utility companies to properly safeguard their assets. “The North American Electric Reliability Corporation (NERC), which oversees the grid in the United States and Canada, has rules known as Critical Infrastructure Protection (CIP) compliance, for how electric companies are required to protect power grid both physically and electronically.”[42] These set of rules and requirements are intended to provide a standard for electrical grid asset monitoring and to provide guidance on how to defend the valuable equipment in the nations bulk electric system.[43]

Additionally, the U.S. National Institute of Standards and Technology (NIST) provides companies with additional guidelines on cyber protection, which has proven to boost security measures at high-voltage transmission sites and power generation facilities.[44] In contrast, Manimaran Govindarasu and Adam Hahn in their article “Cybersecurity of the Power Grid: A Growing Challenge,” claim the NIST guidelines minimally impact the cyber and physical security for low-voltage distribution sites that serve to provide electricity to the end customer. Statistically, cyber-attacks against low-voltage systems account far fewer than those against high-voltage systems found in a power

[42] Manimaran Govindarasu and Adam Hahn, “Cybersecurity of the Power Grid: A Growing Challenge,” US News, last modified February 24, 2017, https://www.usnews.com/news/national-news/articles/2017-02-24/cybersecurity-of-the-power-grid-a-growing-challenge.

[43] Ibid.

[44] Ibid.

plant.[45] Protecting the borders of any power distribution facility is often more difficult than defending the middle of it because multiple companies become involved with daily operations, networking together different systems, adding more physical locations to protect.[46]

According to Symantec, within the last year a complex and highly organized hacking group known as Dragonfly penetrated multiple U.S. power companies, and the group most likely had the opportunity to sabotage electrical production and distribution.[47] The unrestricted access to the power grid would could have knocked power out to customers for days. It is not known for certain why the perpetrators did not conduct any further action. Symantec believes it might have been a proof of concept attack or a political statement to prove to the United States government and agencies in charge of the security for industrial control networks that hackers have the capability to access what they want and when they want to.[48] One thing for sure is cyber-security measures need to drastically change.

Though there have been more frequent and increasingly sophisticated cyber security events targeting the United States electrical sector, these actions have been largely unsuccessful so far. These cyber-attacks have been simple or crude causing minimal or no outages. While no events have been catastrophic, they make the vulnerabilities of the power grid clearer, that there is potential for more significant damage. The lessons learned from these events will be to harden security systems, advocate for grid modernization, and foster new approaches to increase cyber security to prevent a perilous attack.

[45] Ibid.

[46] Ibid.

[47] Elizabeth Weise, “Intrusion - But No Attack - On U.S. Energy Grid Is a Warning, Says Former NSA Official,” USA Today, last modified September 7, 2017, https://www.usatoday.com/story/tech/news/2017/09/06/dozens-power-companies-breached-hackers-cybersecurity-researcher-says/638503001/.

[48] Ibid.

D. RESEARCH DESIGN

This thesis assesses the empirical evidence for each of the three elements of robustness, collaboration, and mitigation of cyber security employed in the power grid. It uses comparative case studies of the Ukraine power grid attacks in 2015 and 2016 as well as the Dragonfly 2.0 campaign, which has targeted the United States, Switzerland, and Turkey. It also uses statistical analysis on the number of successful intrusions and attacks against United States energy service provider companies. Case studies and statistical analysis through the review of published literature are the primary approaches to answer my research question as these are the most appropriate to provide the best evidence to make a causal argument. The purpose of this thesis is not to infer or speculate who the primary cyber threat actors are but rather to focus on how cyber security in an electrical grid is applied, how it is exploited when the electrical grid is not adequately protected, and recommended approaches to better strengthen the barriers within the energy critical infrastructure.

E. THESIS OVERVIEW

This first chapter serves as an introduction to provide the reader with the problem description of the energy sectors susceptibility to hacking and a broad overview of three primary elements of robustness, collaboration, and mitigation. The second chapter will provide in detail power grid vulnerabilities that can be exploited through real world case studies. The third chapter will review the power grids critical infrastructure management and give an overview of the defense in depth security architecture and its strategy elements. The fourth chapter will assess the public and private electrical sectors collaboration of cyber security practices and standards and the existing landscape for electrical grid cyber security governance. This chapter will discuss the collaboration between the public industry and the United States government and the standards, guidelines, and practices they promote to protect the energy sectors computer network. The fifth chapter will delve into the challenges within specific areas of vulnerability in the power grid control centers, substations, and communication centers. It will also discuss safeguard measures that are currently in place and the technologies and actions that help mitigate the impact of a potential cyber-attack. The sixth chapter will conclude the thesis by identification of the challenges the energy sector faces when implementing power grid safeguards, the public and private pre-planned responses, and possible lessons to improve cyber security.

II. ANALYSIS OF THE CYBER-ATTACKS ON THE UKRAINIAN AND WESTERN ENERGY SECTORS

Espionage is not a new concept. Since there have been enemies, the role of espionage played out in warfare has meant the difference between winning and losing. Espionage in the modern era has taken a new turn involving armies of nefarious computer hackers. These cyber crooks use their technical expertise to gain military, political, or economical advantage. Russia is one of the most infamous state sponsors for large-scale cyber-attacks and their training ground to conduct cyber espionage and cyber-attacks have been in their neighboring country Ukraine. The following case studies will exhibit Russia's cyber might and identify how it is using its proxies for non-linear strategic cyber-attacks in the east that will have long term consequences in the west.

A. CYBERWAR ON UKRAINE'S POWER GRID

It sometimes seems like any network connected to the internet, including those in at an electrical plant are swarming with hackers attempting to gain unauthorized access.[49] Russian hackers have obtained hands-on access to utility control systems in the United States and abroad.[50] Andy Greenberg's 2017 article "How Power Grid Hacks Work, and When You Should Panic" undoubtedly indicates that although cyber-attack dangers are real and continue to happen regardless of endless cyber security update measures. Greenberg claims that there is no need to sound the alarm for every attempted power grid penetration. Giving each attempted attack and responding to them all with equal attention would be equivalent to treating every convenience store shoplifter as they were an unstable and precarious leader with access to a nuclear arsenal.[51] A breach to a power grid can range from a typical malware infection to months or years of nation-state funded

[49] Andy Greenberg, "How Power Grid Hacks Work, and When You Should Panic," Wired, last modified October 13, 2017, https://www.wired.com/story/hacking-a-power-grid-in-three-not-so-easy-steps/.

[50] Ibid.

[51] Ibid.

reconnaissance.[52] These types of incidents can have drastically dissimilar consequences, ranging from meager personal information acquisition to a cascading infrastructure catastrophe. The event that occurred in Ukraine characterizes the aftermath of the latter.

On December 23, 2015, Ukrainian Kyivoblenergo, an electricity distribution company specializing in electrical transmission and supply, announced service disruptions to its customers.[53] Power outages are common during harsh winter times in former USSR countries because outdated equipment can struggle with electrical demands, when customers lost power, there was no immediate reason to suspect unusual circumstances surrounding this outage. However, it came to light that something was exceptionally different about this outage because customers did not lose power from severe weather event or aging equipment that failed. Disruptions had occurred because of a third party's illegal entry into Kyivoblenergo's mainframe and remote networks through cyber-enabled backdoors. The Kyivoblenergo power grid is managed by control stations that are connected to substations, switches, and sensor in arrangements termed supervisory control and data acquisition (SCADA) systems. For approximately three hours, seven 110 kV and 23 35 kV substations were remotely disengaged. The cyber-attack put other parts of the distribution grid to a halt, which forced Kyivoblenergo employees to switch to manual mode, and restored power using Soviet-era manual controls.[54] Despite restoration to the three affected substations, Kyivoblenergo continued to run under constrained operations.

Kyivoblenergo's initial estimates put the affected total customers at around 80,000, but after the realization that two other companies were also attacked updated estimates brought the affected total to 225,000 customers that lost power throughout the region.[55] Not long following the cyber-attack, Ukrainian government officials held Russian security

[52] Ibid.

[53] Electricity Information Sharing and Analysis Center (E-ISAC*), Analysis of the Cyber-attack on the Ukrainian Power Grid* (Washington, DC: E-ISAC, 2016), https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[54] Peter Behr and Blake Sobczak, "Utilities Look Back to the Future for Hands-on Cyberdefense," E&E News, last modified July 21, 2016, https://www.eenews.net/stories/1060040590.

[55] Pavel Polityuk, Oleg Vukmanovic, and Stephen Jewkes, "Ukraine's Power Outage Was a Cyber-attack: Ukrenergo," Reuters, last modified January 18, 2017, https://www.reuters.com/article/us-ukraine-cyber-attack-energy/kiev-power-outage-in-december-was-cyber-attack-ukrenergo-idUSKBN1521BA.

services accountable for the outages.[56] As a result of the allegations against the Russian Federation, "investigators in Ukraine, as well as private companies and the U.S. government, performed analysis and offered assistance to determine the root cause of the outage."[57] The Ukrainian power grid attacks became the first publicly acknowledged power outage as a result from a cyber-attack.[58]

1. The Final Stages of the Cyber-Attack

The cyber-attack was carefully coordinated and synchronized, most likely because of extensive reconnaissance and exploitation of the vulnerable Ukrainian networks. An investigation revealed that the cyber-attacks, which disrupted power to several regional and central sites, happened approximately 30 minutes apart from each other.[59] As reported by the Department of Homeland Security, remote operation of the breakers could have been managed a couple ways by the external hackers: using bundled administrative SCADA software pre-installed from the original equipment manufacturer (OEM) or via a virtual private network (VPN) that allows a remote encrypted connection from a hackers computer to manipulate the controls of another computer over the internet.[60] However, the Escal Institute of Advanced Technologies investigation, a for-profit company that provides training in cyber and information security, found that the rogue players attained genuine credentials from electrical plant employees months before the cyber-attack to assist with

[56] Ibid.

[57] Electricity Information Sharing and Analysis Center (E-ISAC), *Analysis of the Cyber-attack on the Ukrainian Power Grid* (Washington, DC: E-ISAC, 2016), https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[58] Ibid.

[59] John Leyden, "BlackEnergy Malware Activity Spiked in Runup to Ukraine Power Grid Takedown," The Register, last modified March 4, 2016, https://www.theregister.co.uk/2016/03/04/ukraine_blackenergy_confirmation/.

[60] Marco Chiappetta, "Hackers Brought Down Ukrainian Power Grid in December, Homeland Security ICS-CERT Confirms," Forbes, last modified February 27, 2016, https://www.forbes.com/sites/marcochiappetta/2016/02/27/hackers-brought-down-ukrainian-power-grid-in-december-homeland-security-ics-cert-confirms/.

gaining remote access.[61] The cyber weapons used or the hackers' comprehensive knowledge about the power grid was not their key asset, it was their ability to perform long term surveillance on several central facilities leading to the use of a multiple phased plan of attack.

Investigations confirmed that during the final stages of the industrial sabotage, the hackers initiated the KillDisk wiper malware on network drives that hindered or permanently disabled Ukrainian power grid equipment that is essential to run the facilities that serve its customers.[62] "The KillDisk software is a type of malware that deletes particular files on target systems as well as corrupts the master boot record, the first sector of any hard disk that identifies where and how an operating system is located in order for it to load, thus incapacitating the system it hijacks."[63] Additionally, the hackers maliciously corrupted the firmware of certain Serial-to-Ethernet converters at select substations, making them inoperable.[64] These tiny boxes in the substations have the job of translating internet protocols to communicate with older equipment.[65] Furthermore, to hinder the Ukrainians from executing emergency action plans for incident response and restoration, the hackers remotely disconnected uninterruptable power supplies (UPS) to two of the electrical companies control centers that provide emergency backup power in the event primary power is lost.[66] These critical pieces of equipment that are supposed to

[61] Electricity Information Sharing and Analysis Center (E-ISAC), *Analysis of the Cyber-attack on the Ukrainian Power Grid* (Washington, DC: E-ISAC, 2016), https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[62] Zack Whittaker, "US Report Confirms Ukraine Power Outage Caused by Cyberattack," ZDNet, last modified February 29, 2016, https://www.zdnet.com/article/us-report-confirms-ukraine-power-outage-caused-by-cyberattack/.

[63] Ibid.

[64] Del Rodilas, "Hack on Ukrainian Power Grid Highlights the Urgency for Accelerated Threat Intelligence in Industrial Control Systems - Palo Alto Networks," Palo Alto Networks, last modified April 7, 2016, https://researchcenter.paloaltonetworks.com/2016/04/utilities-pan-os-7-1-utilities/.

[65] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," Wired, last modified June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

[66] D. E. Whitehead, "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies," *Schweitzer Engineering Laboratories, Inc.* (September 2017): 8, https://doi.org/10.1109/CPRE.2017.8090056.

provide near instantaneous emergency power to equipment when the main input power source fails were reconfigured to power off instead of power on.

2. BlackEnergy Malware

Kyivoblenergo also claimed that they had been infected with BlackEnergy, a Trojan used to initially conduct cyber espionage, setting forth the path for denial-of-service (DoS) and information destruction attacks.[67] The cyber espionage allowed hackers to illicitly acquire login credentials that enabled them to remotely manipulate the power grid. The hackers targeted electric company employees who serve Ukraine's 24 geographical regions with a variety of administrative accesses using an email spoofing tactic called spear phishing. [68] Kim Zetter,, in her article "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," asserts that when the Word documents were delivered in emails, and the unbeknownst victim opened and accepted an 'Enable Macros' popup request, a backdoor to the system opened. Neither BlackEnergy nor KillDisk encompassed the mechanisms used to deliberately cause an outage. However, the codes were used to attack and delay restoration efforts, respectively.

B. CYBERWAR ON THE WESTERN POWER GRID

Symantec, an American software company that provides cyber security software and services, has recently detected a strikingly new trend of cyber-attacks aimed at energy sector organizations.[69] The infamous Dragonfly organization, also known as Energetic Bear, has been the driving force behind the cyber-attacks targeting the western power grid. The Dragonfly organization is confirmed to be operating since at least 2011 when attackers aimed their campaign at the United States and Canadian aviation and defense companies.

[67] Thomas Brewster, "NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid," *Forbes*, last modified July 3, 2017, https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/#788e7bec6b89.

[68] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[69] Pierluigi Paganini, "Dragonfly 2.0: The Sophisticated Attack Group Is Back with Destructive Purposes," Security Affairs, last modified September 7, 2017, https://securityaffairs.co/wordpress/62782/hacking/dragonfly-2-0-campaigns.html.

Initial Dragonfly operations seemed to be for exploration, scouting, and sophisticated cyber espionage campaigns. They evolved into Dragonfly 2.0 where its operations progressed into positioning for destructive activities.[70] Dragonfly's objective shifted from reconnaissance to digital invasion by gaining access to energy facility operational systems. The posture change may indicate Dragonfly's motive may be shifting from intelligence collection to industrial sabotage.[71]

It was in 2013 that Dragonfly had begun another stage in their attacks, concentrating on United States' and European energy companies. Dragonfly scaled back operations in 2014 when they were detected by Symantec but reemerged in December 2015. A new wave of attacks began with the sending of malicious emails masked as a New Year's Eve party invitation to energy sector targets, according to Symantec.[72]

1. Dragonfly 2.0 Targets Energy Sector Gaining Access to SCADA Systems

The attack campaign continued in 2017 with sustained phishing, typically with Microsoft Word documents disguised as a resume or report attached to emails. Unbeknownst to company employees, the attachments contained a template injection attack, a silent way to harvest network credentials using the server message block (SMB) protocol. According to TechTarget, a digital marketing company, defines SMB protocol as "a client-server communication protocol used for sharing access to serial ports, printers, files and other resources on a network."[73] The malicious documents did not rely on traditional methods such as Visual Basic for Applications (VBA), the programming language for Microsoft Office software suite, or a list of executable commands used to spread the malicious software.[74] Instead, the email attachment uploads a service request

[70] Ibid.

[71] Ibid.

[72] Ibid.

[73] "Server Message Block Protocol," Search Security, accessed August 30, 2018, https://searchnetworking.techtarget.com/definition/Server-Mesdsage-Block-Protocol.

[74] Edward Kovacs, "Template Injection Used in Attacks on U.S. Critical Infrastructure SecurityWeek.Com," Security Week, last modified July 10, 2017, https://www.securityweek.com/template-injection-used-attacks-us-critical-infrastructure.

file through an SMB portal to collect an unsuspecting computer user's authentication information.[75]

2. Backdoor.Dorshel and Backdoor.Goodor Malware

With the illegally acquired credentials, hackers were able to conduct follow-up attacks against targeted organizations. They used a variety of techniques to install Backdoor.Dorshel or Backdoor.Goodor malware that allowed remote access to computer terminals.[76] Attackers with unrestricted remote access were able to chart their targeted domain and systems as well as increase their administrative rights, which allowed them to connect to industrial control systems that potentially operate the electrical grid. Additionally, the attackers were able to download sensitive information to their remote command and control mainframe. "Most modern SCADA systems will at least contain the following peripherals: supervisory computers, remote terminal units (RTU), programmable logic controllers, communication infrastructure, and human-machine interfaces."[77] Even though the attackers were able to acquire unauthorized entry to SCADA systems, which gave them access to remotely control electrical production, transmission, and distribution, no service interruptions or outages were reported.

Throughout the 2014 and 2017 attack campaigns, DragonFly used state-of-the-art malware specially developed to attack energy sector webpages in addition to email spoofing attacks targeting dozens of U.S. power companies. Given the perseverance and the advanced operations, it is problematic to attribute the cyber-attack to a source, since proxies, third parties, and fake artifacts in malware code are used to obfuscate their true

[75] Sean Bird, "Attack on Critical Infrastructure Leverages Template Injection," *TALOS Intelligence* (blog), July 7, 2017, http://blog.talosintelligence.com/2017/07/template-injection.html.

[76] Pierluigi Paganini, "Dragonfly 2.0: The Sophisticated Attack Group Is Back with Destructive Purposes," Security Affairs, last modified September 7, 2017, https://securityaffairs.co/wordpress/62782/hacking/dragonfly-2-0-campaigns.html.

[77] Donald Krambeck, "An Introduction to SCADA Systems," All About Circuits, last modified August 31, 2015, https://www.allaboutcircuits.com/technical-articles/an-introduction-to-scada-systems/.

origin. Hackers imbedded strings of Russian and French coding, an attempt to elude authorities.[78]

C. PLAN OF ATTACK—TECHNIQUES AND PROCEDURES

Like the typical cyber-attack on a home computer, the Ukraine power grid attack started simple with company employees commonly receiving strings of phishing emails containing an attachment disguised with malware. This case is no different than a hacker tapping into a personal home network, except that it was performed on a grander scale. The key goal with the BlackEnergy malware was to steal user credentials for use months later to control breakers and manipulate the grid.[79] These hacks not only required a high level of problem-solving skills to combine all the collected information, but a lot of patience. "The attackers then used stolen VPN credentials to reach the industrial control systems network, and remote access tools to control the human machine interface (HMI)."[80] HMIs, in the simplest terms, are any software or device that permits a human to interact with physical equipment. This can be as simple and ubiquitous as our smartwatches and smartphones or as technically advanced as a multi-touch enabled control panel at a power plant. With remote control of the power grid, the Russian hackers were able to manipulate the control system to pull the substation breakers to cause the blackout.

The hackers went to great lengths to hide their tracks and managed to buy themselves time by installing their own custom firmware. Russian hackers are experts at concealing participation in any state sponsored cyber-attacks. Additionally, the hackers waged a telephone denial-of-service attack against customer call centers, thwarting the

[78] Andy Greenberg, "Hackers Gain Direct Access to US Power Grid Controls," Wired, last modified September 6, 2017, https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/.

[79] GReAT, "BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents," Securelist - Kaspersky Lab's Cyberthreat Research and Reports (blog), January 28, 2016, https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/.

[80] Andrew Thomas, "Requirements for IIoT Data Communication," Skynet, last modified July 5, 2017, https://skkynet.com/requirements-iiot-data-communication/.

ability for customers to report the outage and providing the hackers with another smokescreen to go undetected.[81]

The Russian government adamantly denies any participation in any of the staging hacks preceding the Ukrainian power grid cyber-attacks, regardless of evidence pointing to Russian affiliated hackers. The official Russian government posture about their role in cyber-space is that it only participates in defensive cyber security measures, which was confirmed in their doctrinal statement released in the latter half of 2011.[82] Though the Kremlin claims to not participate in offensive cyber activities, it has become more obvious from other cyber-attacks against France, Germany, and Georgia that offensive practices have become conventional in Russian military operations and has most likely already been incorporated into their strategic deterrence agenda.

D. KEEPING CYBER-ATTACKS ON THE POWER GRID IN PERSPECTIVE

In retrospect, after all the details have been analyzed and released, it is obvious how the hackers were able to go undetected for so long only to be singled out after the cyber-attacks took place. Nonetheless, it is an undertaking to understand what is going on within a power grid network if there are not enough adequately trained personnel or resources to detect abnormal activity. Also, if there is one takeaway the United States can learn from the Ukrainian attacks it is that if America succumbs to a similar attack, it will not be as easy as manually flipping Soviet era circuit breakers to restore power. Most of America’s industrial control systems have migrated to automated systems, which are limited to their programming and less versatile than a human performing a flexible variety of tasks like replacing a failed part.

[81] Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,” Wired, last modified March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[82] Park Donghui, Julia Summers, and Michael Walstrom, “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks,” The Henry M. Jackson School of International Studies, last modified October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

Future attacks will most likely happen, so it is crucial power companies value the significance of protecting their assets against a cyber-attack, because doing nothing to prevent one will cost more than stopping one with cyber security measures in place.[83] The impact of a power outage is typically measured in the amount of time power is restored, the impact it has on other critical infrastructures, and the number of electrical customers affected.[84] According to the E-ISAC report on the Analysis of the Cyber-attack on the Ukrainian Power Grid, on a macro scale, the Ukrainian power outages have a low impact because of its short duration and the small populace actually affected by the outage. However, from a business and economic standpoint, any unexpected disruption to the normal operations would be rated critical or high in terms of dependability of their organizational system.[85]

E. ANTICIPATORY RESPONSES

All electric companies in the North American continent have been trying to decipher and take their own actions in lieu of the investigation reports and released data that headlined in Ukraine.[86] The theme of what can be done to prevent and prepare for a catastrophic attack on the most important critical infrastructure has been brought to the attention of stakeholders in "Capitol Hill, trade associations, the Electricity Information Sharing and Analysis Center (E-ISAC), and regulators."[87] Remote manipulation of the power grid by aggressive state actors is a real and troublesome fact and investors and U.S.

[83] Marco Berger, "Cybersecurity and the Power Grid: Preparing for the Future," Transmission & Distribution World, last modified November 27, 2017, https://www.tdworld.com/smart-grid/cybersecurity-and-power-grid-preparing-future.

[84] Electricity Information Sharing and Analysis Center (E-ISAC), *Analysis of the Cyber-attack on the Ukrainian Power Grid* (Washington, DC: E-ISAC, 2016), https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[85] Ibid.

[86] Brian Harrell, "Why the Ukraine Power Grid Attacks Should Raise Alarm," CSO, last modified March 6, 2017, https://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html.

[87] Ibid.

government officials need to take a step back and realize the United States is an optimal next target. [88]

The Russian hackers that targeted Ukrainian power facilities were not amateurs that happened to mistakenly stumble upon an unlocked computer. Russia has a reputation for having some of the world’s most talented and devious hackers, which was highlighted during the power grid cyber-attacks. These well-funded professional hackers planned their assault over many months, meticulously using every piece of illegally acquired information to their own advantage. The only way to bolster cyber security measures against hackers, is to think like a hacker. It only takes one mistake by a company employee or an unforeseen loophole in the newly installed data center software for a hacker to take advantage of these vulnerabilities. Hackers, whether Russian or another aggressive state actor, are in front of their computer screens constantly probing at a power grids defense.

To beat a hacker, utility companies sometimes must think like a hacker. Power companies can engage in ethical hacker services against their own security services. Ethical hacking allows a computer professional to methodically break into a selected computer system to identify and fix system weaknesses.[89] Better to find your own susceptibilities and repair them than have an aggressor exploit them. The entire process may seem counterintuitive. Although, there is no better way for a company to learn the intricacies of their own power grid if it is not broken into.

F. STOPPING SCADA ATTACKS

SCADA systems and their expanding advancements have developed unanticipated dangerous weaknesses that, if taken advantage of, can ultimately destroy or permanently hinder the proper operation of a segment or the entire U.S. power grid.[90] Over 90% of electrical companies in the United States are investor-owned businesses that put a premium

[88] Ibid.

[89] “Ethical Hacker," Search Security, accessed August 30, 2018, https://searchsecurity.techtarget.com/definition/ethical-hacker

[90] Andrés Prisco, Felipe Sánchez, and John Freddy Duitama M., “Intrusion Detection System for SCADA Platforms Through Machine Learning Algorithms,” in *IEEE Xplore Digital Library* (2017): 6, https://doi.org/10.1109/ColComCon.2017.8088210.

on having low costs over the needs of cyber and physical security to maximize profit.[91] Because the majority of the electric sector offers company shares to the general public, the front of numerous investors' minds is to maximize productivity, which in turn will maximize cash flow, and potentially hamper security concerns.[92] However, even just enforcement of conventional best practices assists with mitigating a lot of the dangers presented by Dragonfly. Phishing emails is one of the most common practices used by hackers to obtain sensitive information. Targeting energy sector senior employees with malicious attachments is nothing new and likely to continue in the foreseeable future. Although, training and cognizance of suspicious emails will curtail the infection frequency. Two-factor or multi-factor authentication, an added layer of security that requires not only the username and password, but something that is unique to the user or a physical token is an additional way to verify trusted users.[93]

SCADA systems at almost every scale perform well. However, as they incorporate more technology into them, they also increasingly integrate added open system architecture becoming networked, making them vulnerable to security risks.[94] For instance, using TCP/IP to communicate between the control center and remote equipment or among equipment in a substation.[95] The advanced SCADA systems' key attribute is its ability to perform a supervisory operation over a variety of other proprietary devices. Modern SCADA systems have evolved significantly, and because utility companies recognize the easier

[91] Nikhil Parthasarathy, "Cybersecurity and the US Energy Grid," Stanford University, last modified December 20, 2016, http://large.stanford.edu/courses/2016/ph240/parthasarathy2/.

[92] "How Energy Companies Make Profit: A Closer Look at the Data," Carbon Brief: Clean on Climate, last modified November 11, 2013, https://www.carbonbrief.org/how-energy-companies-make-profit-a-closer-look-at-the-data.

[93] "What Is Two Factor Authentication?" Secure Envoy, accessed September 2, 2018, https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm.

[94] D. F. Merchán, "Open Source SCADA System for Advanced Monitoring of Industrial Processes," *IEEE Xplore Digital Library* (2017): 160–65, https://doi.org/10.1109/INCISCOS.2017.9.

[95] Ibid.

accessibility, improved efficiency, and lower costs gained through connecting their TCP/ IP networks to their SCADA systems, it has opened themselves to the risk of tampering.[96]

Dragonfly is proof that bold hackers have no limit and stop at nothing when trying to conduct cyber-espionage against the United States. [97] Symantec's security response attack investigation team indicates that although successful cyber-attacks have been recorded throughout the globe, there is still no sufficient evidence that the U.S. power grid has been infiltrated and deliberately disrupted. Nonetheless, intelligence gathering for possible future attacks is expected. There is no need to dread the lights will shutoff anytime soon, yet electrical grid operators and managers must keep a keen eye on any abnormal trends.[98] Cyber-attacks are frequently cast in the spotlight for a moment and the gravity of their breaches eventually fade until the catastrophe repeats itself. Prolonging to address cyber threats before they develop into a cyber-attack will leave cyber security experts in plight.

DragonFly and other hacking groups with similar techniques and tactics will constantly evolve and continually innovate new attack methodologies to avoid detection.[99] According to Pierluigi Paganini, the electrical industry must be able to combat their adversaries' tactics by having a cyber threat intelligence partnership with power grid regulators, sister companies, and the government because cyber-attacks that prey on the electrical grid will not fade away. According to the U.S. Federal Government, SCADA

[96] "Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group," Symantec, last modified October 20, 2017, https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks.

[97] Andrea Limbago, "Destructive Cyberattacks Are Only Going to Get Worse," Business Insider, last modified September 13, 2017, https://www.businessinsider.com/equifax-breach-proves-that-cyber-attacks-are-only-going-to-get-worse-2017-9.

[98] Andy Greenberg, "How Power Grid Hacks Work, and When You Should Panic," Wired, last modified October 13, 2017, https://www.wired.com/story/hacking-a-power-grid-in-three-not-so-easy-steps/.

[99] "Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group," Symantec, last modified October 20, 2017, https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks.

systems are high value assets and the protection and resiliency of the data contained within the system is the responsibility of both the public and private organizations.[100]

Dragonfly is undoubtedly a highly trained enemy, with the capability to jeopardize numerous organizations, unlawfully obtaining sensitive data, and gaining unauthorized access into critical systems. Though, it is still not fully known the extent of disruption Dragonfly were to cause if they decide to use the information they have acquired in a malicious manner, nor the actual scope of all the intelligence collection they have gathered.[101] It is a loud wake-up call that almost any employee at an energy firm can fall victim to the phishing techniques' devices that have evolved substantially since the early 1990s. Businesses in critical sectors must determine and devote substantial effort to undertake the severe dangers posed by these types of attacks. Energy companies must function with the assumption they have already been hacked and that latent advanced persistent threats are lurking in their environment.

[100] "SCADA/Business Network Separation: Securing an Integrated SCADA System," Automation, accessed September 3, 2018, https://www.automation.com/library/articles-white-papers/hmi-and-scada-software-technologies/scadabusiness-network-separation-securing-an-integrated-scada-system.

[101] Lucian Constantin, "Cyberespionage Group Might Be Planning Electrical Grid Attacks," Forbes, last modified September 6, 2017, https://www.forbes.com/sites/lconstantin/2017/09/06/cyberespionage-group-might-be-planning-electrical-grid-attacks/#7b0c54856701.

III. CRITICAL INFRASTRUCTURE MANAGEMENT

The United States Federal government in conjunction with electric power companies have spent the last decade developing sophisticated and versatile protection systems against cyber-attacks that have the potential to disturb United States electrical grid operations. Simultaneously, exposure to cyber vulnerabilities and subsequent risks have progressed. Network intrusions have drastically surged and the techniques in which they are carried out have evolved. Current cyber security measures in place may not be enough to provide reliant safeguards to face modern and arising threats.

The dependency to the digital world and its accompanying dangers were at the forefront of national interests in the latter half of the 20th century. As we crossed into a new millennium, frantic United States companies and even FEMA prudently prepared for a potential Y2K emergency, fearing that computers would fail to distinguish the year 2000 and cease to perform.[102] Possible digital system disturbances were at the forefront of concern then and have existed since 1878, only a couple of years after the telephone was invented by Alexander Graham Bell when switchboards were hacked.[103] On August 8, 2005, Congress passed the U.S. Energy Policy Act of 2005 sanctioning construction of a self-regulatory electric reliability organization, encompassing the entire North American continent. The Federal Energy Regulatory Commission (FERC) would oversee the U.S. legislation that states compliance with reliability standards would be mandatory and enforceable. This gives FERC the authority and control of compulsory reliability standards to administer the country's power grid.

On March 2007, a test performed at the Idaho National Laboratory, named the Aurora Generator Test, measured the resiliency of a diesel generator running on a supervisory control and data acquisition (SCADA) system. The Department of Homeland Security employed hackers that were successful in exploiting the control systems'

[102] "FEMA Preparing for Y2K Disaster," CNN, February 24, 1999, http://www.cnn.com/TECH/computing/9902/23/fema.y2k/.

[103] Michael Devitt, "A Brief History of Computer Hacking," Dynamic Chiropractic, last modified June 18, 2001, https://www.dynamicchiropractic.com/mpacms/dc/article.php?id=18078.

vulnerabilities to trigger the generator to self-destruct, leaving flying parts and smoke in its wake. DHS administrators silently repaired the unidentified susceptibilities; although, arguably just as important, the experiment brought attention to the new age of cyber warfare.[104]

Though certain technological aspects within the power grid SCADA system require adjustments, as indicated in the Aurora Generator Test, transitioning to a more technology-oriented power grid has more advantages than disadvantages. One of the most notable shifts that can be seen in the power sector is it has transitioned to information and communication technologies (ICT). ICT refers to the communications networks that connect all parts of the grid, including "operations, distribution, customers, service providers, and transmission by facilitating communications between humans, between machines, and between machines and humans."[105] ICT applications can comprise "load analysis and automated dispatch software, sensors for remote measuring, grid management systems, demand response software that allows automated load maintenance, smart meters, and chips and controllers for monitoring smart meters."[106] Though the capability to support both mission-critical and non-mission-critical data and operations has significant advantages, to include high operational performance and the capability for future development, the state-of-the-art technologies do not come without vulnerability drawbacks.

Increased cyber-based incidents in the energy-critical infrastructure sector has multiplied signaling an opportune time to address these obstacles and implement new policies. In return, the North American Electric Reliability Corporation (NERC), a non-profit organization, and the National Institute of Standards and Technology (NIST) a physical science laboratory and non-regulatory agency in the U.S. Department of Commerce, promulgate cyber security guidance and enforcement standards. "Through the

[104] "Cyber-attacks Mounting Fast in U.S." CBS, September 30, 2011, https://www.cbsnews.com/news/cyber-attacks-mounting-fast-in-us/.

[105] "Benefits of Information Communications Technology to Energy," Information Technology Industry Council, accessed September 3, 2018, https://www.energy.gov/sites/prod/files/2015/04/f21/DOEQERITIcomments2014.pdf.

[106] Ibid.

Energy Policy Act of 2005, Congress created a hybrid system for setting electrical grid reliability and security standards; NERC and NIST, write power grid standards, while FERC, a government agency, reviews and approves NERC standards."[107] Their mission is to ensure the reliability of the bulk power system in the United States, Canada, and Mexico. Security standards aid utility companies to preserve a robust defense. NERC has a list of strict guidelines for electric companies to abide by which describe how to physically and electronically protect their systems that are intended to keep equipment to safely operate in the nation's bulk electrical grid. These guidelines are better known as Critical Infrastructure Protection compliance.[108] According to TechTarget, "NERC CIP consists of 9 standards and 45 requirements encompassing the security of electronic boundaries and defense of critical cyber assets as well as security management, personnel and training, and disaster recovery planning."[109] NIST have their own separate recommendations associated with organizing and advancement of smart grid standards and guidelines. Since NIST is a non-regulatory government agency, they only develop metrics, technology and standards on a voluntary basis that power grid engineers and executives can consider in their cyber security risk assessments.[110]

A. DEFENSE IN DEPTH SECURITY ARCHITECTURE

When NERC formed in 2006 the viewpoint of critical infrastructure was it must be surrounded by an electronic security perimeter (ESP), bounding the entire critical asset network, physical and electronic, behind a monolithic border.[111] The decade- old

[107] Thomas Popik, "Examining The FERC-NERC Relationship & Setting Grid Reliability Standards," *Our Energy Policy* (blog), July 16, 2014, http://www.ourenergypolicy.org/examining-the-ferc-nerc-relationship-setting-grid-reliability-standards/.

[108] Manimaran Govindarasu and Adam Hahn, "Cybersecurity of the Power Grid: A Growing Challenge," U.S. News and World Report, last modified February 24, 2017, https://www.usnews.com/news/national-news/articles/2017-02-24/cybersecurity-of-the-power-grid-a-growing-challenge.

[109] "What Is NERC CIP (Critical Infrastructure Protection)?" Search Compliance, accessed September 2, 2018, https://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection.

[110] Ibid.

[111] IOActive: Comprehensive Computer Security Services, *A Risk-Based Approach to Determining Electronic Security Perimeters and Critical Cyber Assets* (Seattle, WA, 2009), https://ioactive.com/pdfs/ARisk-basedApproachToDeterminingESPsAndCCAs.pdf.

philosophy is already obsolete. As such, it would be sufficient to protect the business network and the SCADA system within the confines of a single firewall with the expectation no critical assets would be unlawfully accessed.[112] ESP standards is not a one-size-fits-all and the monolithic model allows a single link to be vulnerable, which fosters failure in what has developed into an intricate network. A “defense in depth” approach is a practical solution to secure a network’s critical infrastructure.[113] Belden, an American manufacturer that designs and sells networking products, claims the need for multiple overlapping layers of defense throughout a network is because it mandates the need to have selected access to the tiers of a network. The defense in depth strategy continues to employ an ESP firewall between the business network and SCADA security system. Having additional protection within the control system defends substations in the event the primary firewall is circumvented. The concept is both security measures work in tandem, regularly extending over one another to provide redundancy, allowing a substantial amount of protection against human error or an intentional cyber-attack.[114]

B. DEFENSE IN DEPTH STRATEGY ELEMENTS

Defense in depth is not a single solution, but rather a combination of risk assessments, cyber security and network architecture, employee awareness, and security monitoring, incident planning, and response.[115] Technology gives solutions for problems by giving us the tools to lower risk; nonetheless, the best technology created will never fully prevent human error. ICS are often managed via a SCADA system that provides a graphical user interface for operators to observe the status and manipulate a system.[116] Applying a defense in depth strategy in an ICS setting increases the “cost” to hack

[112] “Defense in Depth Cyber Security for Substation Communications,” Belden, February 10, 2016, https://www.belden.com/blog/industrial-security/defense-in-depth-cyber-security-for-substation-communications.

[113] Ibid.

[114] Ibid.

[115] Graham Williamson, “OT, ICS, SCADA – What’s the Difference?” KuppingerCole, last modified July 7, 2015, https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference.

[116] Ibid.

simultaneously increasing defense and detection abilities from malicious operatives.[117] Decreasing the amount of chances an antagonist is able to successfully maneuver within any given power grid's network or system is the objective. The following are a few of the recommended strategies and solutions that can be used collectively to form layers of defense.

1. Risk Assessments

Operating an electrical company faces risk like any other business and there must be a process in place to properly manage them, so an electrical company is not exposed to threats. Risk assessments are defined as "the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, other organizations, and the nation, resulting from the operation of an information system."[118] Assessing risk mandates institutions recognize and classify their risks and susceptibly to them, the amount of damage these weaknesses can precipitate to an organization, and the probability that a detrimental catastrophe will probably happen.[119] The risks associated with first generation SCADA systems were often overlooked because the systems were strictly isolated at the time, meaning was virtually impossible for an outside entity to penetrate the system. As second and third generation SCADA systems became more distributed and networked, hackers exploited security gaps of control systems linked to the internet.

There are several approaches to risk assessment standards, protocols, and frameworks that administrators can practice within the energy sector. The most prominent of these standards are the NIST 800-82 that recommends established security and vulnerability testing methodologies be incorporated into SCADA/ICS. The other leading

[117] Department of Homeland Security, *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* (September 2016), https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[118] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53 Revision 4 (Gaithersburg, MD: National Institute of Standards and Technology, 2013), https://doi.org/10.6028/NIST.SP.800-53r4.

[119] Ibid.

document is NERC's Vulnerability and Risk Assessment and critical infrastructure protection standards, which are mandated by the Federal Energy Regulatory Commission. Risk assessment is crucial in securing a SCADA/ICS sites against a security intrusion. Regrettably, risk assessment is filled with uncertainty such as the complexity of protocols and the frustration in determining breach repercussions.

2. Cyber Security Network and Security Architecture

Combining once-isolated ICS environments have certainly assisted in making the complex networks into a seamless and more manageable infrastructure. However, connecting the ICS networks and integrating information technology mechanisms with the ICS realm exposes vulnerabilities that electrical companies must address before severe issues arise. Some of the common ICS network architecture flaws are insecure connectivity to internal and external networks, a deficiency of competent understanding of requirements for ICS settings, and using technologies with identified vulnerabilities, generating previously concealed cyber risk in the control domain.[120]

It was challenging to merge modern IT systems into an ICS setting that was previously isolated from an outside network that most likely lacked any security measures. To create a layered defense, IT administrators and operators need to have intimate knowledge of how every single piece of technology functions and how it interconnects within surrounding equipment.[121] Dividing common control architectures into zones can assist a power grid's SCADA architecture to produce distinct boundaries, locations of where multiple layers of defense can be applied. Some of the most common architectural zones that can be applied to an ICS is zone segmentation of a business and ICS systems.[122] Each zone performs together to accomplish the goal of linking the ICS network while securing communication pathways between trusted environments. According to Luciana

[120] "Overview of Cyber Vulnerabilities," Department of Homeland Security, accessed September 3, 2018, https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities.

[121] Luciana Obregon, and Barbara Filkins, "Secure Architecture for Industrial Control Systems," SANS Institute, last modified September 2015, https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327.

[122] Ibid.

Obregon, author of the dissertation "Secure Architecture for Industrial Control Systems," configuring the network's routers, servers, and switches to be segregated via firewalls promotes the principle of least privilege, restricting user access based on their job, therefore producing subnetworks to reduce the surface area an attacker can work in if a layer is compromised.

After an organization such as an electric company completes the construction of a solid network architecture, administrative controls must be implemented at the system, network, physical, and application levels to guarantee information security.[123] These include but are not limited to data security, user security, platform security, application security, policy and security management, and perimeter security.[124] These security architecture components work in unison, superimposing a network architecture and delineates the location of defense in depth measures within a system.

3. Employee Awareness

The largest factor to power grid ICS cyber-attacks are caused by unintentional actions by entry-level staff with basic network access to routinely do their job. Eight-four percent of cyber security intrusions are attributed to human error.[125] Hackers find uninformed employees to be the most promising victims to conduct their targeted infiltrations that threaten normal operations of ICS, which have the potential to result in immense physical damage and disruptions. The most frequent types of cyber-attacks target ICS clients and exposed servers, which social engineering and spear-phishing tactics are taken advantage of because of a high rate user error.[126]

A knowledgeable and attentive workforce does not guarantee industrial assets are fully protected, but it is one of the most inadequate and easily modified element to safeguard industrial assets from cyber-attacks and newly developed security threats.

[123] Ibid.

[124] Ibid.

[125] "Safeguard Your Industrial Assets by Training Your Shop Floor Team in Cybersecurity," Internet of Things, last modified May 25, 2018, https://www.iotforall.com/iiot-cybersecurity-employee-training/.

[126] Ibid.

Despite how far technology advances, a power grid's network will continue to be susceptible if an employee is unable to distinguish a dangerous phishing link from a safe one. Cyber security awareness consequently needs to be elevated to the minimum standard of awareness parallel to compliance, safety, quality, and ethics. This mentality and way of thinking must be completely ingrained within the organizational psyche, reaching as low as an apprentice ready to be hired to as high as senior executives and boardroom members.[127]

Conducting cyber security culture surveys within an organization is one of the most effective and economical components in a layered defense.[128] This approach to information security tailors' employee behavior and ultimately help promote a culture that highlights the importance of having a secure computer network. The survey initially begins with an evaluation of the institutions current security culture. As areas of security concerns are identified, companies can develop a plan of action that balance protecting a company's sensitive data while allowing employees to productively do their job. Tailored training topics that align with concise computer network guidelines with the aim to alter the mindsets and routines of electric utility personnel will lead to organizational change. Cyber security education measurements can be taken periodically to determine which best practices in the workplace culture are effective and to identify any plan of action shortfalls.[129] The cyber security deficiencies can then be addressed to shape the information security culture in a way that best suits the management of an electrical company and its customers.

Training and awareness programs are essential in an ICS security program because it provides staff a clear understanding on the importance of information security and the expected behavior as a company employee to reduce security risks. A keen and well-informed organization is the most valuable line of defense in safeguarding a power grid.

[127] Nadya Bartol, "Ensuring Cybersecurity in the Electric Utility Industry," BCG, last modified August 16, 2017, https://www.bcg.com/en-us/publications/2017/power-utilities-technology-digital-ensuring-cybersecurity-electric-utility-industry.aspx.

[128] Ibid.

[129] Ibid.

Even though security risks triggered because of human error will never be eliminated, raising awareness as well as recognition of ICS security, employees will enhance their comprehension of all the consequences derived from an incident and thus will be more prone to act in accordance with corporate guidelines that curb breaches.

4 Security Monitoring, Incident Planning, and Response

Overseeing a SCADA/ICS network for an irregular activity or signs of a possible attack is tedious and can be overwhelming. In the complex electrical grid environment, monitoring and detection services is an important aspect to defense in depth of defending critical assets. Simply having a border surrounding an ICS does not adequately defend critical assets from breaches. In a defense in depth architecture, a system must not only be able to protect from intrusion, but it must also alert an organization after intrusion so that it can take defensive measures to stop an attempted hack from success. Security monitoring is a universal term and can mean a plethora of different things depending on the sector that is being discussed. NIST SP 800-137 is the standard utility companies follow when applying a continuous security model into their risk management and strategies plan. The primary functions of this special publication are direction on how to establish and implement an effective security monitoring program, and how to analyze and respond to the results.[130]

An all-inclusive incident response plan needs to be a key instrument in any ICS cyber security toolbox. Having an established incident response capability will make the handling of complexity of a computer security incident within the capacity of a trained workforce. NIST SP 800-61, Computer Security Incident Handling Guide, gives cyber security experts instruction on how to evaluate data acquired from a breach and provides recommended follow-on procedures after an incident.[131] Electrical companies are identical

[130] Michael Devitt, “A Brief History of Computer Hacking,” Dynamic Chiropractic, last modified June 18, 2001, https://www.dynamicchiropractic.com/mpacms/dc/article.php?id=18078.

[131] Paul Cichonski, Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, Special Publication 800-61 Revision 2 (Gaithersburg, MD: National Institute of Standards and Technology: U.S. Department of Commerce, 2012), https://doi.org/10.6028/NIST.SP.800-61r2.

to any other business that manage vital data in respect to data security breach liability. State jurisdictions that lack adequate cyber security laws that mandate how vital data and customer information is managed can still result in an electrical company to be held liable for any damages because of a cyber security breach, when the breach was reported, and if any actions were taken to reduce the impact of the breach.

IV. ASSESSING PUBLIC AND PRIVATE SECTOR COLLABORATION

As the United States physical infrastructure advances to digitization, cyber security has to be placed as a priority because of the mounting dangers facing the nation. Since the Reagan presidency when the first presidential directive on computer security was written, the nation has not emphasized cyber security enough as a top priority investment. Hackers attempting to access unauthorized control systems and networks have grown in scope and magnitude. Conversation about cyber security is making its way from talks in the basement to the situation room. It is no longer a subject to be taken lightly.

The public and private energy sector stakeholders must determindely work together to avert cyber threats that have yet to be disovered and bring an end to the ones already known. It is a complex but important situation to create a cyber security structure that takes public and private interests into consideration. For a public and private relationship to be successful, crucial cyber security issues have to be addressed while taking business practices into consideration such as being able to stay competitive in the energy sector, providing an environment where company information is safeguarded but at the same time can be shared as necessary.[132]

In order for cyber security professionals to fulfill their craving of having an advantage over emerging threats, an intelligence database for the entire electrical industries IT professionals to utilize is required. Combating the cyber threat has to change from reactiveness to proactivness. In just a couple of years, U.S. utility companies will spend approximately $7.25 billion on cyber security.[133] Cyber security defense spending will certainly be expensive, but if the boundaries of public and private cooperation are not

[132] Harry Raduege, "The Public/Private Cooperation We Need on Cyber Security," *Harvard Business Review*, last modified June 18, 2013, https://hbr.org/2013/06/the-publicprivate-cooperation.

[133] Constance Douris, "Utilities Will Spend Billions on Cybersecurity as Threat Grows," *Forbes*, last modified September 21, 2017, https://www.forbes.com/sites/constancedouris/2017/09/21/utilities-will-spend-billions-on-cybersecurity-as-threat-grows/.

crossed to pave the path for a reliable and safe national energy critical infrastructure, the estimated cost will drastically increase.

A. EXECUTIVE ORDER 13636

Cyber security cannot just be a problem for Washington or for private corporations to face alone. For the public and private cyber security framework to foster growth and development while providing an appropriate level of protections to the energy infrastructure, a partnership must exist that promotes national cyber security strategies. These partnerships enable the Federal Government and the American public to recognize the importance of thwarting cyber security threats. Equally important in protecting the power grid from cyber-attacks is altering our mindset and archaic approaches. Cyber security executive orders signed by the President of the United States provide a nearly immediate precedent on cyber security compliance objectives.

On February 12, 2013, former President Barack Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," provided all critical infrastructure companies a venue to report cyber threat information, which allows contractors access to a real-time Department of Homeland Security controlled database.[134] The participation by utility companies is on a voluntary basis but does provide quick access to classified cyber threat and technical information to companies that opt in.[135] Private companies are primarily concerned about information sharing as a breach of their privacy and liability to their company. Anything that would ultimately reduce their bottom line is often frowned upon. Though Executive Order 13636 does not completely solve the cyber security problem, it provides additional protection to critical assets in the absence of inclusive cyber security legislation.

[134] Michael Schmidt and Nicole Perlroth, "Executive Order on Cybersecurity is Issued," *New York Times*, last modified February 12, 2013, https://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html.

[135] Executive Order No. 13636, 3 C.F. R. 13636 (2013), https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-13636.

B. PRESIDENTIAL POLICY DIRECTIVE-21 (PPD-21)

The Presidential Policy Directive-21 (PPD-21) was signed by former President Barack Obama the same day Executive Order 13636 was authorized and provides a concise framework for the presidential administration to secure the nation's critical infrastructure.[136] Not to be confused with an executive order, which must be "circulated to a general counsel or similar agency attorney as a matter of circulation accountability," a PPD does not have a Federal Register publication requirement.[137] According to Veronica Chinn, author of Information Sharing with the Private Sector, Executive Order 13636 and PPD-21 both focus on national security as a result of a deliberate cyber-attack, but there are variations in their method to protect against it. The goal of PPD-21 is to detect and stop cyber threats in their tracks, increase defenses, lower the number of susceptibilities, drop the number of cyber-attacks, and improve recovery.

C. EXECUTIVE ORDER 13691

"Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, builds upon the foundation established by Executive Order 13636 by encouraging the development of information sharing and analysis organizations (ISAOs) for cyber security information and collaboration within the private sector and between the private sector and government."[138] ISAOs are seemingly like extensions of ISACs that were implemented years prior to share cyber threat information among the private energy sector. The intent of Executive Order 13691 is to provide facilitation of real-time cyber-information among the Federal government and the participants.

[136] "Presidential Policy Directive - Critical Infrastructure Security and Resilience," The White House, last modified February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[137] Veronica Chinn, Lee Furches, and Barian Woodward, *Information-Sharing with the Private Sector* (National Defense University Press, 2014), http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577502/information-sharing-with-the-private-sector/.

[138] Department of Homeland Security, *Executive Order 13636 and 13691 Privacy and Civil Liberties Assessment Report* (Department of Homeland Security, 2018), https://www.dhs.gov/sites/default/files/publications/2017%20EO%2013636_13691%20Section%205%20Report_Signed%20012618_Final.pdf.

Like Executive Order 13636, information sharing is not required under Executive Order 13691, but rather highly encouraged. Former President Barack Obama declared the cyber threats against the nation's critical infrastructure as a national emergency.[139] The former President also made clear cyber security is inherently a public-private mission because most of the critical infrastructures in the nation are privately owned.[140] Because Executive Order 13691 is not law, it does not provide an inclusive set of tools required to eliminate cyber threats, which would need to come from a bill introduced by Congress.

D. ENHANCE INFORMATION SHARING

Many utility companies in the United States hold the position that not sharing cyber threat information via some of the established outlets is necessary because it allows them to have the upper hand when it becomes necessary to respond to cyber-attacks on the electrical grid system. NERC operates the Electricity Information Sharing and Analysis Center (E-ISAC) whose primary mission is to be the principal organization that electricity providers can securely give and receive cyber threat information.[141] The E-ISAC gathers and analyzes IT data, communicates mitigation tactics with stakeholders, and coordinates incident management with stakeholders within the electricity subsector with government partners, and across independent sectors.[142] Regardless of its significance, all cyber security incidents can be reported to E-ISAC.

Information sharing within the electric industry affiliates enables them to have the resources to determine who and what developing dangers are and allows E-ISAC to give

[139] "Executive Order Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," The White House, last modified December 29, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency.

[140] "Cyber Executive Order Continues the Push for Public-Private Partnerships," Crowell Moring, February 20, 2015, https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Cyber-Executive-Order-Continues-the-Push-for-Public-Private-Partnerships.

[141] "ES-ISAC Is Now E-ISAC," Curricula, last modified November 18, 2015, https://www.getcurricula.com/es-isac-now-e-isac/.

[142] Ibid.

electricity representatives advanced notice of a possible network infiltration.[143] When organizations share more and more information with E-ISAC, the data is compiled, analyzed, and distributed so that electrical organizations are able to make well-informed and educated decisions to lower cyber and physical risks on their systems. It is just as important for those working in the cyber and physical security realm in the electric industry to have precise and real-time information brought by information sharing via E-ISAC tools as it is for those who operate the SCADA systems to have real-time data on their networked data communications and graphical user interfaces, so they can also respond to system complications accordingly. The following are additional key benefits of information sharing besides the ability to compile information and provide analysis results for E-ISAC members:

- Provides an environment for malware analysis where it can be reverse engineered to improve their understanding on how to counter an attack.
- Strategic data is shared throughout the electrical sector, which in turn can create mitigating actions to prevent potential threats to perform malicious activities as well as lowering an organization's cyber risk.
- Information is shared with the other 19 members of the National Council of ISACs that help infrastructure owners and operators within the 16 critical infrastructure sectors protect their physical assets, workers, and clients from cyber and physical dangers.[144] With this, information can be shared with other critical infrastructure sectors to identify similar threat campaign tactics, techniques, and procedures.

Electrical companies are straining to keep up with cyber threats that are outperforming their stove-piped cyber security defenses. Sharing information about cyber threats among trusted electricity stakeholders with the federal, state, and local governments

[143] "Understanding Your E-ISAC," NERC, accessed August 25, 2018, https://www.nerc.com/pa/CI/ESISAC/Documents/Understanding%20Your%20E-ISAC_June%2028%202016_FINAL.PDF.

[144] "National Council of ISACs," National Council of ISACs, accessed August 25, 2018, https://www.nationalisacs.org/about-isacs.

can shift the tide from a highly defensive posture to a vastly offensive position. Rather than fixing the damage conducted after a cyber-attack, a central information-sharing system will allow cyber analysis and developers to get ahead of the threat by piecing together a cyber threats intention and determine the tools they will likely use in their attack.

Measures to improve security and resilience rely on timely and effective information sharing throughout the entire energy sector. The United States has the potential to effectively share cyber security information with the federal government and the entire private electrical industry and its partners alike. These energy sector partnerships have the organizational capacity and fortitude to develop a framework that establishes expected roles of each entity and how they are tasked to accomplish it[145]

E. BI-DIRECTIONAL INFORMATION SHARING

The energy sector's public divisions are unable to undertake the burden of financing and managing increasing energy demands alone; however, through the engagement of public-private partnerships (PPPs), each division can benefit through common interests of provisioning energy. Giving private companies the option to participate in PPPs allows both parties to share the benefits and responsibilities from these long-term contracts. The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-founded by the Department of Energy and managed by NERC's E-ISAC, the electrical industries' leading cyberthreat sharing group.[146] Through this collaboration, energy sector participants have access to a database that allows input and output of classified and unclassified threat data, a panoramic view of the nation's grid security. The Department of Energy's intelligence community facilitates data analysis that will ultimately boost a company's cyber-defense capabilities in that they are able to develop better hardware and software to recognize and protect against their electrical systems.

[145] "National Electric Grid Action Plan," The White House, accessed August 24, 2018, https://www.whitehouse.gov/sites/whitehouse.gov/files/images/National_Electric_Grid_Action_Plan_06Dec2016.pdf.

[146] "Energy Sector Cybersecurity Preparedness," Department of Energy," accessed September 4, 2018, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity.

The goal is to have all electric companies trust to use the CRISP technology; however, until the Federal Government finds a solution to subsidize the costs to run the program that will allow thousands of smaller electric companies to participate, about one quarter of the country will remain at a greater risk to cyber threats than the rest.[147] According to Peter Behr, an E&E News reporter, the larger corporate-sized U.S. electrical companies do not face any complications using the cyber threat information CRISP database because they have the budget and technical skills to take advantage of the program. The smaller municipal electric companies that are not participating in CRISP are not optimal targets for cyber-hackers nor pose a national threat if they were. However, if hackers were to successfully infiltrate even a rural town's power plant that caused electrical disruptions to its small population, it would be a bitter loss for U.S. cyber-defense and would be exacerbated if there was physical damage.

CRISP, like any other information sharing initiative, can pose more risks than rewards to private corporations. Private companies have had concerns that the E-ISAC shares cyber-intelligence information with its parent association, NERC. If an electrical company fails a baseline cyber security audit that NERC's cyber security enforcement department conducted, it can put doubt into how the sensitive information is being used.[148] This fear or doubt may prevent utility companies from submitting their cyber security vulnerabilities to E-ISAC because it may come back to bite them later. Even though E-ISAC cannot force utility companies to voluntarily divulge cyber security threat data, FERC and NERC have the capability to mandate it. This, however poses, the problem that utility companies may have less desire and motivation to find these threats.

There must be a drive for companies to want to participate in programs like CRISP. It is not likely that all companies will voluntarily engage in information sharing even if it is valuable to its industry partners. Aside from the high costs associated with participating in CRISP, industry and government partners need to incentivize the program so that even

[147] Peter Behr. "DOE Seeks to Offer Cyberthreat-Sharing Defenses to Small Utilities," E&E News, last modified July 6, 2016, https://www.eenews.net/stories/1060039828.

[148] Blake Sobczak, "Grid Monitor Gambles on More Utility Information-Sharing," E&E News, February 7, 2018, https://www.eenews.net/stories/1060073087.

the small electric companies have interest in joining. Even the small guys want to ensure that they are getting something valuable in return for the information they share with E-ISAC. There is certainly demand for cyber threat information by cyber security experts; however, the daunting task to find a practical solution that will balance costs and benefits may hinder forward progress. To expand CRISP's membership base, E-ISAC must focus on the outliers—the companies not participating—and demonstrate to them the utility, quality, and impact of cyber security information sharing on a company's overall security posture.[149] Additionally, E-ISAC must be able to alleviate collaborative barriers that deter utility companies from joining. Examples are technological barriers, a lack in interoperability/compatibility among sharing organizations and firms as well as legal barriers that relate to companies thinking of legal repercussions from the release of personal identifiable information (PII).[150] The goal is to double the number of CRISP participants by the start of fiscal year 2021.

F. SUMMARY

There is a paradigm of having too much or too little information sharing within the public and private sector. Not all private corporations find it necessary to share information and are more inclined to restrict them, especially after headlined events like WikiLeaks, wherein U.S. Army Private First-Class Manning publicly released thousands of intelligence reports, or the abundant number of U.S. Hospital Health Insurance Portability and Accountability Act (HIPPA) data breaches. While it is certainly necessary to safeguard sensitive information, the solution is not to isolate information that can contribute to the energy industries' cyber security. Any breach in sensitive information cannot ever be taken lightly; therefore, these occasions are reasons to enhance policies and procedures related to the access and flow of information. Private corporations that choose to not participate in cyber security programs established under Presidential Executive Orders 13636 and 13691

[149] Priscilla Koepke, "Cybersecurity Information Sharing Incentives and Barriers" (working paper, MIT Management Sloan School, 2017), 39, http://web.mit.edu/smadnick/www/wp/2017-13.pdf.

[150] Ibid.

are hindering the dependency national security has on information sharing and those who rely on those contributions to protect the energy sector.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SAFEGUARDS AND MITIGATION

Gas, water, and food supplies can be stockpiled in mass quantities; Although, that is not the case with energy. As energy is produced, it is immediately consumed, which makes for a tedious and meticulous balancing act because supply and demand is continually fluctuating. Electricity management in North America is a 24-hour-a-day operation that guarantees a consistent and dependable energy source supplying electricity to residential houses and companies. The complex electrical grid from generation, transmission, and distribution involves close collaboration between a multitude of North American energy organizations.[151]

To be considered the largest interconnected machine on Earth, the United States' electrical grid consists of more than 200,000 miles of high-voltage transmission lines, 5.5 million miles of local distributed lines, millions more of digital controls, and thousands of energy-generating plants.[152] The electricity grid is the most complex machine, composed of national power plants and regional facilities, moved across a network of substations, and transmission lines used to transport the energy to consumers across the country.[153]

To date, there have been no known successful attacks to cause a blackout in North America; nonetheless, utility companies are constantly warding off thousands of attempts monthly. Jon Wellinghoff, an electrical grid expert and former Federal Energy Regulatory Commission chair, believes that physical security should take a higher precedence than cyber-attacks.[154] On the other hand, multiple utility executives believe the grid industry

[151] North American Reliability Corporation, *High-Impact Low-Frequency Event Risk to the North American Bulk Power System* (North American Reliability Corporation, June 2010), https://www.energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

[152] Weeks, Jennifer, "U.S. Electrical Grid Undergoes Massive Transition to Connect to Renewables - Scientific American," Scientific American, last modified April 28, 2010, https://www.scientificamerican.com/article/what-is-the-smart-grid/.

[153] "U.S. Electricity Grid & Markets," Overviews and Factsheets, United States Environmental Protection Agency, August 30, 2017, https://www.epa.gov/greenpower/us-electricity-grid-markets.

[154] Plumer, Brad, "It's Way Too Easy to Cause a Massive Blackout in the U.S.," Vox, last modified April 4, 2014, https://www.vox.com/2014/4/14/5604992/us-power-grid-vulnerability.

must match the amount of money spent on cyber security defenses as is spent on natural disasters.[155] Although grid cyber-attacks by single individuals, terrorists, and criminal organizations are not off the table, the chief threat that would require advanced skills and resources to cause considerably disastrous service interruption to the public population are state adversaries. The following discussed vulnerabilities are just some of the areas a mediocre hacker can exploit let alone a nation state actor with a cyber army aligned to the aims of their government.[156]

A. ELECTRICAL GRID–SPECIFIC AREAS OF VULNERABILITY

The United States electrical grid has had credible cyber-attack threats for at least two decades. It would not be impossible to effectively interrupt normal operations, but it would certainly be challenging because the grid has been built to be resilient, safe, and reliable.[157] The National Security Telecommunications Advisory Committee (NSTAC) categorizes the top three most susceptible areas to cyber threats within an electrical grid to be its control center, substation and communication infrastructure.[158]

1. Control Center

Inside a power grid’s control room is where power in its designated region is disbursed as well as where the mainframe is located that allows operators to observe grid stability. Modern power distribution control centers in the United States regulate daily services of the distribution network to provide continuous power supplies to the end

[155] Ibid.

[156] “The Nation State Actor,” BAE Systems, accessed September 3, 2018, https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor.

[157] Shelby Lin Erdman, “How Vulnerable Is the U.S. Power Grid to a Cyberattack? 5 Things to Know,” AJC, last modified March 19, 2018, https://www.ajc.com/news/national/how-vulnerable-the-power-grid-cyberattack-things-know/YujzcltJ5wB2z8zJHyzPvI/.

[158] Sans Institute, “Can Hackers Turn Your Lights Off? The Vulnerability of the U.S. Power Grid to Electronic Attack,” (Institute InfoSec Reading Room, SANS Institute, 2001), https://www.sans.org/reading-room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack-606.

customers. A distribution operator manning a multiple monitor console can maintain control of the grid through fault, outage, and dynamic load management.[159]

Part of the electrical grid hackers have most potential to gain administrative access to is located within its corporate management information system (MIS). These computerized records contain financial data, information systems applications, customer, and employee data that can be accessed at entry levels of management. Connecting an MIS to an energy management system (EMS), commonly referred to as SCADA, is particularly dangerous to network security because it can provide a portal into central operations of an electrical plant. EMS has an indispensable role in electric power systems control centers, because of their real-time SCADA applications that provide supervisory control and data acquisition including load shedding, data links, and control sequences.[160] EMS can also provide dispatch and control and energy scheduling and accounting. EMS permits electric companies to improve their operation and maintenance of their transmission and sub-transmission networks. However, it also has its shortcomings in that it is not a closed-loop system; it can connect to the internet or may connect to another utility whose LAN is connected to the internet, giving hackers an opportunity to venture into restricted space. Additionally, another danger can stem from a utility company's remote administration and maintenance ports, that allow employees to login so that they may perform day-to-day administrative duties and/or remotely troubleshoot any issues.[161] Not all EMS systems have advanced token-based authentication systems, leaving access to the dial-in administrative ports without this technology susceptible to malicious activity.

[159] Jennifer Weeks, "U.S. Electrical Grid Undergoes Massive Transition to Connect to Renewables - Scientific American," Scientific American, last modified April 28, 2010, https://www.scientificamerican.com/article/what-is-the-smart-grid/.

[160] Sans Institute, "Can Hackers Turn Your Lights Off? The Vulnerability of the U.S. Power Grid to Electronic Attack" (Institute InfoSec Reading Room, SANS Institute, 2001), https://www.sans.org/reading-room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack-606.

[161] Ibid.

2. Substations

Substations, also known as terminal stations, integrate portions of the distribution and long-distance and short-distance electrical transmission systems. To minimize attenuation when electricity travels long distances, voltage is increased. Substations in turn will step down the electrical voltage so that it can be distributed to the consumer.[162] Likewise, substations perform the step-up in voltage when electricity is travelling in the opposite direction.[163] Additionally, these high-voltage electric system facilities have the capability to move equipment, circuits/lines, and generators in and out of an electrical system. There are a variety of electrical substations based on their application, voltage grade, and by the physical make-up of the structure. Generally, substations will have these aggregate functions:

- Provide measurement readings of electricity that is distributed to various termination points
- Regulate voltage fluctuations and distribute electricity to end users
- Change voltage level for transmission and distribution facilities referred to as step-up and step-down
- Switching points where circuits can be isolated for maintenance
- Reduce the number of electrical surges to the electrical grid and act as a lightning arrester
- Protect vital equipment in the distribution system from short-and high-circuit currents with the use of circuit breakers and fuses
- Linking structure between one or more utility companies

[162] “Electrical Substations,” Power Lines Inc., last modified July 2, 2014, http://powerlinesinc.com/electrical-substations/.

[163] Ibid.

- Load shed by reducing the electrical demand of equipment in parts of the distribution system to prevent entire system failure[164]

a. Remote Terminal Units

Substations are typically unmanned and are controlled using remote terminal units (RTU) and controllers for substation and power system automation, which are integrated into SCADA and energy management systems. An RTU is a microprocessor-controlled electronic device that links physical equipment such as a transformer or a breaker to a SCADA system. The RTUs and an assortment of other smart digitally programmable equipment such as programmable logic controllers (PLC) leave substations susceptible to hacking.

RTUs, a serial-based piece of equipment, run on DNP3, which refers to "Distributed Network Protocol 3.0," a communications protocol used to enhance administrative functions and information transmittal explicitly used in SCADA applications.[165] It is the second most widely used protocol in SCADA/ICS systems within the electric utility sector because it works reliably over varied and low-quality media, it is resistant to EMI-induced distortion, and it is able to combine 65,000 devices in a single link.[166] DNP3, however, was developed by Westronic Systems in 1993 when security was not the primary interest when developing computer protocols.[167]

One of the traditional methods to exploit against DNP3 are DoS attacks, in which a targeted system's bandwidth is overwhelmed with digital traffic, tying up valuable resources, preventing legitimate users from accessing a system with the intent of ultimately crashing the targeted computer or network.[168] Man-in-the-middle attacks (MITM) via the

[164] "Electric Power E-Tool: Illustrated Glossary: Substations," Department of Labor, accessed September 3, 2018, https://www.osha.gov/SLTC/etools/electric_power/illustrated_glossary/substation.html.

[165] Paul Smart, "Getting to Know DNP3," Campbell Scientific, last modified January 20, 2016, https://www.campbellsci.com/blog/getting-to-know-dnp3.

[166] "SCADA Hacking: SCADA Protocols (DNP3)," Hackers Arise, last modified February 10, 2015, https://www.hackers-arise.com/single-post/2017/02/10/SCADA-Hacking-SCADA-Prortocols-DNP3.

[167] Ibid.

[168] Ibid.

DNP3 protocol can be used to inject false commands and responses within an RTU. This type of cyber-attack allows a malicious actor to impersonate communicating computer systems into thinking they are speaking to a legitimate node. Rather, the attacker can manipulate or even steal data between two communicating hosts and the theft may not be noticed until it is too late.[169]

3. Communications Infrastructure

The final segment where a multitude of security vulnerabilities persist is in the communications infrastructure, the part of the grid where control systems connect and exchange data. As the nation moves into having a fully automated smart grid, the communication infrastructure that controls signal and provides measurements and readings is supposed to be reliable and efficient.

Communication technology is certainly an indispensable component for future smart grids; although, there are numerous hurdles the United States must face to have a highly defensed, robust, and operational effective smart grid network. The energy sector's communication infrastructure, now commonly known as the smart grid, is composed of a complex network of networks, integrating both power and communications infrastructures. Communication networks in a power grid provide it with the necessary infrastructure that allows a utility company to manage all their equipment from a central location. The smart grid is a massive system that incorporates a multitude of communication and networking technologies to use with its applications. Some of the methods of communication are transmitted through copper cable, power line carrier, fiber optic cables, and wireless communications to include microwave, satellite, and cellular.[170] Power plants and substations that operate traditional transmission systems opt for wired sensor technologies because they generally maintain a higher level of security and reliability over wireless communication. However, due to the high cost associated with wired communication

[169] "Man in the Middle Attack: Tutorial & Examples," Veracode, accessed September 3, 2018, https://www.veracode.com/security/man-middle-attack.

[170] Ataul Bari, "Challenges in the Smart Grid Applications: An Overview," *International Journal of Distributed Sensor Networks* 10, no. 2 (February 20, 2014), https://doi.org/10.1155/2014/974682.

system installation and maintenance costs, the expense from an economic standpoint is a motivation utility companies elect to install wireless networks.

a. Multi-hopping Networks

The drawback of wireless communications is their limited range. To overcome this, intelligent communication systems such as SCADA can utilize multi-hop routing, in which a coverage area is larger than a node can transmit data, so the system uses nodes between itself and the destination as relays. Compared to wired networks, multi-hop networks can seamlessly extend range to remote areas without having to deploy cables and can enable faster data rates and higher output. Despite these benefits, multi-hop networks expose themselves to more cyber-attack risks because data is required to be transmitted on a hop-by-hop basis.[171] Every node in a multi-hop mesh network fundamentally acts as a router and therefore makes it another site for a potential cyber-attack.

Multi-hopping networks, if not administered properly, are susceptible to black and gray wormholes in which a hacker disturbs a networks data routing path. If a node/computer falls victim to malicious code, it can impersonate a trusted computer, and alter and/or disrupt data that moves through a network. In a gray wormhole attack, an attacker will filter what information can flow through the network. A single node or a collective set of nodes will selectively drop data packets.[172] In contrast a blackhole attack is when an attacker uses the shortest path attraction to attract traffic, which will subsequently drop all the packets of data sent to the infected node.[173] Wormhole attacks are relentless in that they can be simple to initiate although problematic to detect.

[171] Thelma Allen, “Smart Grid Wireless Network Security,” NIST, last modified April 12, 2018, https://www.nist.gov/programs-projects/smart-grid-wireless-network-security.

[172] Rupali Sharma, “Gray-Hole Attack in Mobile Ad-Hoc Networks: A Survey,” International Journal of Distributed Sensor Networks (2016): 4, http://ijcsit.com/docs/Volume%207/vol7issue3/ijcsit2016070389.pdf.

[173] G. S Jackson, “Security Issues in Wireless Mesh Networks,” Chron, accessed September 3, 2018, https://smallbusiness.chron.com/security-issues-wireless-mesh-networks-46553.html.

b. Wireless Sensor Networks

Technology that is introduced into smart grids generally have the intention to advance its dependability and effectiveness but may simultaneously expose the smart grid to vulnerabilities if the newly developed service is installed without focusing on current and relevant security risks. Wireless sensor networks (WSN) have revolutionized the electrical power grid by incorporating cost-saving multifunctional sensors that accurately communicate atmospheric and physical environment data to control centers so that operators can make informed decisions. According to Piyush Ghune with the Malwa Institute of Technology, "harsh and complex electric-power-system environments pose great challenges in the reliability of WSN communications in smart-grid applications," reasons that prevent its extensive placement into an electrical grid. [174] WSNs communicate on unlicensed industrial, scientific, and medical (ISM) radio frequency (RF) bands, which means they are shared in environments making sensor nodes susceptible to jamming attacks and eavesdropping. Jamming attacks are the most common type of attacks that jeopardize the integrity of WSNs. Radio jamming is the broadcast of a signal to one or more radio frequencies to stop radio communication, ultimately rendering equipment intended for monitoring, controlling, measuring, and fault diagnosis at various domains of a smart grid network useless.[175]

"Defending WSN networks can be a complex undertaking due to the commodity nature of wireless technologies and an increasingly sophisticated user base means that adversaries are able to easily gain access to communications between sensor devices by purchasing their own device and running it in a monitor mode."[176] Unlike conventional DoS attacks as in Distributed Network Protocols 3.0 in remote terminal units in which a machine or network resource is flooded with superfluous requests to overload it, a jamming

[174] Piyush Ghune, "Application of Wireless Sensor Networks in Smart Grid - Opportunities, Challenges & Technologies Available," IEEE Network, accessed September 1, 2018, https://pdfs.semanticscholar.org/9465/91f50e41243930861c043df6566bfcf891ca.pdf

[175] "Radio Jamming," SESP Group, accessed September 3, 2018, http://www.sesp.com/radio-jammers.asp.

[176] Wenyuan Xu, "Jamming Sensor Networks: Attack and Defense Strategies," IEEE Network 20, no. 3 (May 2006): 41–47, https://doi.org/10.1109/MNET.2006.1637931.

attack takes advantage of using the same frequency used in smart grid equipment so that it will stop communicating within its network.

B. A PATH FORWARD

Smart grids have become the electric industry's power grid standard of operation in the United States but not without a cost. Though the smart grid brings in a new era of reliability and efficiency with automation and high-tech digital sensors and operational controls that respond to electric demand, they inherently have their own risks. The responsibility for heading the way to modernize the nation's electrical grid is the Office of Electricity (OE), a branch of the U.S. Department of Energy.[177] OE oversees making sure the nation's power grid system is secure, resilient, reliable, and ready for future use with micro-grids and electric vehicles.

To address the lacking security measures in the control center, substation, and communication systems, OE should setup a comprehensive advanced grid research and development support activity with the collaboration of state and logical agencies. The activity should prioritize smart grid modernization. The program would have the purpose of building a reliable energy infrastructure that will be able to integrate the needs of the future. Grid modernization will ideally improve the physical framework of the electrical grid with new attributes, such as incorporating solar panels that have two-way directional flow of energy to and from an electrical grid. Through a grid modernization initiative, areas of vulnerability will be addressed as well.

[177] "DOE's Office of Electricity Delivery and Energy Reliability (OE): A Primer, with Appropriations for FY2017," EveryCRSReport, last modified December 13, 2016, https://www.everycrsreport.com/reports/R44357.html.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND POLICY RECOMMENDATIONS

The rapid change in technology combined with increasing demand for power continues to be a challenge for cyber security experts. The electrical grid since its inception has always been susceptible to physical threats. Cyber security experts are just now realizing the seriousness of the threat lurking in the digital world within the internet-dependent power grid. Through case studies and research of this thesis, some of the most common power grid vulnerabilities and ways to exploit them painted a picture of reality—a reality that is only a short reach away with the wrong intention.

A. POLICY RECOMMENDATIONS

The primary function of this thesis is to investigate and provide recommendations for enhanced cyber security of the U.S. power grid infrastructure. Key policy and procedural components require further development to better identify, analyze, and evaluate cyber risks, emphasized by the Russian attacks on Ukraine and western power grids. The three fundamental cyber security elements that require reinforcement to improve cyber security for critical energy infrastructure were identified as: security system robustness, joint public and private collaboration, and options to mitigate risk.

The following are the policy recommendations that stem from the fundamental cyber security elements. First, today's smart grid SCADA systems must use a defense in depth approach consisting of a layered defense model that allows the failure of a single security measure and allows data to continually be protected with additional security mechanisms. The systems and controls that make up the defense in depth architecture will work in harmony to maintain a robust architecture but can be adjusted to fight developing cyber security threats. Reliable service has always been a priority in the electrical business, but as cyber threats evolve, the systems and defense architecture that manage our electricity must also evolve so the same reliable service is maintained. The defense in depth architecture must center on deterrence, resiliency, and restoration.[178]

Next, the federal government must fund programs that increase incentives and decrease barriers as they relate to cyber threat information sharing. The paths for information sharing have existed for several years now. The Department of Homeland Security has developed many information sharing programs. One of the DHS flagship information sharing programs is the Cyber Information Sharing and Collaboration Program (CISCP). This public and private information sharing network allows companies to provide other companies with any cyber threat, incident, and vulnerability information they face, and provides a collaborative environment where analysts can learn from each other's cyber threats. There are six other information sharing programs like CICSP that are overshadowed by DHS, including CRISP run by E-ISAC. Ultimately, all these voluntary programs have similar agendas, -to create partnerships and to have a means to share valuable information companies can act on.

Information is certainly flowing within the information sharing programs, but they are not at the elevated levels of private-sector participation—a blow to the Cybersecurity Act of 2015. This was legislation signed by former President Obama to establish a means for the federal government and the private-sector to share information while having certain legal protections. It seems like companies are eager to receive information but very few take the additional steps to give any back. The government does not make it easy to get into any information sharing program. To receive information from DHS's automated indicator sharing program, companies must install unique technology, consent to data security agreements, and go through a clearance process.[179]

Lastly, advanced grid research and development that focuses on grid modernization will prepare the nation for the needs of the 21st century and beyond. Modernizing an

[178] John Di Stasio, "The Value of Defense in Depth: Cybersecurity of the Electrical grid." *Morning Consult* (blog), April 6, 2017, https://morningconsult.com/opinions/value-defense-depth-cybersecurity-electric-grid/.

[179] Shaun Waterman, "Experts Say Government's Information Sharing Program Is All Take and No Give." *Cyberscoop* (blog), November 15, 2017, https://www.cyberscoop.com/dhs-ais-program-house-homeland-committee/.

electrical grid for the future is no simple task. To develop new transformational energy technologies to mitigate current and unforeseen risks will require assistance from multiple government agencies, private corporations, and even the energy customers.

B. OTHER RESEARCH OPPORTUNITIES

This examination of cyber security in the electrical grid represents a small cross-section of the 15 other critical infrastructure sectors identified in the Presidential Policy Directive 21 (PPD-21). Furthermore, this study only provides a glimpse of recognized deficiencies in the physical and cyber security domain within the energy infrastructure. Furthermore, examining additional case studies might expose trends that cause cyber deterrence to succeed or fail in its implementation.

Exploring the cyber security defense practices of alternate countries with well-established critical infrastructures can possibly assist with molding a more effective policy to defend the United States. Besides a country’s technological capacity, other factors play a vital role in promoting cyber security awareness to include pertinent political legislation, economic strength, foreign policy, and building capacity. These represent vital aspects that will allow any government the ability to provide necessary protection against cyber-attack for all its electrical grid security participants. Researching alternative approaches to cyber security resilience in China, a country with a massive electrical grid infrastructure, could present practical alternatives for U.S. energy system resiliency, or at least promote new innovations

Most of this study focused on cyber-attacks and cyber threats within the digital realm. However, protecting the power grid is a tactic that expands beyond the Internet of Things (IoT), defined as the concept of systems interconnected with sensors, computers, software, sensors, and practically anything electronic via the internet to move information around. Cyber security is certainly a topic that cannot be ignored, but as more focus is put on it, defense specialists cannot overlook the importance of physical security and what can be done to ensure its resiliency. The protection of physical equipment and structures in an asset-intensive industry tends to be ignored in organizations that are heavily reliant on technology. As previously suggested in this thesis, electric facilities are choke points because they provide an enabling function for all other critical infrastructure sectors.[180] The threats are out there, and they have successfully attacked critical infrastructures. But the question is, how much is being done to protect the power grids' physical perimeter?

Since September 11, 2001, the thought of how to physically protect U.S. critical infrastructures and key assets has drastically changed. Words like "homeland," "terrorist," "ISIS," and "jihad" have inundated our vocabulary; it has become common to substitute the word "if" with "when" to describe the next occurrence of a terrorist attack. The truth is, physical security threats to critical infrastructure, including the power grid, have not changed much since the 9/11 attacks, but there is now heightened awareness of its reality. The comprehensive definition of physical security is to design a robust system and its facilities to deter or mitigate the risk of an attack and be resilient if one were to happen.[181] In 2013, while the electrical industry had their focus on cyber threats, Pacific Gas and Electric's Metcalf substation in Coyote, California was attacked by a well-orchestrated team of snipers that damaged 17 transformers.[182] Even though several areas of the Silicon Valley, the world's leading hub for technology, avoided losing power, the nation's top electrical utility regulator referred to this incident as "the most significant incident of domestic terrorism involving the grid that has ever occurred."[183] Very little of the American public was made aware of this incident because most of the headlines were overwhelmed by the Boston Marathon terrorist bombings that occurred one day prior, while the Metcalf attack did not meet the FBI's requirements to be considered a deliberate

[180] Ralph Cicerone, *Terrorism and the Electric Power Delivery System* (Washington, DC: The National Press Academies, 2012), 156, https://doi.org/10.17226/12050.

[181] G. D. S. Associates. "Physical Security Threats and the U.S. Power Grid." GDS Associates, Inc. Engineers & Consultants, January 19, 2016, https://www.gdsassociates.com/physical-security-threats-u-s-power-grid/.

[182] David Baker, "FBI: Attack on PG&E South Bay Substation Wasn't Terrorism," SFGate, September 11, 2014, https://www.sfgate.com/business/article/FBI-Attack-on-PG-amp-E-substation-in-13-wasn-t-5746785.php.

[183] Jose Pagliery, "Sniper Attack on California Power Grid May Have Been 'An Insider,' DHS Says," CNNMoney, last modified October 17, 2015, https://money.cnn.com/2015/10/16/technology/sniper-power-grid/index.html.

terrorist act.[184] Although this incident did not result in the aftermath of the 2003 Northeast blackout, the widespread power outage that affected large populations in the United States Midwest, Northeast, and parts of Canada, it is a stark reminder of some of the broader physical security problems the U.S. energy sector has yet to identify.

[184] Carl Vinson, Jerry Haldenstein, William Coston, Lynn Fisher, and Sofia Delgado Persuquia. "Review of Physical Security Protection of Utility Substations and Control Centers," The Florida Public Service Commission Office of Auditing and Performance Analysis, last modified December 2014, http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Physical_Security_2014.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allen, Thelma. "Smart Grid Wireless Network Security." NIST. Last modified August 16, 2016. https://www.nist.gov/programs-projects/smart-grid-wireless-network-security.

Automation. "SCADA/Business Network Separation: Securing an Integrated SCADA System." Accessed September 3, 2018. https://www.automation.com/library/articles-white-papers/hmi-and-scada-software-technologies/scadabusiness-network-separation-securing-an-integrated-scada-system.

BAE Systems. "The Nation State Actor." Accessed September 3, 2018. https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor.

Baker, David. "FBI: Attack on PG&E South Bay Substation Wasn't Terrorism." SFGate, Last modified September 11, 2014. https://www.sfgate.com/business/article/FBI-Attack-on-PG-amp-E-substation-in-13-wasn-t-5746785.php.

Bar, Ataul, Jin Jiang, and Walid Saad. "Challenges in the Smart Grid Applications: An Overview." *International Journal of Distributed Sensor Networks* 10, no. 2 (February 2014). http://journals.sagepub.com/doi/10.1155/2014/974682.

Bartol, Nadya, Michael Coden, David Gee, and Craig Lawton. "Ensuring Cybersecurity in the Electric Utility Industry." BCG. Last modified August 16, 2017. https://www.bcg.com/en-us/publications/2017/power-utilities-technology-digital-ensuring-cybersecurity-electric-utility-industry.aspx.

Behr, Peter, and Blake Sobczak. "SECURITY: Utilities Look Back to the Future for Hands-on Cyberdefense." E&E News. Last modified July 21, 2016. https://www.eenews.net/stories/1060040590.

Behr, Peter. "DOE Seeks to Offer Cyberthreat-Sharing Defenses to Small Utilities." E&E News, Last modified July 6, 2016. https://www.eenews.net/stories/1060039828.

Belden. "Defense in Depth Cyber Security for Substation Communications." February 10, 2016. https://www.belden.com/blog/industrial-security/defense-in-depth-cyber security-for-substation-communications.

Bellis, Mary. "So... What Is Electricity?" ThoughtCo. Last modified February 28, 2018. https://www.thoughtco.com/what-is-electricity-4019643.

Berger, Marco. "Cybersecurity and the Power Grid: Preparing for the Future." Transmission & Distribution World. Last modified November 27, 2017. https://www.tdworld.com/smart-grid/cybersecurity-and-power-grid-preparing-future.

BEST. “United States Utility Company List by State.” Accessed September 2, 2018. http://www.bestenergynews.com/solar/utility_co/utility_companies.php.

Bird, Sean, Earl Carter, Erick Galinkin, Christopher Marczewski, and Joe Marshall. “Attack on Critical Infrastructure Leverages Template Injection.” *TALOS Intelligence* (blog), July 7, 2017. http://blog.talosintelligence.com/2017/07/template-injection.html.

Brewster, Thomas. “NotPetya Ransomware Hackers ‘Took Down Ukraine Power Grid.’” *Forbes*, July 3, 2017. https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/#788e7bec6b89.

Carbon Brief. “How Energy Companies Make Profit: A Closer Look at the Data.” November 11, 2013. https://www.carbonbrief.org/how-energy-companies-make-profit-a-closer-look-at-the-data.

CBS. “Cyber-attacks Mounting Fast in U.S.” September 30, 2011. https://www.cbsnews.com/news/cyber-attacks-mounting-fast-in-us/.

Chakrabortty, Aranya, and Alex Huang. “*Digital Grid: Transforming the Electric Power Grid into an Innovation Engine for the United States*.” arXiv:1705.01925. NC: North Carolina State University, 2017. http://arxiv.org/abs/1705.01925.

Chiappetta, Marco. “Hackers Brought Down Ukrainian Power Grid in December, Homeland Security ICS-CERT Confirms.” *Forbes*. Last modified February 27, 2016. https://www.forbes.com/sites/marcochiappetta/2016/02/27/hackers-brought-down-ukrainian-power-grid-in-december-homeland-security-ics-cert-confirms/.

Chinn, Veronica, Lee Furches, and Barian Woodward. “Information-Sharing with the Private Sector.” National Defense University Press. Last modified April 1, 2014. http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577502/information-sharing-with-the-private-sector/.

Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. “Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology.” National Institute of Standards and Technology. Last modified August 2012. https://doi.org/10.6028/NIST.SP.800-61r2.

CNN. “FEMA Preparing for Y2K Disaster.” February 24, 1999. http://www.cnn.com/TECH/computing/9902/23/fema.y2k/.

Constantin, Lucian. “Cyberespionage Group Might Be Planning Electrical Grid Attacks.” Forbes. Last modified September 6, 2017. https://www.forbes.com/sites/lconstantin/2017/09/06/cyberespionage-group-might-be-planning-electrical-grid-attacks/#7b0c54856701.

Coresman, Anthony, and Justin Cordesman. *Cyber Threats*. Santa Barbara, CA: Praeger, 2001. ABC-CLIO.

Crowell Moring. “Cyber Executive Order Continues the Push for Public-Private Partnerships.” February 20, 2015. https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Cyber-Executive-Order-Continues-the-Push-for-Public-Private-Partnerships.

CSRC. “Industrial Control System.” Accessed September 2, 2018. https://csrc.nist.gov/Glossary/?term=4752.

Curricula. “ES-ISAC Is Now E-ISAC.” November 18, 2015. https://www.getcurricula.com/es-isac-now-e-isac/.

Cytek. “Consulting for Critical Infrastructure.” Accessed September 1, 2018. https://www.cytek.com/consulting-for-critical-infrastructure/.

Department of Energy. “Electricity 101.” Accessed September 2, 2018. https://www.energy.gov/oe/information-center/educational-resources/electricity-101.

Department of Energy. “Energy Sector Cybersecurity Preparedness." Accessed September 14, 2018. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity.

Department of Energy. “Reducing Cyber Risk to Critical Infrastructure: NIST Framework.” Accessed September 1, 2018. https://www.energy.gov/oe/cybersecurity-critical-energy-infrastructure/reducing-cyber-risk-critical-infrastructure-nist.

Department of Homeland Security Privacy Office and the Office for Civil Rights and Civil Liberties. “Executive Orders 13636 and 13691 Privacy and Civil Liberties Assessment Report.” January 26, 2018. https://www.dhs.gov/sites/default/files/publications/2017%20EO%2013636_13691%20Section%205%20Report_Signed%20012618_Final.pdf.

Department of Homeland Security. “Critical Infrastructure Sector Partnerships.” Accessed December 8, 2017. https://www.dhs.gov/critical-infrastructure-sector-partnerships.

Department of Homeland Security. “Overview of Cyber Vulnerabilities.” Accessed September 3, 2018. https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities.

Department of Homeland Security. “What Is Critical Infrastructure?” December 19, 2012. https://www.dhs.gov/what-critical-infrastructure.

Department of Homeland Security. *NIPP 2013Partnering for Critical Infrastructure Security and Resilience*. Washington DC: DHS, 2013. https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

Department of Homeland Security: Office of Cybersecurity and Communications. "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies." September 2016. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

Devitt, Michael. "A Brief History of Computer Hacking." Dynamic Chiropractic. Last modified June 18, 2001. https://www.dynamicchiropractic.com/mpacms/dc/article.php?id=18078.

Di Stasio, John. "The Value of Defense in Depth: Cybersecurity of the Electric Grid." *Morning Consult* (blog), April 6, 2017. https://morningconsult.com/opinions/value-defense-depth-cybersecurity-electric-grid/.

Donghui, Park, Julia Summers, and Michael Walstrom. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks." The Henry M. Jackson School of International Studies. Last modified October 11, 2017. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

Douris, Constance. "Utilities Will Spend Billions on Cybersecurity as Threat Grows." Forbes. Last modified September 21, 2017. https://www.forbes.com/sites/constancedouris/2017/09/21/utilities-will-spend-billions-on-cybersecurity-as-threat-grows/.

E-ISAC. "Understanding Your E-ISAC." June 2016. https://www.nerc.com/pa/CI/ESISAC/Documents/Understanding%20Your%20E-ISAC_June%2028%202016_FINAL.PDF.

Electric Light & Power. "Updated: Electric Utilities Make Headway on Harvey Outage Restorations." Accessed September 2, 2018. https://www.elp.com/articles/2017/08/harvey-causes-300-000-power-outages-at-peak.html.

Electricity Information Sharing and Analysis Center (E-ISAC). "Analysis of the Cyber Attack on the Ukrainian Power Grid." March 18, 2016. https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

Electronic Privacy Information Center. "EPIC - PPD-21." Accessed September 2, 2018. https://epic.org/foia/dhs/ppd-21.html.

Erdman, Shelby Lin. “How Vulnerable Is the U.S. Power Grid to a Cyberattack? 5 Things to Know.” AJC. March 19, 2018. https://www.ajc.com/news/national/how-vulnerable-the-power-grid-cyberattack-things-know/YujzcltJ5wB2z8zJHyzPvI/.

Every CRS Report. “DOE’s Office of Electricity Delivery and Energy Reliability (OE).” December 13, 2016. https://www.everycrsreport.com/reports/R44357.html.

Executive Office of the President. “National Electric Grid Plan.” December 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/National_Electric_Grid_Action_Plan_06Dec2016.pdf.

FireEye. “Sb-Critical-Infrastructure,” 2017. https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/pf/ms/sb-critical-infrastructure.pdf.

G. D. S. Associates. “Physical Security Threats and the U.S. Power Grid.” January 19, 2016. https://www.gdsassociates.com/physical-security-threats-u-s-power-grid/.

Ghune, Piyush, Ruchita N Ghune, Pawan Pandey, and Pushpendra Mishra. “Application of Wireless Sensor Networks in Smart Grid - Opportunities, Challenges & Technologies Available.” PDFS. Accessed September 1, 2018. https://pdfs.semanticscholar.org/9465/91f50e41243930861c043df6566bfcf891ca.pdf.

GReAT. “BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents.” *Securelist - Kaspersky Lab’s Cyberthreat Research and Reports* (blog), January 28, 2016. https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/.

Greenberg, Andy. “Hackers Gain Direct Access to US Power Grid Controls.” Wired. September 6, 2017. https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/.

Greenberg, Andy. “How an Entire Nation Became Russia’s Test Lab for Cyberwar.” Wired. June 20, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.

Greenberg, Andy. “How Power Grid Hacks Work, and When You Should Panic.” Wired. October 13, 2017. https://www.wired.com/story/hacking-a-power-grid-in-three-not-so-easy-steps/.

Hackers Arise. “SCADA Hacking: SCADA Protocols (DNP3).” February 10, 2015. https://www.hackers-arise.com/single-post/2017/02/10/SCADA-Hacking-SCADA-Prortocols-DNP3.

Hall, David. “Why Public-Private Partnerships Don’t Work.” PSI. February 2015. http://www.world-psi.org/sites/default/files/rapport_eng_56pages_a4_lr.pdf.

Harrell, Brian. “Why the Ukraine Power Grid Attacks Should Raise Alarm.” CSO. March 6, 2017. https://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html.

IEEE Conference Publication. “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies.” Accessed September 2, 2018. https://ieeexplore.ieee.org/document/8090056/.

Information Technology Industry Council. “Benefits of Information Communications Technology to Energy Infrastructure.” Accessed September 3, 2018. https://www.energy.gov/sites/prod/files/2015/04/f21/ DOEQERITIcomments2014.pdf.

Internet of Things. “Safeguard Your Industrial Assets by Training Your Shop Floor Team in Cybersecurity.” May 25, 2018. https://www.iotforall.com/iiot-cybersecurity-employee-training/.

IOActive. *A Risk-Based Approach to Determining Electronic Security Perimeters and Critical Cyber Assets*. Seattle, WA: IOActive, 2009. https://ioactive.com/pdfs/ ARisk-basedApproachToDeterminingESPsAndCCAs.pdf.

Jackson, G. S. “Security Issues in Wireless Mesh Networks.” Chron. Accessed September 3, 2018. https://smallbusiness.chron.com/security-issues-wireless-mesh-networks-46553.html.

Jagasia, Arnav. “A Look into Public Private Partnerships for Cybersecurity: Penn Wharton Public Policy Initiative.” Penn Wharton Public Policy Initiative. April 18, 2017. https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for.

Knake, Robert. “A Cyberattack on the U.S. Power Grid.” Council on Foreign Relations. April 3, 2017. https://www.cfr.org/report/cyberattack-us-power-grid.

Koepke, Priscilla. "Cybersecurity Information Sharing Incentives and Barriers." Working paper, MIT Management Sloan School, 2017. web.mit.edu/smadnick/www/wp/ 2017-13.pdf.

Kovacs, Edward. “Template Injection Used in Attacks on U.S. Critical Infrastructure.” Security Week. July 10, 2017. https://www.securityweek.com/template-injection-used-attacks-us-critical-infrastructure.

Krambeck, Donald. “An Introduction to SCADA Systems.” All About Circuits. August 31, 2015. https://www.allaboutcircuits.com/technical-articles/an-introduction-to-scada-systems/.

Lee, Robert, and Sergio Caltagirone. “Dragonfly 2.0: Hackers Don’t Control America’s Power Grid,” Fortune. September 11, 2017. http://fortune.com/2017/09/11/dragonfly-2-0-symantec-hackers-power-grid/.

Lendvay, Ronald. “Shadows of Stuxnet: Recommendations for U.S. Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack.” Master’s thesis, Naval Postgraduate School, 2016. https://calhoun.nps.edu/bitstream/handle/10945/48548/16Mar_Lendvay_Ronald.pdf?sequence=1&isAllowed=y.

Leyden, John. “BlackEnergy Malware Activity Spiked in Runup to Ukraine Power Grid Takedown.” The Register. March 4, 2016. https://www.theregister.co.uk/2016/03/04/ukraine_blackenergy_confirmation/.

Limbago, Andrea. “Destructive Cyberattacks Are Only Going to Get Worse.” Business Insider. September 13, 2017. https://www.businessinsider.com/equifax-breach-proves-that-cyber-attacks-are-only-going-to-get-worse-2017-9.

Manimaran, Govindarasu, and Adam Hahn. “Cybersecurity of the Power Grid: A Growing Challenge.” US News. February 24, 2017. https://www.usnews.com/news/national-news/articles/2017-02-24/cybersecurity-of-the-power-grid-a-growing-challenge.

Martin, Chris, and Will Wade. “America’s Power Grid.” Bloomberg. March 14, 2016. https://www.bloomberg.com/quicktake/u-s-electrical-grid.

Merchan, Daniel, Johnnathan Peralta, Andres Vazquez-Rodas, L. I. Minchala, and D. Astudillo-Salinas. “Open Source SCADA System for Advanced Monitoring of Industrial Processes.” *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, 160–65, 2017. https://doi.org/10.1109/INCISCOS.2017.9.

National Academy of Sciences, National Academy of Engineering, and National Research Council. *America’s Energy Future: Technology and Transformation*. Washington, DC: National Academies Press, 2010. https://www.nap.edu/read/12091/chapter/1#ii.

National Council of ISACs. “About ISACs.” Accessed September 14, 2018. https://www.nationalisacs.org/about-isacs.

National Institute of Standards and Technology. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication 800-53 Revision 4. Greensburg, MD: National Institute of Standards and Technology, 2013. https://doi.org/10.6028/NIST.SP.800-53r4.

National Research Council. *America’s Energy Future: Technology and Transformation*. Washington DC: National Academic Press, 2009. https://doi.org/10.17226/12091.

National Research Council. *Terrorism and the Electric Power Delivery System*. Washington DC: National Academic Press 2012. https://doi.org/10.17226/12050.

North American Reliability Corporation. “High-Impact Low-Frequency Event Risk to the North American Bulk Power System.” June 2010. https://www.energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

Obregon, Luciana, and Barbara Filkins. “Secure Architecture for Industrial Control Systems.” September 23, 2015, 27, https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327.

Office of the Director of National Intelligence. “Executive Order 13636.” Accessed September 2, 2018. https://www.dni.gov/index.php/ic-legal-reference-book/executive-order-13636.

Pagliery, Jose. “Sniper Attack on California Power Grid May Have Been ‘An Insider,’ DHS Says.” CNNMoney. October 17, 2015. https://money.cnn.com/2015/10/16/technology/sniper-power-grid/index.html.

Parthasarathy, Nikhil. “Cybersecurity and the US Energy Grid.” Stanford University. December 20, 2016. http://large.stanford.edu/courses/2016/ph240/parthasarathy2/.

Peterson, Andrea. “Hackers Caused a Blackout for the First Time, Researchers Say.” *Washington Post*. January 5, 2016. https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/?noredirect=on&utm_term=.17f8269a82ae.

Pierluigi Paganini. “Dragonfly 2.0: The Sophisticated Attack Group Is Back with Destructive Purposes.” Security Affairs. September 7, 2017. https://securityaffairs.co/wordpress/62782/hacking/dragonfly-2-0-campaigns.html.

Plumer, Brad. “It’s Way Too Easy to Cause a Massive Blackout in the U.S.” Vox. April 4, 2014. https://www.vox.com/2014/4/14/5604992/us-power-grid-vulnerability.

Polityuk, Pavel, Oleg Vukmanovic, and Stephen Jewkes. “Ukraine to Probe Suspected Russian Cyber-attack on Grid.” Reuters. January 18, 2017. https://www.reuters.com/article/us-ukraine-cyber-attack-energy/kiev-power-outage-in-december-was-cyber-attack-ukrenergo-idUSKBN1521BA.

Popik, Thomas. “Examining The FERC-NERC Relationship & Setting Grid Reliability Standards.” OurEnergyPolicy. July 16, 2014. http://www.ourenergypolicy.org/examining-the-ferc-nerc-relationship-setting-grid-reliability-standards/.

Power Lines Inc., “Electrical Substations.” July 2, 2014. http://powerlinesinc.com/electrical-substations/.

Prisco, Andrés, Felipe Sánchez and John Freddy Duitama M. “Intrusion Detection System for SCADA Platforms Through Machine Learning Algorithms.” *IEEE Colombian Conference on Communications and Computing (COLCOM)*, no. 1 (August 2017): 1-10. https://doi.org/10.1109/ColComCon.2017.8088210.

Raduege, Harry. “The Public/Private Cooperation We Need on Cyber Security.” Harvard Business Review. June 18, 2013. https://hbr.org/2013/06/the-publicprivate-cooperation.

Reuters. “Ukraine to Probe Suspected Russian Cyber-attack on Grid.” December 31, 2015. https://www.reuters.com/article/us-ukraine-crisis-malware/ukraine-to-investigate-suspected-computer-attack-on-energy-grid-idUSKBN0UE0ZZ20151231.

Rodilas, Del. “Hack on Ukrainian Power Grid Highlights the Urgency for Accelerated Threat Intelligence in Industrial Control Systems.” Palo Alto Networks. April 7, 2016. https://researchcenter.paloaltonetworks.com/2016/04/utilities-pan-os-7-1-utilities/.

SANS Institute. “Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack.” InfoSec Reading Room Paper, SANS Institute, 2001. https://www.sans.org/reading-room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack-606.

Schmidt, Michael S., and Nicole Perlroth. “Executive Order on Cybersecurity Is Issued.” New York Times, February 12, 2013. https://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html.

SearchNetworking. “Server Message Block Protocol (SMB Protocol).” Accessed September 2, 2018. https://searchnetworking.techtarget.com/definition/Server-Mesdsage-Block-Protocol.

SearchSecurity. “Ethical Hacker.” Accessed September 2, 2018. https://searchsecurity.techtarget.com/definition/ethical-hacker.

Secure Envoy. “What is Two Factor Authentication?” Accessed September 2, 2018. https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm.

SESP Group. “Radio Jamming.” Accessed September 3, 2018. http://www.sesp.com/radio-jammers.asp.

Sharma, Rupali. “Gray-Hole Attack in Mobile Ad-Hoc Networks: A Survey.” 7 (2016): 4 http://ijcsit.com/docs/Volume%207/vol7issue3/ijcsit2016070389.pdf.

Smart, Paul. “Getting to Know DNP3.” Campbell Scientific. January 20, 2016. https://www.campbellsci.com/blog/getting-to-know-dnp3.

Sobczak, Blake. “Grid Monitor Gambles on More Utility Information-Sharing.” E&E News. February 2016. https://www.eenews.net/stories/1060073087.

Symantec. “Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group.” October 20, 2017. https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks.

The Guardian. “Mass Blackout Hits California, Arizona and Mexico.” September 9, 2011. https://www.theguardian.com/world/2011/sep/09/blackout-california-arizona-mexico-san-diego.

The Hill. “Why a Power Grid Attack Is a Nightmare Scenario.” Accessed September 2, 2018. http://thehill.com/policy/cybersecurity/281494-why-a-power-grid-attack-is-a-nightmare-scenario.

The Independent. “This Is What an Executive Order Is and How They Can Be Overruled.” January 30, 2017. http://www.independent.co.uk/news/world/americas/presidential-executive-orders-donald-trump-what-are-they-constitutional-limits-congress-anti-a7554231.html.

The White House. “Executive Order Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.” December 29, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency.

The White House. “Presidential Policy Directive - Critical Infrastructure Security and Resilience.” February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Thomas, Andrew. “Skkynet Requirements for IIoT Data Communication.” Skynet. July 5, 2017. https://skkynet.com/requirements-iiot-data-communication/.

Transmission & Distribution World. “GridEx III Showcases Steady Improvements.” Accessed September 2, 2018. https://www.tdworld.com/transmission/gridex-iii-showcases-steady-improvements-participation-coordination.

Trend Micro USA. “Industrial Control System.” Accessed September 2, 2018. https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system.

U.S. Energy Information Administration (EIA). “U.S. Electric System Is Made up of Interconnections and Balancing Authorities.” July 2016. https://www.eia.gov/todayinenergy/detail.php?id=27152.

United States Department of Labor. “Electric Power E-Tool: Illustrated Glossary: Substations.” Accessed September 3, 2018. https://www.osha.gov/SLTC/etools/electric_power/illustrated_glossary/substation.html.

United States Environmental Protection Agency. “U.S. Electricity Grid & Markets.” Overviews and Factsheets. August 30, 2017. https://www.epa.gov/greenpower/us-electricity-grid-markets.

Veracode. “Man in the Middle Attack: Tutorial & Examples.” Accessed September 3, 2018. https://www.veracode.com/security/man-middle-attack.

Vinson, Carl, Jerry Hallenstein, William Coston, Lynn Fisher, and Sofia Delgado Persuquia. “Review of Physical Security Protection of Utility Substations and Control Centers.” The Florida Public Service Commission Office of Auditing and Performance Analysis. December 2014. http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Physical_Security_2014.pdf.

Waterman, Shaun. “Experts Say Government’s Information Sharing Program is All Take and No Give.” *Cyberscoop* (blog), November 15, 2017. https://www.cyberscoop.com/dhs-ais-program-house-homeland-committee/.

Weeks, Jennifer. “U.S. Electrical Grid Undergoes Massive Transition to Connect to Renewables - Scientific American.” Scientific American. April 28, 2010. https://www.scientificamerican.com/article/what-is-the-smart-grid/.

Weise, Elizabeth. “Intrusion - But No Attack - on U.S. Energy Grid Is a Warning, Says Former NSA Official.” USA Today. September 6, 2017. https://www.usatoday.com/story/tech/news/2017/09/06/dozens-power-companies-breached-hackers-cybersecurity-researcher-says/638503001/.

WhatIs. “What Is NERC CIP (Critical Infrastructure Protection)?” Accessed September 3, 2018. https://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection.

Whitehead, D. E., K. Owens, D. Gammel, and J. Smith. “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies.” *2017 70th Annual Conference for Protective Relay Engineers (CPRE),* (April 2017): 10, https://doi.org/10.1109/CPRE.2017.8090056.

Whittaker, Zack. “US Report Confirms Ukraine Power Outage Caused by Cyberattack.” ZDNet. February 29, 2016. https://www.zdnet.com/article/us-report-confirms-ukraine-power-outage-caused-by-cyberattack/.

Williamson, Graham. “OT, ICS, SCADA – What’s the Difference?” KuppingerCole. July 7, 2015. https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference.

Xu, Wenyuan, Ke Ma, W. Trappe, and Yanyong Zhang. “Jamming Sensor Networks: Attack and Defense Strategies.” *IEEE Network* 20, no. 3 (May 2006): 41–47. https://doi.org/10.1109/MNET.2006.1637931.

Zetter, Kim. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” Wired. March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zirin, James. “Are We on the Brink of a Cyber-War?” Huffington Post. April 26, 2010. https://www.huffingtonpost.com/james-d-zirin/are-we-on-the-brink-of-a_b_475237.html.

Zucchetto, James. “Terrorism and the Electric Power Delivery System.” The National Academies Press. Accessed September 2, 2018. https://www.nap.edu/read/12050/chapter/8.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California