The Vulnerability of the United States Electrical Power Grid

Karyn Melligan
American Military University

Perhaps no other sector of the United States critical infrastructure is as important to as the electrical power grid. Modern technology has improved the quality of American lives in countless ways, however the over reliance on the electrical power grid for this technology and everyday life has increased the risks associated with catastrophic failure. This study discusses the risks and the vulnerability of the United States electrical power grid and provides recommendations that can be implemented to secure the United States electrical power grid from both physical and cyberattack.

Keywords: electrical power grid, cyberattack, vulnerability, critical infrastructure

INTRODUCTION

The vulnerability of the United States electrical power grid, arguably the most critical of our nation's critical infrastructure, has become an alarming and increasing reality. Various segments of our critical infrastructure, including transportation, telecommunications, public safety, the financial industry, and other utilities, are dependent upon the electrical power grid. Conversely, the electrical power grid depends upon other critical infrastructure, namely oil, gas, and telecommunications, to operate. Current threats to the United States electrical power grid include physical attacks, cyberterrorism attacks, weather, natural disasters, electromagnetic pulse, and aging facilities. The Department of Homeland Security has noted that state actors who are a threat to the United States electrical power grid include Russia, China, Iran, and North Korea, while organized crime and jihadist extremist terrorists are among notable non-state actors (Angerholzer, Cilluffo, Mahaffee, & Vale, 2014).

The purpose of this study will be to discuss the vulnerability of the United States electrical power grid and steps that can be taken to protect this portion of our critical infrastructure through a qualitative review of current and potential threats, current policies, and shortcomings within these policies. Included in this discussion will be a summary of specific power failure incidents since 2001, an analysis of the risks to our electrical grid, and recommendations to counter the threat to our electrical power grid.

Vulnerability of the United States Electrical Power Grid

Throughout the United States, millions of Americans depend upon electricity to make their morning coffee, access the Internet, watch television, use the ATM, pump gasoline, shop for groceries, and hundreds of other activities. Our energy sector, transportation, financial and telecommunications infrastructures have become increasingly interconnected, "virtually every crucial economic and social

function depends on the secure and reliable operation of these infrastructures" (Amin & Giacomoni, 2011, p. 34). The United States electrical power grid is vulnerable to natural disasters, weather, and terrorist attacks, the result of which could create an adverse effect on our every day lives, our nation's economy, and ultimately, our national security.

While terrorist attacks, both physical and cyber, are a growing fear in securing our electrical power grid, the aging infrastructure of the electrical power grid itself is of significant concern. Aging equipment, obsolete system layout, and outdated engineering create higher failure rates, higher maintenance and repair costs, and ineffective power delivery. An additional challenge to securing our electrical power grid lies in the fact that approximately 85% of the United States critical infrastructure, including the electrical power grid, is privately owned creating both legal and ethical implications with public-private partnerships and the Department of Homeland Security (Busch & Givens, 2012).

Physical Power Failure Incidents

In August 2003, upstate Ohio transmission lines overburdened with high current demand brushed up against overgrown shrubbery and trees, which caused the transmission line to trip off-line. Under normal circumstances, such a failure would set off alarms in the local utility's control operations; however, a software bug in the alarm system of a control room at FirstEnergy Corporation failed, and operators were initially unaware of the incident. Once aware of the situation, as operators attempted to determine the source of the transmission line failure, three additional lines tripped off-line, resulting in a cascading electrical failure and blackout impacting over 45 million residents in the Northeastern and Midwestern regions of the United States as well as Southeast Canada. Over 256 power plants experienced electrical failure, as did major cities including New York, Detroit, Albany, Hartford, and Cleveland. Full restoration of electrical power took four days in the United States, over a week in Southeast Canada.

On September 8, 2011, over 2.7 million customers in Southern California, Arizona, and Baja California lost electrical power for approximately twelve hours when a technician, switching out a capacitor bank on a 500kV line at an APS substation in North Gila, Arizona made a procedural error causing the line to trip which created a cascading power failure. The entire San Diego region was without power, impacting schools, restaurants, airline flights, public transportation, water and sewage stations, grocery stores, banks, and ultimately 1.4 million individuals (Federal Energy Commission, 2012). Though the Federal Energy Regulatory Commission determined that the outage was caused by 'human error,' six utilities were cited for reliability violations and fined in relation to the incident (Lee, 2012).

When Hurricane Sandy washed ashore in October 2012, over eight million homes in New York, New Jersey, and 19 other states lost electrical power resulting in $14 to $26 billion in electrical outage costs. Storm surge waters flooded electric substations, and terminals responsible for the production of petroleum and petroleum-based products were damaged (Lacey, 2014). As a direct result of these power failures, planes were grounded; trains stop running; water pumps lost compression causing potential contamination of the water supply; raw sewage spilled into waterways; oil refineries were shut down; cellular phone transmission was interrupted; cable television service was disabled, and grocery stores were unable to check out customers.

On April 16, 2013, multiple snipers attacked the Pacific Gas & Electric Metcalf substation in San Jose, California, with high-powered rifles for a full 19 minutes, firing over 100 rounds of ammunition at a bank of transformers, severely damaging seventeen transformers (Smith, 2014). While Pacific Gas & Electric was able to avoid a blackout by transferring power from their Silicon Valley power plants, it would take a full 27 days before the Metcalf substation was again operational. Jon Wellinghoff, then chairman of the Federal Energy Regulatory Agency, later described the attack as "the most significant incident of domestic terrorism involving the grid that has ever occurred" (Follett, 2016, p. 3).

In August 2013, just months after the terrorist attack on the Metcalf substation in California, three consecutive attacks occurred on Entergy Arkansas substations and transformers. On August 21, 2013, a support tower for a 500,000-volt electricity line was sabotaged, causing the tower to fall onto a railroad track, which in turn caused a train to sever multiple power lines cutting electrical power to Cabot,

Arkansas. A month later, on September 29, 2013, an attack on the Entergy electricity station in Scott, Arkansas, caused over two million dollars in damage.

In June 2014, a bomb, later described by police as a 'crude incendiary device,' was placed under a 50,000-gallon diesel tank in Nogales, Arizona. Though the device had been ignited, it failed to ignite the diesel fuel storage tank. Had the device ignited the storage tank, over 30,000 residents could have lost electrical power for a significant amount of time (Kreft, 2014).

Cyberattacks

The office of Electricity and Energy Reliability has stated, "Addressing cybersecurity is critical to enhancing the security and reliability of the nation's electric grid. Ensuring a resilient electric grid is particularly important since it is arguably the most complex and critical infrastructure that other sectors depend upon to deliver essential services" (Department of Energy, 2014). In a series of cyber war research initiatives between 2005 and 2014, the United States government and researchers demonstrated the effectiveness of cyberattacks to compromise power systems.

In 2006, the United States government intelligence, in conjunction with the Israeli Intelligence Corps, participated in an operation named "Operation Olympic Games." The Stuxnet computer worm was developed as part of this joint program, and by the time it was "found" in June 2010 had infected in excess of 100,000 computer systems across the globe despite having been programmed to infect only computer systems within Iran (Goodin, 2016). The Stuxnet computer worm destroyed approximately 20% of the centrifuges in Iran's Natanz Nuclear Power Plant but was also part of a larger United States cyberattack plan targeting Iran's communications systems, air defense systems and power grid (Kelley, 2012). Stuxnet's ultimate value was its ability to physically damage infrastructure by compromising supervisory control and data acquisition (SCADA) systems and revolutionizing cyber warfare because of the ability to target industrial facilities. Though the Stuxnet computer worm was designed by United States and Israel intelligence, and not utilized in an attack on the United States electrical grid, the ease with which the Stuxnet computer worm destroyed the Iranian centrifuges and ease in which the Stuxnet computer worm was able to infect other computers beyond the intended target, demonstrates the inherent risk to our own electrical grid. The 'success' of the Stuxnet computer worm led researchers to develop as an additional component of "Olympic Games" the Flame virus which in addition to compromising Iranian SCADA systems, had the capability to take screenshots, log keyboard strokes, activate cameras and microphones, and send and receive commands and data via Bluetooth wireless technology (McElroy & Williams, 2012; Zetter, 2012).

In 2007, in a controlled test named 'Aurora,' Idaho National Lab researchers utilized a computer virus to manipulate computer network systems, that controlled diesel generators (Donolo, Gusman, Mynam, Salmon & Zeller, 2009). The tests "involved the opening and closing of circuit breakers, which resulted in an out-of-synchronism condition (Donolo et al., p. 21). This out-of-synchronism condition placed stress upon critical components within the generators resulting in a system failure. The Aurora test demonstrated the ease in which a computer virus could manipulate power grid systems, create physical damage, and cause cascading power failures.

In 2011, a group of Russian hackers known as "Dragonfly" began various Stuxnet type cyberattacks against control systems found in petroleum pipeline operators, electrical grid operations, electricity generation operations, and additional critical energy infrastructure within the United States (Thomson & Rhan, 2014) Later that same year, from December 2011 through June 2012, a cyber hacker named UglyGorilla was able to obtain sensitive data from gas pipeline companies, penetrating computer systems of the United States 300,000-mile pipeline network that is a critical component of the nation's economy. In 2014, the United States Justice Department brought charges against five members of China's elite military cyber division in response to the hack. The investigation by the Justice Department exposed an ongoing sophisticated cyber theft campaign that had been happening since 2006 by the Chinese military (Sobczak, Northley & Behr, 2017).

Each of these incidents demonstrates the vulnerability of the electrical power grid within the United States and the ease with which the electrical power grid can be compromised and taken off-line. Due to

the inter-reliant configuration of the electrical power grid, a singular failure, no matter the cause, may result in cascading power outages impacting millions of people and create significant economic costs.

RESEARCH QUESTION

How does Department of Homeland Security legislation influence the mitigation of natural and man-made threats targeting the American electrical power grid system?

LITERATURE REVIEW

The United States electrical power grid consists of over 15,000 electrical generators in over 10,000 power plants, 55,000 plus substations, 200,000 miles of transmission lines, 250,000 miles of distribution lines, and an astonishing one trillion dollars in physical assets (Amin & Giacomoni, 2012). Despite this vast interconnected network, if just nine of the over 55,000 electrical substations were attacked or taken off-line by terrorists, the entire United States electrical power grid could be shut down for weeks if not months (Burke & Schneider, 2015; Smith, 2014). The Federal Energy Regulatory Commission notes that this vulnerability is based upon key equipment; high voltage large transformers which carry 60% to 70% of United States electricity, weighs hundreds of tons, costs millions of dollars and can take over a year to replace (Burke & Schneider, 2015).

Of the 198 reported cyber incidents in 2012, 48% involved the energy sector, primarily electricity. Schainker, Douglas, and Kropp (2006) discuss the threats to both the physical and cyber systems of the United States electrical power grid noting the rise of terrorism plots, attacks and natural disasters in the last ten years, which illustrate the vulnerability of the electrical power grid and the far-reaching impact of an incident which takes our power grid off-line. Noted is the increasing dependence upon the Internet, computerized monitoring and grid control systems that are at increasing risk to cyberterrorism attack and the anonymity in which such an attack could occur. "Cybersecurity is only as strong as the [weakest link] in the chain of interconnected information and communication systems that utilities use … and successful implementation of new cybersecurity tools are crucial for effective industry-wide cybersecurity" (Schainker, Douglas & Kropp, 2006, p. 33).

Interconnectivity

The interconnectivity of the United States critical infrastructure illustrates the vulnerability of interconnecting networks, the consequences of growing interconnections, and the need for increased security. The interdependent relationship between critical infrastructure sectors can create cascading effects in numerous critical infrastructures when one critical infrastructure sector is damage, disrupted, or destroyed (Alcaraz & Zeadally, 2014). Modern society has become reliant upon these critical infrastructures, the damage or destruction of which could create supply shortages, substantial economic impact and public disorder (Arianos, Bompard, Carbone & Xue, 2009). The importance of these critical infrastructures is a crucial issue in learning how to protect them from the threat of failures and terrorist attacks. This threat is compounded by the same interconnectivity that has allowed for substantial growth, a disruption, which could last for weeks or even months, the impact extreme.

Yates (2013) notes the potential loss of life from a disruption of the electrical power grid infrastructure, observing that when critical infrastructure systems fail, loss of life possible and probable. Yates posits that a loss of electrical power could result in immediate deaths and injuries from blackout conditions but also increased fatalities and injuries from fires, carbon monoxide poisoning, hypothermia, hyperthermia, respiratory issues, and failure of life support systems and degradation of water supply systems.

The Northeast Blackout in 2003, which was caused by a cascading failure of the Northeast Interconnection portion of the United States power grid, knocked out power to an estimated fifty million individuals and resulted in an estimated $10 billion impact on the combine United States/Canada economy. Businesses and banks closed, schools closed, subways stopped running, traffic lights failed to

work, and hospitals were forced to rely upon emergency back up generating systems (Yates, 2012). In a study conducted by Anderson and Bell (2012) on the mortality rates of the Northeast Blackout, 90 deaths were directly attributed to the blackout; 12 accidental, 78 non-accidental.

Vulnerability

Amin and Giacomoni (2012) examine the vulnerability of the existing electrical power grid to both terrorist attacks and natural disasters based on the interdependencies in energy, transportation, and telecommunications, and financial infrastructures. The challenge presented by these interdependencies is establishing a secure yet interconnected system in one of the most complex and most extensive power grids. The sheer size and complex nature of the United States electrical power grid make it impossible to protect the entirety of this critical infrastructure. Amin and Giacomoni (2012) note that of the over 450,000 miles of 100-Kv or higher transmission lines, thousands of miles of lower voltage lines and the ever-increasing renewable energy sources such as land-based wind installations, "make it probable that a well-organized, determined group of terrorists could take out portions of the grid" (p. 35).

A 2001, SANS Institute white paper, stated the dire consequences of an attack on the electrical power grid succinctly. "Without electrical power, just about everything in our information age society and economy goes dead: respirators, heaters, air conditioners, and refrigerators in hospitals and homes, perishable food supplies in markets, stock trading on Wall Street, financial transfers between banks, and much more, including, of course, the lights, everywhere from Manhattan to Watts" (SANS Institute, 2001, p. 1). The threat is not merely to the safety and security of the United States public, but ultimately to our nation's homeland security. Vulnerability extends to our nation's defenses, including satellites, stealth aircraft, and even communications to troops in the field. As the threats to our nations power grid rises, so do the concerns of protecting this critical infrastructure.

In a report published by the Department of Energy in 2003, the electrical grid was described as "aging, inefficient and incapable of meeting future energy needs ... without operational changes and substantial capital investment," a full twenty percent of sustained power outages from 2008 to 2011 attributed to failing electrical grid equipment (United States Department of Energy, 2003, p. iii). Increasingly, the sophisticated nature of malicious code and intrusions through cyberattacks challenges the United States' electrical power grid. Existing control systems were initially designed for proprietary, stand-alone networks, and as these stand-alone systems were connected to the Internet, protocols, and technology to secure these systems were absent. The numerous communications media and protocols used in communication and control of power systems varied to include not only commercial telephone lines but also wireless, microwave, optical fiber, and Internet communications. As these communication media and protocols have been changed and enhanced via the Internet, the use of electronic transmission to connect major substations with smaller sites has increased the need for security.

In 2010, Congresswoman Yvette Clarke warned of the vulnerability of the electrical grid to advanced viruses explicitly designed to target control systems and that China, Russia, Iran and North Korea "are known to regularly use offensive cyberattack capabilities, while terrorist organizations continue to work to develop these capabilities" (Clarke, 2010, p. 1). As well, the National Academy of Sciences warned in 2009 that a geomagnetic storm, which would impact our electrical grid, is inevitable and could cause "$1 to 2 trillion in damage" (National Academy of Sciences, 2009, p. 2) the resulting damage taking five to ten years to recover from.

METHODOLOGY AND RESEARCH STRATEGY

This research focused on the United States electrical power grid, vulnerabilities, and recent attacks or incidents that compromised the electrical power grid. This research addresses how Department of Homeland Security legislation and policies influence the mitigation of natural and man-made threats targeting the American electrical power grid system. In reviewing the scholarly literature relevant to this qualitative study, the following databases were searched, and data was gathered from: Academic Search Premier, EBSCOhost, LexisNexis Academic, United States Department of Justice, United States

Department of Homeland Security, Federal Emergency Management Agency, the United States Code, SAGE Journals, SAGE Knowledge, SAGE Research Methods, Ebook Central and the Homeland Security Digital Library. Additionally, an Internet search utilizing Google Scholar and Google was conducted to obtain current news articles relative to key terms. Terms used in the literature search included: *critical infrastructure, critical infrastructure protection, critical infrastructure strategies, cyberattacks, terrorist attacks, terrorist attacks on electrical facilities, electrical power grid, electrical power grid security, vulnerability of the electrical power grid, SCADA, Department of Homeland Security, Homeland Security policies, Presidential Directives, NIPP, and public-private partnerships.*

ANALYSIS AND FINDINGS

The United States electrical power grid, as we know it, is actually made up of ten 'power markets', which are connected to three electrical grids. The Eastern Interconnection, The Western Interconnection and the Texas Interconnection deliver electricity from electricity producers to consumers over high voltage transmission and distribution lines. Within each of the three Interconnections are various 'power markets,' which consist of private utility providers, power plants, suppliers, and electrical distribution networks. At present, there are over 500 companies within these three Interconnections operating our electrical power utilities. In 2009, plans were proposed to unite the Eastern, Western, and Texas Interconnection electrical grids via three 5 GW superconductive high-voltage direct-current power transmission lines in Clovis, New Mexico, at the 22-acre Tres Amigas SuperStation (Bryan, 2017). At a proposed cost in excess of $2 billion, this Super Grid would increase transmission capacity while ensuring the reliability of the United States electrical power grid. Among the proposed Super Grid features is a controlled flow of energy while isolating each of the three independent grids to ensure the synchronization of the grids. However, the developers of the project have failed to meet contractual milestones, including payments, and in February 2017, Tres Amigas relinquished leased land back to the New Mexico State Land Office and announced the project was being scaled back to a $200 million project (Bryan, 2017).

The North American Electric Reliability Corporation (NERC) is a regulatory authority that oversees the electrical utility system within the United States to assure reliability and security of the electrical grid system in the United States; however, each individual power company is responsible for 'grid security.' The Federal Energy Regulatory Commission (FERC) is responsible for regulating the transmission, distribution, and sale of electricity within the United States as well as enforcing energy industry regulations. The Department of Energy is the lead government agency responsible for the security of the electrical power grid and serves as the sector-specific agency, while the Department of Homeland Security coordinates both security and preparedness (Department of Homeland Security, 2010).

In 1998, then-President Clinton signed Presidential Decision Directive 63 (PDD 63) regarding critical infrastructure protection within the United States. One of the goals of PDD 63 was to create public-private partnerships to ensure information sharing between the private sector and the government to secure critical infrastructure with the establishment of the Information Sharing and Analysis Centers. In the aftermath of the terrorist attacks on September 11, 2001, the federal government has actively sought to combat threats to our nation's critical infrastructure. Both the United States Patriot Act and the National Infrastructure Protection Plan define critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters" (United States Patriot Act, 2001, p. 103).

In 2003, the Department of Homeland Security released the *National Strategy to Secure Cyberspace,* which included five priorities for establishing and improving secure cyber networks. These five priorities included a national cybersecurity response system, threat, and vulnerability reduction program, awareness and training program, as well as securing the federal government's cyberspace and the creation of a National Security and International Cyberspace Security Cooperation. The Department of Homeland Security recognized the federal government's responsibility to protect key infrastructures in the 2003 *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.*

In Presidential Policy Directive 21, which established a national policy on critical infrastructure security, the energy sector was declared uniquely vital to our nation's infrastructure because the fifteen other critical infrastructure sectors rely upon the energy sector (Obama, 2013). Presidential Policy Directive 21 also directed the Secretary of Homeland Security to provide strategic guidance, unity of effort, and coordination of the federal government efforts to promote security and resilience of the United States' critical infrastructure. This task included identifying and prioritizing critical infrastructure, identifying physical and cyber threats, identifying of vulnerabilities and consequences, and establishing two critical infrastructure centers. These two centers, one for physical infrastructure, the second for cyber infrastructure, would be operated by the Department of Homeland Security, and serve as sources of situational awareness and information for critical infrastructure partners. PPD 21 also required the Secretary of Homeland Security to develop a description of the Department of Homeland Security and federal government's role in critical infrastructure, to evaluate existing public-private partnerships, and to develop a situational awareness capability for critical infrastructure and update the National Infrastructure Protection Plan (NIPP).

In 2013, then-President Obama also signed Executive Order 13636, which mandated that the Secretary of Homeland Security and the Secretary of Defense would provide "classified cyber threat and technical information to eligible private critical infrastructure companies" (Obama, 2013). This mandate resulted in the creation of the National Cyber Security & Communications Integration Center (NCCIC), which provides 24 hours a day situational awareness and incident management. In 2013, the Cyber Warrior Act was introduced in Congress to allow the National Guard in each state to establish a National Guard Cyber and Network Incident Response Team to support federal and state efforts to protect against cyberattacks on critical infrastructure.

As threats to the electrical power grid have increased, the Department of Homeland Security and the North American Electric Reliability Corporation, in conjunction with other agencies, have participated in electrical grid security exercises, which assess readiness and resilience of the electrical power grid. The North American Electric Reliability Corporation has conducted four biannual GridEx exercises to demonstrate response and recovery from simulated cyber and physical security threats and incidents, the latest in the fall of 2017. The Department of Homeland Security has conducted Cyber Storm exercises biannually since 2006 to assess critical infrastructure organization's capability to prepare for, mitigate against, and respond to cyberattacks and their potential effects. Both GridEx and Cyber Storm allow the respective electrical power grid agencies, other critical infrastructure organizations, and the Department of Homeland Security to implement mitigation efforts, and best practices to respond to and recover from either a physical or cyberattack.

CONCLUSIONS AND RECOMMENDATIONS

Since September 11, 2001, the respective Presidents of the United States, Congress, and the Department of Homeland Security have initiated legislation, presidential directives, executive orders, and policies designed to strengthen our electrical power grid along with other critical infrastructure. These legislative actions, directives, executive orders, and policies in conjunction with policies of the North American Electric Reliability Corporation and the Federal Energy Regulatory Commission have provided focus on securing our electrical power grid from both physical and cyberattacks. However, these legislative actions, directives, executive orders, and policies have done little to address the aging physical assets and structure of the electrical power grid or to protect the electrical power grid infrastructure as a whole adequately. Much of the SCADA technology in the electrical power grid is over 40 years old, is too slow for current challenges and fails to sense or control enough necessary components within the electrical power grid. Incompatible control protocols still exist even in neighboring power companies, and most utility control centers rely upon human operators and telephone calls, especially during emergencies. Additionally, while the federal government, the Department of Homeland Security, the NERC and the FERC have called for investment by electrical power companies in terrorism protection measures, financial considerations, the perceived low risk of a terrorist incident, perceptions regarding shared

government responsibility and available government funding for expenditures are outweighed by day-to-day threats and operational needs.

Recommendations have been made within both the federal government and the electrical power sector for a Smart Grid, a self-healing smart grid that provides real-time self-monitoring and transmission and would minimize the impact of a terrorist attack. However, the cost to build a smart grid across the entire United States is estimated to cost $13 billion a year for ten years (Amin & Schewe, 2017), and no consensus exists on how this Smart Grid would be paid for. Additional recommendations have included federal government incentives to provide funding for the creation of a smart grid, but collaborative and coordinated decision making within the electrical industry has proven to be an obstacle (Amin & Schewe, 2017).

The sheer size of the electrical power grid within the United States makes it logistically and physically impossible to secure and protect the entire electrical infrastructure sector from a physical attack. Cyberattacks on the electrical power grid have the potential to be more destructive than a physical attack; however, security protocols against cyberattacks and intrusion may be less costly and more easily implemented. Among these security protocols should be considered layered security, deception, and new security features. Layered security would combine multiple security technologies at each layer of the computer system, reducing the risk of unauthorized access. Deception would hide or mask the real system increasing the difficulty of a successful cyberattack on a network system. Finally, new security features need be developed to detect intrusion, provide multiple levels of encryption, and authentication to prevent unauthorized intrusion.

While no singular solution to securing our electrical power grid currently exists, steps taken since the terrorist attacks of September 11, 2001, by the Department of Homeland Security, the federal government, the Department of Energy and various other agencies, especially the sharing of information regarding threats have served to mitigate against both physical and cyberattacks partially. However, until all 500 power companies can come together along with the federal government and devise an across the board strategy to deal with the threats to and vulnerability of the electrical power grid, we will continue to see events occur either from natural or man-made incidents.

REFERENCES

Amin, M., & Schewe, P. (2017). Preventing blackouts: Building a smarter power grid. *Energy.*

Amin, S., & Giacomoni, A. (2012). Smart grid-safe, secure, self-healing. *IEEE Power & Energy.*

Angerholzer, M., Cilluffo, F., Mahaffee, D., & Vale, M. (2014). *Securing the U. S. electrical grid.* Center for the Study of the Presidency & Congress. Washington, D.C.

Arianos, S., Bompard, E., Carbone, A., & Xue, F. (2009). Power grid vulnerability: A complex network approach. *American Institute of Physics.*

Bryan, S. (2017, February 15). New Mexico grid linkup plan scaled back to $200M project. *U.S. News.* Retrieved from https://www.usnews.com/news/new-mexico/articles/2017-02-15/developers-moving-forward-with-new-mexico-power-grid-project

Burke, S., & Schneider, E. (2015). Enemy number one for the electric grid: Mother Nature. *SAIS Review*, 35(1).

Busch, N., & Givens, A. (2012). Public-private partnerships in homeland security: Opportunities and challenges. *Homeland Security Affairs*, 8(18), 1-24.

Clarke, Y. (2011, November 11). Congresswoman says chance of cyberattack against electric grid is 100%. *InfoSecurity Magazine.*

Committee on Science and Technology for Countering Terrorism. (2002). *Making the Nation Safer. The Role of Science and Technology in Countering Terrorism.* National Research Council, National Academy Press, Washington, D.C.

Department of Homeland Security. (2003). *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* Washington, D.C.: United States Government Printing Office.

Department of Homeland Security. (2014). *Energy Sector-Specific Plan: An annex to the National Infrastructure Protection Plan.* Washington, D.C.: DHS. Retrieved from www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf

Donolo, M., Guzman, A., Mnyan, V., Salmon, D., & Zeller, M. (2009). Mitigating the Aurora vulnerability with existing technology. *Schweitzer Engineering Laboratories Inc.*

Federal Emergency Regulatory Commission. (2012). *Arizona-Southern California Power Outages on September 8, 2011: Causes and Recommendations*.

Follet, A. (2016, January 10). Lights out: The top 7 threats to America's power grid. *The Daily Caller.* Retrieved from http://dailycallernewsfoundation.org

Goodin, D. (2016, February 16). *Massive US-planned cyberattack against Iran went well beyond Stuxnet*. ARS Technica. Retrieved from https://arstechnica.com/tech-policy/2016/02/massive-us-planned-cyberattack-against-iran-went-well-beyond-stuxnet/

Halper, E., & Lifsher, M. (2014, February 6). Attack on electric grid raises alarm. *Los Angeles Times.* Retrieved from www.latimes.com

Kelley, M. (2012, June 1). Obama administration admits cyberattacks against Iran are part of joint US-Israeli offensive. *Business Insider*. Retrieved from www.businessinsider.com/obama-cyberattacks-us-israeli-against-iran-2016-6

Kreft, E. (2014, June 16). Another attack discovered at an electricity substation near the border-and one Congressman says it's 'only a matter of time' before more attackers 'exploit this vulnerability'. *The Blaze.* Retrieved from www.theblaze.com

Lacey, S. (2014, June 10). Resiliency: How Superstorm Sandy changed America's grid. *Greentech Media.* Retrieved from https://www.greentechmedia.com/articles/featured/resiliency-how-superstorm-sandy-changed-americas-grid#gs.mn9oCfY

Lee, M. (2014, February 4). Feds blame 6 groups for 2011 blackout. The San Diego Union-Tribune. Retrieved from http://www.sandiegouniontribune.com/sdut-violations-southwest-power-outage-2014feb04-story.html

McElroy, D., & Williams, C. (2012, May 28). Flame: World's most complex computer virus exposed. *The Telegraph.* Retrieved from www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/flame-worlds-most-complex-computer-virus-exposed.html

Obama, B. (2013a). *Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience*. Washington D.C.: The White House.

Obama, B. (2013b). *Executive Order 13636: Improving Critical Infrastructure Cybersecurity*. Washington D.C.: The White House.

SANS Institute. (2001). Can hackers turn your lights off? The vulnerability of the US power grid to electronic attack. *Information Security.*

Schainker, R., Douglas, J., & Kropp, T. (2006). Electric utility responses to grid security Issues. *IEEE Power & Energy.*

Smith, R. (2014, February 5). Assault on California power station raises alarm on potential for terrorism. *Wall Street Journal.*

Sobczak, B., Northey, H., & Behr, P. (2017, May 23). Cyber raises threat against America's energy backbone. *Energy Wire*. Retrieved from www.eenews.net

Thomson, A., & Rahn, C. (2014, July 1). Russian hackers threaten power companies, Researchers say. *Bloomberg.* Retrieved from http://www.bloomberg.com/news/2014-06-30/symantec-warns-energetic-bear-hackers-threaten-energy-firms.html

United States Department of Energy. (2003). *Grid 2030: A national vision for electricity's second 100 years*. Retrieved from http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Electric_Vision_Document.pdf.

United States Patriot Act, U.S. H.R. 3162, Public Law 107-56

Wald, M. (2014, March 13). Power grid preparedness falls short report says. *New York Times.*

Yates, A. (2013). Death modes from a loss of energy infrastructure continuity in a community setting. *Homeland Security & Emergency Management*, 10(2), 587-608.

Zetter, K. (2012, May 28). Meet Flame, the massive spy malware infiltrating Iranian computers. *Wired.* Retrieved from www.wired.com/2012/05/flame