Global Security Studies, Fall 2016, Volume 7, Issue 4

Vulnerabilities in the North American Power Grid

Gabrielle Vianna
Conflict Management and Resolution Graduate Program
University of North Carolina Wilmington
Wilmington, NC 28412
ggv4123@uncw.edu
gabriellevianna01@gmail.com

Abstract

Throughout the past century the power grid system has been assembled and modified to accommodate the rapid growth and need for reliable electricity across the United States, southern parts of Canada, and Baja California. The importance of the electric power grid system has been recognized by modern adversaries as a critical asset that can be exploited to cripple the United States. Although the Department of Energy and private power corporations have created reliability standards in order to reduce the risks of cyber and physical threats to the power grid system, the grid system still presents vulnerabilities that can be exploited by state and non-state actors.

Keywords: NERC, CIP, BPS, Reliability, Denial-of-Service, Malware, Blackstart, Infrastructural Integrity, Policy Recommendations

Introduction

In a world with constant emerging security threats, physical and digital attacks on the Untied States' power grid system have evolved into a critical national security concern. State and non-state actors alike have demonstrated that the capabilities and resources exist in order to effectively compromise the integrity of power grid system for extended periods of time. U.S. governing bodies ranging from the Department of Energy (DoE) down to local power corporations have attempted to address these trepidations through the emplacement of mandatory compliance standards. Despite compliance with the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards, the North American bulk power system (BPS) still remains vulnerable to threats from state and non-state actors.

The North American Power Grid

The late 19th and early 20th centuries marked the beginning of the electric power revolution as steam, hydraulics and coal gas became outdated and began to loose its battle with the demand for more electric power. As electric power infrastructure continued to evolve in North America, by the 20th century there were approximately 4,000 individual electric facilities (EIA, 2008). These electric utilities operated independently of each other and only supplied electricity to a specified and limited area. However, as the demand for electricity grew throughout the United States power companies began to interconnect these power utilities in order to comply with the demand for rapid growth in a cost effective manner (EIA, 2008). At the time it had also allowed the reduction of the "amount of extra capacity that each utility had to hold to ensure reliable service" (EIA, 2008). Thus the interconnected electric systems of today

emerged. Currently there are three major interconnected electric systems: The Eastern Interconnection, the Western Interconnection and the Texas Interconnection, which serve their perspective regions and include numerous subsidiaries operating under their supervision (reference the image below) (EIA, 2008).

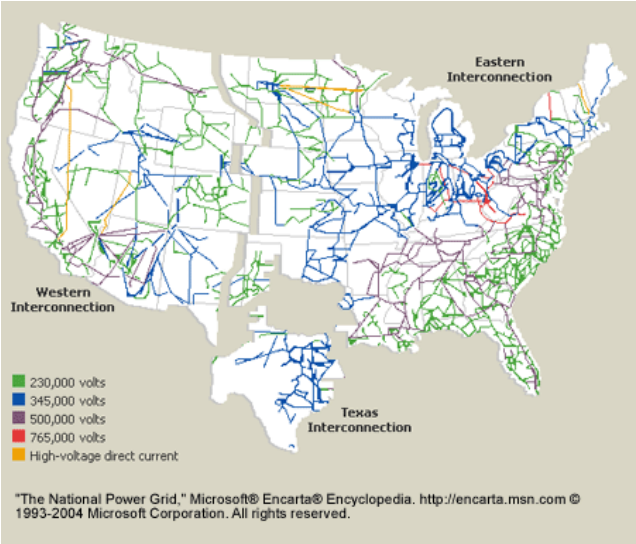

Fig. 1 Basic Breakdown of U.S. Power Interconnections (Encarta, 2004)

The three regional interconnections are designed to generally operate autonomously, although these regions do have limited interconnections (EIA, 2008). This synchronization between the three interconnections has resulted in "about 2,000 electric distribution utilities, more than 300,000 miles of transmission and distribution lines, millions of customers, and more than 7,200 power plants and generating facilities that each has at least one megawatt of generating capacity" (EIA, 2008). The power grids across the United States generally work in a linear system in which the energy is produced at individual generating stations from organic and non-organic methods such as coal, natural gas, hydroelectric dams, nuclear power plants, wind turbines, and solar panels (UCS, 2015). These generating stations vary in their ability to rapidly speed up and slow down their electricity output (UCS, 2015). Since generating stations produce energy at low voltages it has to go through a generator step up transformer which converts energy to the appropriate voltage required to travel over the transmission lines which usually consists of voltage between the ranges of 110 kV - 765 kV (UCS, 2015). The transmission lines' voltage is increased for its transfer to the distribution lines because the higher the voltage the less energy is lost during transportation. Currently the U.S. national energy grid looses an annual average of 6% of electricity during the transference process (UCS, 2015). The transmission lines are also referred to as bulk power and is essentially the backbone of the energy grid. Before the energy reaches the distribution lines it has to go through a step down transformer substation which converts the high voltage energy into lower voltages designed to allocate electricity at the appropriate levels for primary, secondary and sub-transmission consumers (UCS, 2015). Consumers that receive power from distribution lines usually consist of homes, businesses and other common facilities that are present in urban and rural communities (reference image below).

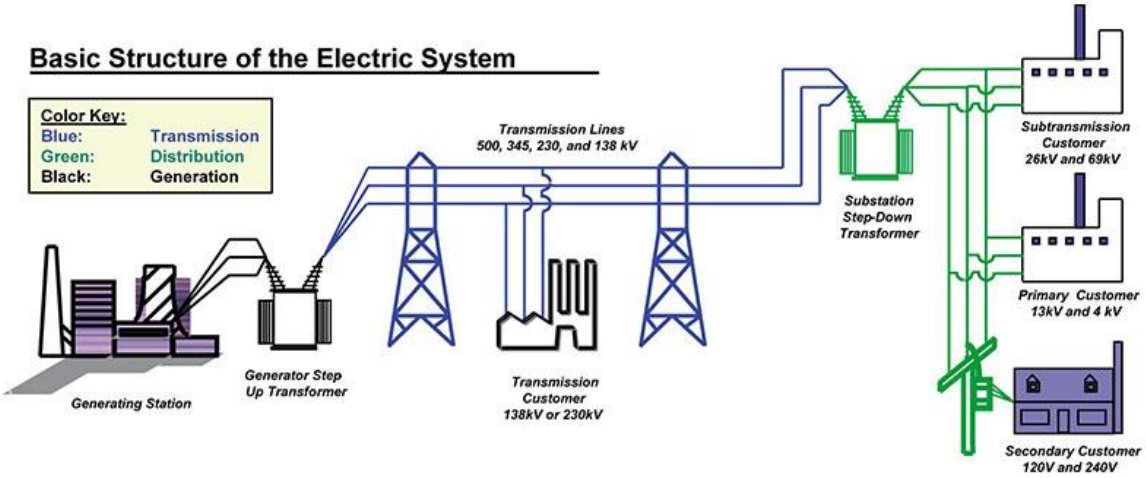

Fig. 2 Basic Structure of the Electric System (Union of Concerned Scientists, 2015)

The electric grid across the United States has some design reassurances that increase the reliability of the electric power supplied to consumers in case man-made accidents or natural disasters occur. This includes the fact that transmission lines are generally pulling energy from various energy sources (DoE, 2016). If one energy source fails, the other energy source will automatically supply the required energy to consumers. However, these original emergency reliability precautions were specifically designed to respond to traditional energy threats.

The threats to the power grid have evolved from traditional threats to non-traditional threats, such as physical and cyber attacks from non-state actors and possible hostile state actors. The continental energy-governing bodies have begun to implement reliability standards assisting in the prevention of and response to attacks on the energy grid (Lee, Assante & Conway, 2016). One such energy governing body is the North American Reliability Corporation (NERC), a:

> not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people (NERC, 2016).

NERC was recognized on January 1, 2007 and descended from the North American Reliability Council, which was established in 1968 (NERC, 2013). The original NERC was created in order to pursue electricity reliability standards in reaction to the U.S. Electric Power Reliability Act of 1967 (NERC, 2013). This legislation followed the most wide-spread blackout or wide-spread electricity failure recorded to date (NERC, 2013). On November 9, 1965 an immense blackout affected the Northeastern United States and Southeastern portions of Ontario, Canada. The U.S. legislation guided energy corporations to voluntarily create and enforce reliability standards,

which aim to ensure dependability by identifying risks to the BPS which in turn provides assurance to the consumer (NERC, 2016).

Critical Infrastructure Protection Standards

With the rise of non-traditional threats by state and non-state actors have become a critical national security issue, NERC had created the nine CIP standards that provide physical, personnel and cyber security regulations (Rouse, 2012). The nine standards are as follows: sabotage reporting, critical cyber asset identification, security management controls, personnel and training, electronic security perimeter(s), physical security of critical cyber assets, systems security management, incident reporting and response planning, and recovery plans for critical cyber assets (Subnet, 2016). These CIP standards were intended to allow energy corporations to identify and develop risk analyses for critical assets and implement safeguards to prevent and respond to the destruction of critical assets.

The first CIP standard pertains to sabotage reporting. The purpose of this regulation is to ensure any irregularities suspected of being sabotage are detected and reported to the pertinent systems, governmental agencies and regulatory entities (Subnet, 2016). This assists with the information flow of possible follow-on sabotage attacks, ensure that the appropriate personnel are trained to recognize and understand how to report possible sabotage attacks on facilities and multi-sites that have the possibility of effecting the larger interconnection (Subnet, 2016). For example, if a foreign entity is attempting to digitally sabotage a generating station the system should be able to apply associated processes to be able to identify and report the irregularity to the appropriate level of security and possibly prevent the sabotage from affecting the rest of the interconnection.

The second CIP standard is the critical cyber asset identification and protection policy. The purpose of this standard is not to identify every single cyber asset but to identify ones that could have an immense impact on the interconnection (NERC, 2010). This standard is designed to give energy corporations the initiative to provide the basis to be able to identify the effects critical cyber assets have on the interconnection and explore their vulnerabilities (Subnet, 2016). This provides an understanding of which cyber assets unique to each corporation are essential for the overall reliability of the BPS. NERC defines cyber assets as:

> Control systems comprising devices or sets of devices that act to manage, command, or regulate the behavior of processes, devices, or other systems; data acquisition systems comprising collections of sensors and communication links that act to sample, collect, and provide data regarding the facility's systems to a centralized location for display, archiving, or further processing; networking equipment including devices such as routers, hubs, switches, firewalls, and modems; hardware platforms running virtual machines or virtual storage (NERC, 2010).

This standard also instructs corporations to consider what role these critical assets play in the reliability equation, for instance consider if the critical cyber assets are able to provide real-time operation information or are able to connect to other cyber assets. This will help determine their roles, possible vulnerabilities and the effects on the BPS if they were compromised (NERC, 2010). For instance, if a non-state actor attempted to digitally attack one of the most critical cyber assets, the energy corporation and the interconnection would already have systems and

protocols in place that protect the critical cyber asset from such attacks and if the non-state actor was successful, the energy corporations would have the ability to quickly identify the possible repercussions of the attack on the BPS.

The third CIP standard concerns the security management controls. This standard is in place to direct energy corporations to have hard and soft documented security management controls that will protect critical cyber assets (Subnet, 2016). The requirements include ensuring proper cyber security policy, leadership, exceptions, information protection, and access control (Subnet, 2016). In general, this standard is to ensure physical security measures are in place and implemented and the protection of mission essential information such as floor plans to certain facilities and disaster recovery plans are afforded the appropriate classification and protection (Subnet, 2016). For example, if an agent of a foreign intelligence service was attempting to access innocent response protocol, they would likely be denied due to corporate leadership's confirmation that CIP-003 was implemented.

The fourth CIP standard is responsible for ensuring that individuals who have access to facilities that hold critical cyber assets receive the appropriate risk analysis, clearances, awareness and training (Subnet, 2016). This standard ensures that operators receive the appropriate training and awareness in order to be able to avoid sensitive information spillage. It also outlines that only stable, cleared personnel are able to access sensitive information through direct or indirect access (Subnet, 2016). For example, CIP-004 is designed to assist corporations with identifying the type of personnel who are qualified to work within the BPS and ensure those personnel obtain the appropriate follow on training. Another example is if an unauthorized individual attempted to access the facility absent the appropriate escort, NERC CIP-004 would stop the action, document the incident and report the information to the appropriate entities. It would ensure that a pattern would emerge if an un-cleared individual attempted to access multiple facilities unescorted.

The fifth CIP standard is the identification and implementation of electronic security perimeters for all areas holding critical cyber assets and the documentation of all access points (Subnet, 2016). The requirements include installing electronic security perimeters, electronic access controls, monitoring electronic access, conducting cyber vulnerability assessments, and maintaining all documentation regarding compliance is fully annotated and follows CIP- 002 guidelines (Subnet, 2016). In general, CIP-005 provides extensive documentation on individuals and time periods in which authorized individuals accessed certain areas and facilities. It would provide authorities the applicable evidence on access details to certain facilities and areas within those facilities in case an investigation was initiated.

The sixth CIP standard, CIP-006, is the chief standard on physical security principles. This standard ensures proper Standard Operating Procedures (SOP), documentation and implementation of the appropriate physical security measures in regards to critical cyber assets (Subnet, 2016). Main requirements of CIP-006 are the control of access, logging access, retaining access records and conducting maintenance and testing of physical security measures (Subnet, 2016). This standard is one of the basic standards which ensure the reliability compliance.

The seventh CIP standard is emplaced to assure corporations "define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using

reasonable business judgment" (Subnet, 2016). This standard requires entities to have a set methods and procedures for redeploying and disposing of critical cyber assets, installing anti-malware software, and other cyber security protection precautions.

CIP-008 is responsible for executing incident reporting and response planning (Subnet, 2016). It requires corporations to have and maintain an incident reporting plan which will allow the immediate report of physical or cyber attacks, disturbances, or other incidents (Subnet, 2016). It requires a cyber security incident response plan and cyber security incident documentation be in place for immediate use.

CIP-009 requires recovery plans are set in place in case a critical cyber asset attack is successful (Subnet, 2016). The standard obligates energy corporations to emplace and practice recovery plans, exercises, change control, backup and restore procedures, and testing backup media (Subnet, 2016). Personnel are required to confidentially know and understand these procedures. Multiple recovery plans must be available for use in determining the severity of the disturbance in reliability of the BPS. For instance, if a state or non-state actor was able to physically or digitally cause a blackout, each corporation must have a plan set aside to execute a black start, restoring power to a BPS, by relying on an internal transmission network (Knight, 2001).

Implementation and enforcement of these nine standards are critical for the reliability of the BPS. They provide the basic security measures to ensure critical cyber assets are protected and assist in the deterrence of physical and cyber disturbances or attacks against the power grid. Although NERC and the DoE have already implemented regulations and standards in order to ensure reliability, multiple vulnerabilities to the power grid still exist.

Case Study: Attack on Ukrainian Power Grids

One method of being able to identify the threats and possible vulnerabilities to the U.S. power grid system is by analyzing threats and attacks conducted in foreign states' power grid systems. The cyber attacks against multiple Ukrainian power grid systems is an incident that has been studied by U.S. corporations and inter-agency teams in order to better prepare the U.S. power grid for similar attacks. It is important to note that the attack on Ukrainian power grid systems was the first time a state or company to publically announce the hacking of their systems which resulted in loss of power to customers (E-ISAC, 2016). In late December 2015, a Ukrainian regional power provider, Kyivoblenergo, experienced power outages when a cyber attack against the company's "Supervisory Control and Data Acquisition (SCADA) distribution management system", which means the controls to circuit breakers to a substation, were remotely controlled and turned off (E-ISAC, 2016). After the substations were remotely turned off the attackers logged the operator personnel off of the control panel and changed their passwords so that the operators could not log back onto their systems (Zetter, 2016). This same type of attack method occurred simultaneously at two other power distribution systems which resulted in approximately 30 substations being taken off-line (Zetter, 2016). This automatically resulted in 225,000 customers without power for several hours (E-ISAC, 2016). The foreign attacker entity also disabled the backup energy systems for two of the distribution centers so that the power operators had also experienced power outages (Zetter, 2016). Although, the power outage only lasted a few hours the damage to the three oblenergos, Ukrainian power companies, was more extensive than originally announced (E-ISAC, 2016). The attackers also "impacted additional portions of the distribution grid and forced operators to switch to manual mode" (E-

ISAC, 2016). The damage to the distribution grid was so extensive, operators continue to provide energy through manual modes (E-ISAC, 2016). These attacks were coordinated to against the regional distribution centers, making the region in general susceptible.

These attacks were reported as sophisticated and well-coordinated attacks which were conduced almost simultaneously, approximately thirty minutes apart (E-ISAC, 2016). It is also reported that the attacker(s) were a well-resourced entity that likely had a structured team (E-ISAC, 2016). The attacking entity exhibited the ability of using multiple tactics, techniques and procedures (TTP) in order to navigate the digital structure and defenses of the regional distribution centers:

The attackers demonstrated a variety of capabilities, including spear phishing emails, variants of the BlackEnergy 3 malware, and the manipulation of Microsoft Office documents that contained the malware to gain a foothold into the Information Technology (IT) networks of the electricity companies. They demonstrated the capability to gain a foothold and harvest credentials and information to gain access to the ICS network. Additionally, the attackers showed expertise, not only in network connected infrastructure; such as Uninterruptable Power Supplies (UPSs), but also in operating the ICSs through supervisory control system; such as the Human Machine Interface (HMI)…. Finally, the adversaries demonstrated the capability and willingness to target field devices at substations, write custom malicious firmware, and render the devices, such as serial-to-ethernet convertors, inoperable and unrecoverable (E-ISAC, 2016).

The attackers also used denial-of-service (DoS) as they also flooded one of the power companies' customer service call center in order to deny actual customers from getting through to report the incident (E-ISAC, 2016). It is important to note that many initial reports of the attack suggested that the main power tool that disabled the power network was BlackEnergy 3 and KillDisk although these malwares were used to assist in the attack other software was utilized to gain direct remote control access of the software inside the control centers (E-ISAC, 2016).

As stated above these attacks involved extensive research, reconnaissance, development and synchronization. As the investigation in to the attacks became more extensive investigators in the private and governmental sectors discovered that the attacks had used the ICS Cyber Kill Chain which could be attended through open-source networks and was originally developed to enhance the original cyber kill chain developed by Lockheed Martin (E-ISAC, 2016). The new ICS Cyber Kill Chain was made public in 2015 and was developed by SANS Industrial Control Systems (E-ISAC, 2016). Reports indicate the hacking into electric power systems in order to conduct reconnaissance and steal critical information such as credentials began in March 2015 only months prior to the attack (E-ISAC, 2016).

A vulnerability to the Ukrainian power grid systems was the freedom to information about the power digital systems were made public knowledge (E-ISAC, 2016). The methods in which to conduct these types of attacks were also published on open-source networks creating the ease of access to resources and knowledge leading up to the attacks. The attackers followed through both of the dual stage ICS Cyber Kill Chain. In the first stage the attackers conducted extensive reconnaissance, which was undetected by the Ukrainian power companies, the next step was the weaponization of Microsoft Office products such as Word and Excel documents so that they had malware implanted within the documents in order to gain access to the power systems (E-ISAC, 2016).

The next steps in conducting a digital invasion include delivery, exploit and the installation of malware. The Microsoft documents allowed the malware to be delivered to the

electric companies, while the malware exploited the employees of the power companies by promoting the to able macros, as the employees unsuspectedly 'approved' malware into the systems, the malware began to install amongst the command and control (C2) IP addresses (E-ISAC, 2016). These steps in Stage 1 of the ICS Cyber Kill Chain enabled the attackers to initiate Stage 2 which consists of the actual cyber attack. Stage 2 involves five separate steps develop, test, deliver, install/modify, and execute attack (E-ISAC, 2016). During the development stage the attacks refined their own networks so as to leave as little forensic evidence as possible. Reports indicated that the test step was not conducted on the actual electric power systems but were likely conducted on a separate private network developed by the attackers (E-ISAC, 2016). The delivery step was conducted by using remote access to the power systems and the install/modify step modified the malware installed in Stage 1 by means of the remote control of systems (E-ISAC, 2016). The final step was to execute the ICS attack by the attackers accessing the SCADA systems in order to cripple the substations and instilling more long-term disablements to the control center systems (E-ISAC, 2016).

By understanding the development, components and methods to the attack against the Ukrainian power systems it enables the United States and other states to begin to provide modification to their systems, training to appropriate personnel and implementation of measures that complement the NERC CIP standards or even develop additional standards to the U.S. power grid digital systems. In the Ukrainian attack the hackers used spear phishing, credential theft, data exfiltration, VPN access, remote access to workstations, control of HMI, operation of sites controlled by the operator, tools and technology, hindering the response and restoration of oblenergos however the international community including the United States should learn from the tactics used by the Ukrainian attackers however, more importantly they should be concerned about how future potential attackers could modify these attack methods in order to access their power grid systems (E-ISAC, 2016). The redesign of methods is a dangerous tool in which the United States should designate resources and time into developing passive and active digital defenses.

Threats to the North American Power Grid

One such vulnerability lies within the very system that is in place if a blackout occurs. The black start method is designed to re-start power without any assistance from the power grid (Morris, 2011). A black start unit is a device such as a hydro-dam, gas turbine, diesel generator et cetera that can provide an initial form of energy (Morris, 2011). Each interconnection has its own designated black start plants, these plants are responsible for getting the interconnection back on-line in a timely manner (Morris, 2011). However, although CIP ensures black start plants are tested regularly to ensure they meet the standards to perform their required tasks in the event of a blackout, some of these plants have never undergone an actual black start (Morris, 2011). Another critical vulnerability is the energy governing bodies are relying on the assumption that a black start will work because the integrity of the power grid is still intact. In other words, if a terror organization were to damage or destroy the energy lines leading from the black start unit to the transmission lines the black start approach would be ineffective. This would lead to a massive blackout for an extended period of time. The question is how would interconnections get back online with a fragmented power grid? The black start method is the only contingency plan currently utilized in the U.S. power grid system. If the black start method fails, there are no other contingency plans.

A second vulnerability is that NERC and energy corporations have to be able to prevent a non-traditional threat, a reactive response would prove ineffective because electricity failure would still ensue. NERC understands this concept which is a partial reason why the CIP standards were implemented however in today's world of emerging threats NERC and energy corporations will not be able to prevent every single threat to the power grid. It is a daunting task in which NERC and government agencies have been trying to circumvent despite a limited budget and an ever evolving threat.

A third vulnerability is the interconnections themselves. The fact that most of the grids are interconnected makes it is easier to deny power to large areas if the integrity of the transference of electricity is compromised. The Texas Interconnection was sophisticated enough to ensure that most of its' state would have isolated energy systems separate from the Eastern and Western Interconnections. This safeguards Texas from being effected by a blackout from the other two interconnections. To diminish this vulnerability, each state would have to start separating themselves from their perspective interconnections and develop isolated energy systems within their states.

Policy Recommendations

Considering the emerging physical and cyber threats to the electric power grid, a number of policy recommendations should be considered, further developed and implemented. As discussed above one of the key elements in thwarting attacks against the power grid is detection and prevention. NERC should require electricity corporations to have assigned task forces or sections of operator managers that are solely dedicated to detecting cyber and physical intrusions into their specific areas of responsibility (AOR). These task forces should be broken down into smaller groups to ensure they are not overwhelmed with their AORs and can work as efficiently as possible. The goal of these task forces is to prevent and ensure possible adversaries do not access their networks to conduct reconnaissance, other fact-finding missions and instill the appropriate malware in order to steal information. A similar task force should be dedicated to halting attacks in progress.

A major issue that was observed in the attack on the Ukrainian power grid was the lack of information security (InfoSec). The ease of access to open source information related to the Ukrainian power grid systems and technology was a major single point of failure. It is recommended that NERC require a more need to know outlook on information shared with the public. The information about which and how many plants are designated for the black start process should also be kept to a minimum. Any information that could assist in critically crippling the power grids should be considered confidential.

Using a lessons learned approach to the Ukrainian attack should be fully implemented. Any advisory suggestions from the Department of Homeland Security, SANS or E-ISAC should be seriously considered and applied voluntarily to the multitude of energy corporations. The CIP standards focus on the reporting of issues but rarely address the actual response to traditional and non-traditional threats once they are detected. It is critical to understand that significant attacks to the power grid usually take months if not years to plan, conduct reconnaissance and apply. Developing resources that are able to detect these attacks will very likely make major contributions to thwarting future attacks.

The North American interconnections themselves pose a serious threat to the power grids. NERC should consider making each state independent of a regional power grid. Although

this would take significant financial requirements and take several years the outcome would comply with the cost-benefit ratio. The most critical issue is resolving methods for addressing alternatives to the black start approach. Also developing contingency plans for the possible scenario of the integrity of the power grid system being disabled. If a non-traditional threat were to gain knowledge of the locations to all the black start plants and the how to disable the integrity of links between the plants and the transformers, the damage could be significant and result in extended power outages. These two vulnerabilities will not be able to be remedied with a short term solution but be on an extended timeline in order to ensure the solutions are done correctly and in the most effective ways possible.

The Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) reported 295 security incidents against ICSs in the FY 2015 alone and concluded it was likely many more attacks occurred and were under-reported or undetected (NCCIC, n.d.). The NCCIC recommended a seven-strategy process in order to protect ICSs. The seven strategies include: implementing application whitelisting, ensuring proper configuration/patch management, reduce the attack surface area, build defendable environments, manage authentication, monitor and respond, and implement secure remote access (NCCIC, n.d.). The NCCIC states " simply building a network with a hardened perimeter is no longer adequate," and this is a concept that is slowly becoming a reality for many corporations not only in the electric sector but other sectors as well. The common vulnerabilities in the seven-strategy should be addressed by modern corporations and have significant resources toward diminishing those vulnerabilities (NCCIC, n.d.). These strategies and other strategies suggested from lessons learned from various other attacks should be a mandatory requirement for regional energy corporations and systems.

Conclusion

Safeguarding the North American power grid system is a constant and evolving task that is not only a convenience issue but also an issue of national security with immense political ramifications. After the terror attacks on September 11, 2001, U.S. citizens expect the government to play a more preemptive role in preventing attacks against U.S. citizens. These increased expectations are in line with a state-level theory's notion of democratic peace and how the mechanism of institutional constraints includes providing rule of law and satisfying public opinion (Kleinberg, 2016). Under the mechanism of institutional constraints providing rule of law, which in many public opinions is not only dealing with crimes and acts of terror after the fact but preventing terror attacks as well. This standard has rapidly taken place not only in the U.S. but throughout the globe. If states are not able to ensure the safety of their citizens through rule of law, economic stability and other assurances developed states begin to deteriorate. Overall, the gap between developed states and developing states would close ultimately creating an increasingly unstable international system.

Another political and national security aspect that lies within the security of the national power grid is as the U.S. continues to progress in its strategies to protect and prevent physical and cyber attacks on the power grid infrastructure, it is also uncovering new defensive and offensive strategies that could assist the Department of Defense and other federal agencies in possible future conflicts. As an extra advantage it is doing so ethically. They are not exploiting other states' power grids but instead acquiring knowledge from their own sophisticated power grid systems. Other techniques that are being utilized are the studying the events in other states

such as the recent Ukrainian blackout, thought to be implemented by Russia (Rockwell, 2016, p.1). In examining these events in detail, the United States can gain knowledge on other states' capabilities in regards to causing mass blackouts thus further preparing for specific types of attacks. NERC can also learn from successful and failed physical and cyber attacks on North American power grid systems.

As North America continues to prepare for and challenge emerging threats to the power systems, it is critical to recognize successes, failures and future resolutions. The NERC CIP standards have provided a foundation for North American states and corporations to address current and future threats however, in depth solutions to current vulnerabilities must be analyzed and implemented. The mind set of the energy community must change as well, it can no longer afford to have a traditional threat to reliability mindset. It must develop specified teams or task forces designed to solve specific non-traditional threats to the power grid system. Although changes to the energy community will likely have financial implications, the risk-benefit factor will ultimately satisfy current and future reliability requirements and national security requirements.

References

Department of Energy. (2016). Energy sources. Retrieved from http://energy.gov/science-innovation/energy-sources

Electricity-Information Sharing and Analysis Center. (2016). Analysis of the cyber attack on the Ukrainian Power Grid. Retrieved from http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

Kleinberg, H. *Technology and security module one* [PowerPoint Slides]. Retrieved from Lecture Notes UNCW Blackboard: https://uncwcas.uncw.edu/cas/login?service=https%3A%2F%2Fmyseaport.uncw.edu%2Fc%2Fportal%2Flogin

Knight, U.G. (2001, July). *Power systems in emergencies - from contingency planning to crisis management.* Retrieved from http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471490164.html

Lee, R.M., Assante, M.J., & Conway, T. (2016, January 5). *Analysis of the recent reports of http://ics.sans.org/search/results/analysis%20of%20the%20recen* t%20reports%20of%20attacks%20on%20US%20infrastructure%20by%20Iranian%20actors

Microsoft Encarta. (2004). [Image depicts the geographic separation of power interconnections]. National Power Grid. Retrieved from http://encarta.msn.com

Morris, L. (2011, July). Black start: Preparedness for any situation. *Power Engineering.* Retrieved from http://www.power-eng.com/articles/print/volume-115/issue-7/features/black-start-preparedness-for-any-situation.html

National Cybersecurity and Communications Integration Center. (n.d.). Seven strategies to Defend ICSs. Department of Homeland Security. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

North American Reliability Corporation. (2016). *About NERC.* Retrieved from http://www.nerc.com/AboutNERC/Pages/default.aspx

North American Reliability Corporation. (2013, August). *History of NERC.* Retrieved from http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf

North American Reliability Corporation. (2010, June 17) *Security guideline for the electricity sector: Identifying critical cyber assets.* Retrieved from http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf

Rockwell, M. (2016, March 9). *DHS widens warning about Ukrainian electric grid attack.* Retrieved from https://fcw.com/articles/2016/03/09/rockwell-ukraine-grid.aspx

Rouse, A. (2012, July). *NERC CIP*. Retrieved from http://searchcompliance.techtarget.com/definition/NERC-CIP-critical-infrastructure-protection

Subnet. (2016). *NERC CIP Solutions.* Retrieved from http://www.subnet.com/solutions/nerc-cip/cip-007-systems-security-management.aspx

Travis, J. (2012, September 6). *Who is NERC and FERC.* Retrieved from http://controlpowerconcepts.com/blog/who-is-nerc-and-ferc/

Union of Concerned Scientists. (2015). *How the electricity grid works*. Retrieved from http://www.ucsusa.org/clean-energy/how-electricity-grid-works#.VxJsisdllBw

Union of Concerned Scientists. (2015). [Image depicts the basic structure of the electric system]. Basic Structure of the Electric System. Retrieved from http://www.ucsusa.org/clean-energy/how-electricity-grid-works#.VxJsisdllBw

U.S. Energy Information Administration. (2016, April 6). How much electricity is lost in transmission and distribution in the United States. Retrieved from https://www.eia.gov/tools/faqs/faq.cfm?id=105&t=3

U.S. Energy Information Administration. (2015). *What is the electric power grid and what are some challenges it faces?* Retrieved from http://www.eia.gov/energy_in_brief/article/power_grid.cfm

Zetter, Kim. (2016). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired Magazine.* Retrieved from https://www.wired.com/2016/03/inside-cunning-Unprecedented-hack-ukraines-power-grid/