MIT MANAGEMENT
SLOAN SCHOOL

INTERDISCIPLINARY
CONSORTIUM
for IMPROVING
CRITICAL
INFRASTRUCTURE
CYBERSECURITY
(IC)^3

Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US

Abir Shehod

Working Paper CISL# 2016-22

December 2016

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Ukraine Power Grid Cyberattack and US Susceptibility:

Cybersecurity Implications of Smart Grid Advancements in the US

12/13/2016
MIT 22.811 Sustainable Energy

Abir Shehod

Contents

Abstract

Since the US electric grid has become more “smart” and interconnected, the threat of cyber-attacks has become imminent. The cyber-attacks on the Ukrainian power grid were the first publicly acknowledged incidents to result in power outages. The main question this paper will try to answer is whether the US is susceptible to a similar attack. This paper will take a look at the tactics, techniques and procedures (TTP) that were used in the attack, assess the possibility that something similar could happen in the US by looking at the smart grid technology enhancements, how prepared they are and what are the regulations that are put in place currently. The paper will also include criticism of the Department of Homeland Security’s handling of intelligence sharing to the energy sector and conclude with solutions and mitigation to prevent a cyberattack to the US grid.

Introduction

The US has invested heavily in upgrading its electric grid to provide benefits that include efficiency, reliability and remote access capability. However, the smart grid technologies and modernization of the grid, from generation to transmission to distribution, has unleashed an epidemic of largely IP-based digital technologies that are littered with security vulnerabilities. Many of these technologies are automated and wireless, adding endless opportunities to flood the electric grid's threat landscape.

On December 23rd, 2015 Ukrainian Kyivoblenergo, a regional electricity distribution company, was the first to experience a cyberattack that resulted in a power outage. Approximately 225,000 customers lost power. Starting at around 3:35 p.m. local time, seven 110 kV and 23 35 kV substations were disconnected for three hours. The cyber-attack impacted additional portions of the distribution grid and operators were forced to switch to manual mode. Three different distribution oblenergos (a term used to describe an energy company) were attacked. In addition, three other organizations, some from other critical infrastructure sectors, were also breached but did not experience operational impacts. [1]

With the US advancements to modernize and get more of a "smart" grid established, this attack is especially concerning. This paper will walk through the tactics, techniques and procedures used in the Ukraine attack, take a closer look at the state of the US grid by looking at its smart grid enhancements, how prepared it is to handle an attack that causes physical damage, and assess if the regulations that are currently in place are enough. The US handling of the

[1] Lee, Robert, Michael Assante, and Tim Conway. "Analysis of the Cyber Attack on the Ukrainian Power Grid." Electricity Information Sharing and Analysis Center & SANS Industrial Control Systems, March 18, 2016. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

intelligence of the Ukraine attack will be assessed and the paper will conclude with some solutions and mitigations to prevent a similar attack from occurring.

Ukraine Attack Breakdown: Tactics, Techniques & Procedure (TTP)

A team composed of representatives from the National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Computer Emergency Readiness Team (US-CERT), Department of Energy, Federal Bureau of Investigation, and the North American Electric Reliability Corporation traveled to Ukraine to investigate the attacks. The Ukrainian government collaborated openly with the U.S. team and shared information to help prevent future cyber-attacks.[1]

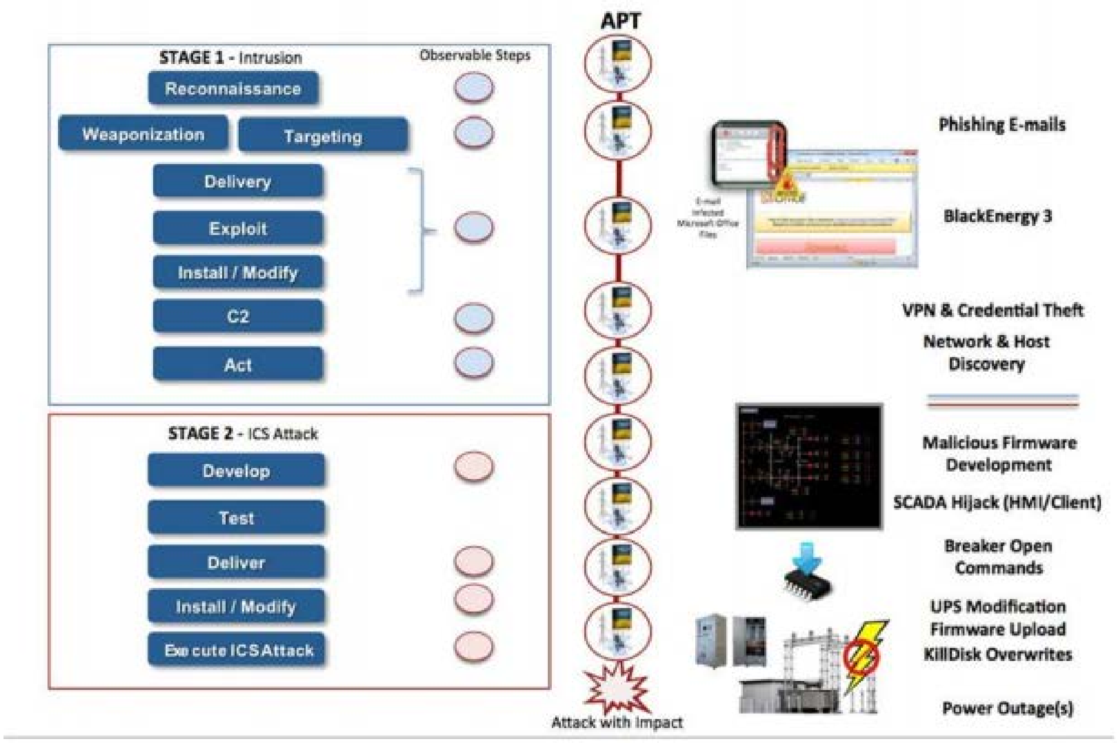


Figure 1 Industrial Control System Kill Chain Mapping Chart[1]

The cyberattack was extremely calculated and strategically planned. The entire attack from March 2015 – December 23, 2015 is graphically depicted above in Figure 1. The initial intrusion into the network was via spearphishing emails with malicious Microsoft Office attachments that began as far back as March 2015. When the personnel opened the document, a popup appeared asking the users to enable the macros in the document. Once the users enabled the macros, BlackEnergy 3 malware was installed on the victims' system. What's interesting to note is that the hacker's entry into the system wasn't through a vulnerability in the code of the devices that controlled the system but a vulnerability in Microsoft Office was ultimately their entryway into the network. The BlackEnergy 3 malware was used to create a communication channel to the adversary's command and control. Through this communication channel, the adversary was able to collect information from the infected system. The adversaries were allegedly in the system for 6 months before the attack occurred. While the adversaries were in the network they were able to perform their reconnaissance by collecting credentials and moving through the network to eventually pivot into the network segments where Supervisory Control and Data Acquisition (SCADA) dispatch workstations and servers existed. However, the SCADA networks were segregated with a firewall but this didn't halt the attackers assault. While in the corporate network, they were able to gain access to where user accounts for networks are managed, the Windows Domain Controllers. They were now able to find credentials for Virtual Private Network (VPN) access to remote into the SCADA network. Once they gained access, they were able to begin coordinating their attack.[1]

The hackers wanted to not only ensure that the power went off for customers, but that it was also difficult for the operators to recover from the outage. They reconfigured the uninterruptible power supply (UPS), that was responsible to provide backup power to two of the control centers. During the reconnaissance phase, the hackers studied each of the distribution managements systems for the grid. They coded malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations; the converters process commands sent from the SCADA network to the substation control systems. It is possible that the attackers gained these credentials, as they gained other legitimate credentials in the system, and used them to push malicious firmware versions to the devices. [1]

The hackers wanted to take out the converters so that it would prevent operators from sending remote commands to re-close breakers once the shutdown happened. In multiple instances, the attackers changed passwords for crucial systems so that valid users were unable to access the systems during the recovery process. Again continuing with the theme that the hackers were trying to make it more difficult for the operators to recover.[1]

Around 3:30 on December 23rd, 2015, the hackers were able to tap into the SCADA networks through the hijacked VPNs and send commands to deactivate the UPS system they had already reconfigured. In one instance, an internal telephone communications server was targeted effectively cutting off all internal communications with regional offices and distribution substations. At a different company, 30 minutes prior to the first unauthorized breaker operation, the actor used the local UPS to schedule a power shutdown of the main datacenter to occur a few hours later. In addition to standard consequences of power loss, a reboot caused the full impact of the KillDisk efforts to take effect. [1]

They launched a telephony denial of service (TDoS) attack against the customer call centers. The TDoS attack is similar to a Distributed Denial of Service (DDoS) attack that sends a flood of data to web servers. The hackers had flooded the system with thousands of fake calls, to prevent legitimate callers from being able to report the outage. The attacks on the UPS, converters and the call center all showed that the hackers strategically plotted the incident to cover all contingencies. Many experts echoed those opinions including Robert M. Lee, a former cyber warfare operations officer for the US Air Force and is co-founder of Dragos Security, a critical infrastructure security company who participated in the investigation, “It was brilliant. In terms of sophistication, most people always [focus on the] malware [that’s used in an attack],” he says. “To me what makes sophistication is logistics and planning and operations and what’s going on during the length of it. And this was highly sophisticated. What sophisticated actors do is they put concerted effort into even unlikely scenarios to make sure they're covering all aspects of what could go wrong."[2]

The hackers then began opening up breakers and took a lineup of more than a dozen substations off the grid. Then they overwrote the firmware on some of the substation serial-to-Ethernet converters, injecting their malicious firmware in place of the legitimate firmware causing the converters to be inoperable and unrecoverable. Once firmware has been rewritten, there's no going back to support recovery; not even with the help of the manufacturer. They were forced to replace the devices. The operators needed to be physically on site to manually switch any command. [1]

Once they neared the end of their assault, the hackers used KillDisk to wipe the files off the operator station's causing them to be inoperable. KillDisk is a piece of malware that wipes or overwrites data in essential system files that causes a computer to crash. The infected computers are unable to reboot because KillDisk also overwrites the master boot record. KillDisk was not executed against every system in the environment; however, management, HR, finance, and ICS operations staff and servers were targeted. There have been unconfirmed reports that the BlackEnergy malware was used to download and launch the KillDisk malware. There were also reports that there were was at least one instance where a Remote Terminal Unit (RTU) product with an embedded Windows HMI card (ABBRTU 560 CMU-02 - PLC Daughter Card) was overwritten with KillDisk.[2]

At 5pm, Prykarpattyaoblenergo posted a note to its web site acknowledging the power outage and reassuring customers that they were working to find the source of the problem. At 5:30pm

[2] 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/.

they posted a second note saying the cause of the outage was hackers; making it the first publically acknowledge cyberattack that caused a power outage. [2]

Ukraine's intelligence community is convinced the attack was orchestrated by Russia although there is no evidence or literature to proof it. Given the political unrest between the two nations, Russia was the likely perpetrator. Russia and Ukraine's relationship has been tense since Russia annexed Crimea in 2014 and Crimean authorities began to nationalize Ukrainian owned energy companies which angered Ukrainian owners. Also before the cyberattack, pro Ukrainian activists physically attacked substations that were providing power to Crimea. This left 2 million Crimean residents with no power in the area that Russia had annexed. It's been speculated that the Ukrainian cyberattack was retaliation for the attack on the Crimean substations. [2] Elizabeth Sherwood-Randall, deputy Energy Secretary, stated Russia was behind the attack to a gathering of electric power grid industry executives in February 2016. This, however, contradicts many top US Intelligence and security officials who feel that the evidence isn't conclusive enough to attribute the attack to the Russian government.[3] What's interesting to note is that if Russia is proven to be the culprit, the US could be vulnerable as relations with Russia and the US are not amicable either. Cyberwar between the two nations could become forthcoming as allegations of Russia's influence on US elections through cyberattacks and leaks are pointing in that direction.[4] Is the US grid capable of handling and recovering from a similar attack with how modernized and smart it's become?

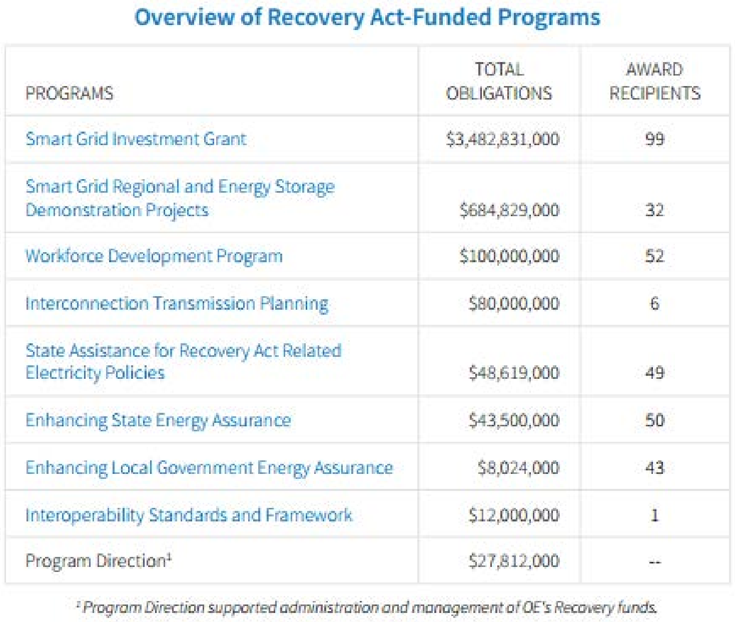
[3] Reporter, Evan Perez, CNN Justice. "U.S. Official Blames Russia for Power Grid Attack in Ukraine." *CNN*. http://www.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html.

[4] CNN, Tal Kopan, Kevin Liptak and Jim Sciutto. "Obama Orders Review of Russian Election-Related Hacking." *CNN*. http://www.cnn.com/2016/12/09/politics/obama-orders-review-into-russian-hacking-of-2016-election/index.html.

The State of the US Grid

Smart Grid Technology Enhancements

US Utilities have invested heavily in "smart grid" technologies, often with the assistance of federal grant money. To help modernize the US's aging energy infrastructure, the American Recovery and Reinvestment Act invested $4.5 billion in the electric sector which was matched by private funding to reach a total of about $9.5 billion according to a March 2015 Department of Energy report. See figure 2 for the overview of Recovery Act-Funded programs [5]



Overview of Recovery Act-Funded Programs

PROGRAMS	TOTAL OBLIGATIONS	AWARD RECIPIENTS
Smart Grid Investment Grant	$3,482,831,000	99
Smart Grid Regional and Energy Storage Demonstration Projects	$684,829,000	32
Workforce Development Program	$100,000,000	52
Interconnection Transmission Planning	$80,000,000	6
State Assistance for Recovery Act Related Electricity Policies	$48,619,000	49
Enhancing State Energy Assurance	$43,500,000	50
Enhancing Local Government Energy Assurance	$8,024,000	43
Interoperability Standards and Framework	$12,000,000	1
Program Direction[1]	$27,812,000	--

[1] Program Direction supported administration and management of OE's Recovery funds.

Figure 2: Overview of Recovery Act-Funded Programs[5]

[5] US Department of Energy. "ARRA GRID MODERNIZATION INVESTMENT HIGHLIGHTS - FACT SHEET," October 2015.http://energy.gov/sites/prod/files/2015/10/f27/OE%20ARRA%20Grid%20Modernization%20Highlights%20october2015_0.pdf.

The Office of Electricity Delivery and Energy Reliability are responsible for driving national efforts to modernize the electricity delivery system, enhance the security and reliability of America's energy infrastructure, and facilitate recovery from disruptions to the energy supply. According to the report 3.4 billion dollars went to help the industry "accelerate" the deployment of smart grid technologies that would help increase "reliability" and "efficiency" and reduce costs. The report even states that the "smart grid is helping reduce storm impacts, and restore service faster when outages occur." The utility companies are also outlined as being beneficiaries of the new enhancements stating that "smaller environmental footprint, reduced peak loads, and lower operational costs" are among the benefits.[5] However, security is mentioned twice in the report and it's not in the context of cybersecurity. The Department of Energy should have included a section in the report outlining how cybersecurity issues are going to be addressed. It seems very premature to be talking about the benefits of the "Smart Grid" without including the challenge of the increased attack surface that's being created simultaneously.

Unfortunately, the implementation of smart grid technologies and modernizing the US grid for sustainability and efficiency has left the US grid's attack surface wider and bigger than Ukraine's. Scott Aaronson, executive director for security and business continuity at the Edison Electric Institute, which represents large, investor-owned utilities said, "We had this rush to automation over the last 15 years or so, on some level almost blind to security risks we are creating. It is good we have automation, which gives us better situational awareness. But it also increases the attack surfaces." [6] Even with all the benefits outlined in the DOE report, implementing smart grid technologies into our grid is increasing its complexity and thus making

[6] Behr, Peter, and Blake Sobczak. "Utilities Look back to the Future for Hands-on Cyberdefense." The Hack, July 21, 2016. http://www.eenews.net/stories/1060040519.

it more vulnerable to attacks similar to Ukraine's. Therefore, it's essentially decreasing the grids reliability.

Preparedness for Physical Damage

The sophistication of the hackers shows that if they wanted to, they could have done much more physical damage than they did. In 2007, The Idaho National Laboratory ran the Aurora Generator Test which showed the physical damage that can be done if an adversary has the motivation and the means.[7] The experiment used a computer program that quickly opened and closed a diesel generator's circuit breakers out of phase from the rest of the grid and caused it to explode. The *Aurora Vulnerability* is especially concerning considering that much of the grid supports Modbus and other legacy communication protocols in the ICS world that were developed without any consideration for security. Legacy communication protocols do not support authentication, confidentiality or reply protection. This is extremely troubling considering that if a single generator fails, it could cause widespread outages and possibly cascading failure of the entire power grid. Even if there are no outages from this type of vulnerability, if a second attack or failure were to occur there would be the issue of replacing the generator or transformer. Replacing a high voltage transformer can be a logistical nightmare and can take up to a year to get one shipped from overseas. At the Ross Dam, moving out one of the old transformers took a crew of 15 men almost 12 hours and took nearly two years to prepare for the day. It can be concluded from this that if a physical failure were to happen to a transformer or generator, it would severely delay the recovery if a blackout were to occur. The Department of Energy and the Electric Power Research Institute worked on RecX,

[7] Zeller, Mark. "Myth or Reality – Does the Aurora Vulnerability Pose a Risk to My Generator?" Schweitzer Engineering Laboratories, Inc., April 2011. https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6452_MythReality_MZ_20110217_Web.pdf?v=20151124-153830.

which was a project to address shortening the time to transport and install a high voltage transformer in less than a week. In 2014, the RecX transformer was successfully installed in five days, 10 hours, and 10 minutes. [8] However, this is an isolated project and the government needs to ensure that every utility is prepared for a high voltage transformer replacement in order to decrease recovery time from a blackout.

Regulations

According to the Energy Policy Act of 2005, the electric power sector must follow the mandatory cybersecurity standards and regulations developed by the Federal Energy Regulation Commission (FERC). The FERC and the North American Electric Reliability Corporation work to create and implement enforceable standards that ensure the safety, reliability and security of the 450,000-mile network of U.S. electric generating plants and high-voltage transmission lines crossing the country. The detailed rules are validated by audits and potential $1-million-a-day fines if a serious breach occurs. The utilities industry uses S.C.A.D.A. to monitor and control tasks, processes and operations in a wide variety of settings, including chemical and electrical power generation plants, water treatment plants and dams. The NERC, Critical Infrastructure Protections (CIP), and Industrial Control System Computer Emergency Response Team (ICS-CERT) regulate these automated systems. While there has been significant progress on addressing known vulnerabilities in SCADA systems, the cybersecurity maturity of these systems is not catching up with the sophistication of the cyberattacks. [9]

Many experts believe that the regulations and standards set in place by these bodies are enough to protect the US from a Ukraine-like cyberattack. NERC CEO Gerry Cauley even went as

[8] Braun, Aryn. “Who Is Guarding the Grid?” *US News & World Report*, September 23, 2016. http://www.usnews.com/news/articles/2016-09-23/is-the-energy-grid-in-danger.

[9] “Cybersecurity Challenge: Protecting Electric, Power, and Utilities.” *National Cybersecurity Institute*, August 18, 2016. http://www.nationalcybersecurityinstitute.org/energy-utilities/cybersecurity-challenge-protecting-electric-power-and-utilities/.

far as saying the following at a Congressional hearing in April 2016, "Our security controls in North America are very different [from Ukraine's]. In the unlikely event of a successful cyber or physical attack, I believe that we are well prepared." [10] However, even though there are standards and regulations put forth it doesn't necessarily mean that organizations are enforcing, monitoring or updating them sufficiently which provides a vast gap and entry point for cyberattacks. Also the federal rules don't specifically apply to the local and regional US distribution utilities which was the segment that was attacked in Ukraine. Naturally, there are those that oppose the NERC CEO's view that the US is "well prepared". "It's my belief that we'll find a large number of smaller utilities certainly that are not CIP compliant because they are not required to be. That means that some of these power companies have the kinds of vulnerabilities that attackers preyed on in the Ukraine. Those are deficiencies that will need to be corrected to ensure we don't have those kinds of attacks," Duane Highley, an executive at an electric co-op in Arkansas and co-chairman of the industry's national cybersecurity coordinating committee.[11]

On the other hand, there is New Jersey that has most advanced state level cybersecurity policies in the US with requirements to state-regulated utilities to create programs to address cyber risk to critical systems, conduct risk assessment, practice response and recovery drills and report cyber incidents. "We feel very fairly confident that with what we have put in place here in New Jersey, what our companies are doing, there is a good chance our companies would have detected that threat," Mroz said. But he added, "I can't tell you with complete confidence

[10] *Hearing on Electric Grid Security*. CSPAN, 2016. https://archive.org/details/CSPAN3_20160414_140000_Hearing_on_Electric_Grid_Security?q=In+the+unlikely+event+of+a+successful+cyber+or+physical+attack%2C+I+believe+that+we+are+well+prepared.#start/5768/end/5828

[11] Behr, Peter, and Blake Sobczak. "Grid Hack Exposes Troubling Security Gaps for Local Utilities." The Hack. Accessed November 28, 2016. http://www.eenews.net/stories/1060040519.

it would have."[11] This is the problem when dealing with cybersecurity: no matter what protection mechanisms a utility puts in place; there is no such thing as absolute security. If there is a capable attacker with the correct means and motive; a utility can never be protected enough.

A report that was put together by the Federal Energy Regulatory Commission and the North American Electric Reliability Corp., reviewed nine registered U.S. utilities showed that all had detailed plans for responding to and recovering from a widespread blackout.[12] The nine utilities cooperating in the review were not named. However, continuing with the government and energy sectors unaligned messages, the report went on to give 102 pages of ways in which the recovery plans should be strengthened. The report included increasing emergency startup and battery backup capacity to bring up systems after outages. It also called for upgrading restoration plans to account for a major change on the grid, for instance power plant closings. Although the report states that plans exist for US utilities, there isn't sufficient information to support whether those plans have been tested and validated so that if an attack were to occur, the US utilities would be fully prepared. To gather more intelligence, NERC sent a confidential survey to power companies on whether they were defending against the tactics used in Ukraine and in July 2016, NERC began conducting compliance audits to get more information on the state of the grid. [11]

[12] "Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans." Federal Energy Regulatory Commission & The North American Electric Reliability Corporation, January 2016. https://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf.

US Grid Susceptibility to Ukraine Attack Methods

Spearphishing

The hackers were able to penetrate the corporate network via a spearphishing attack in Ukraine. In spring 2015, it took a "red team" of National Guard cyber experts 22 minutes to break the Snohomish County Public Utility District, north of Seattle. The utility company had invited them in to test the utility's defenses. "The cyberattack chain that the National Guard used against us, it's almost verbatim what happened in Ukraine," said Benjamin Beberness, the utility's chief information technology officer. In the national guard exercise and at the Ukraine power companies, employees thoughtlessly clicked on a phishing email with hidden malware that took the attackers inside the utility's business computer system. "It only took one click for somebody to get in," Beberness said. This furthermore proves the US susceptibility to this attack method. Once the national guard cyber experts were in the business network, they were able to navigate to the test operations network that replicated the Snohomish control system. The exercise triggered new cyberdefense strategies at Snohomish. [11]

Unfortunately, spearphishing is a commonly used technique. In the State of the Phish report prepared by Wombat Security, they surveyed security professionals from October 1, 2014 to September 30th, 2015 and 67% reported experiencing spear phishing attacks which is up 22 percent from 2014. Spearphishing was a technique also used in the widely publicized German steel mill attack that occurred in December 2014. The steel mill suffered massive damage after a cyberattack. According to the report, the attacker used spearphishing to gain access to the steel mill's office network, then manipulated and disrupted control systems to the degree that a blast furnace could not be properly shut down. [11]

Are US utilities safeguarded against spearphishing attacks? Unfortunately, no; in terms of regulations and standards. Even if US utilities are following the CIP requirements it wouldn't have saved them from a spearphishing attack because CIP rules don't apply to utility business systems. Once an attack has gained access to the corporate network there's no stopping them from finding a way to get into substations and other grid components as can be seen in the Snohomish test and the German steel mill attack. [11]

BlackEnergy

Next let's look at the presence of BlackEnergy in US Utilities. On January 11, 2016, DHS's high-level cyber response team, ICS-CERT, republished a 2014 warning about BlackEnergy malware. The ICS-CERT said that they had "identified a sophisticated malware campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware. Analysis indicates that this campaign has been ongoing since at least 2011. Multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs)." They also said they "cannot confirm" BlackEnergy played a role in Ukraine, but it "strongly encourages" U.S. companies with potential exposure to search for the cyber bug.[13] It can be concluded from these statements that if BlackEnergy malware was already identified to be in "numerous" ICS's environments then the US grid is not as secure as it should be. An adversary could already be lurking in US grid devices and utility systems.

Remote Access Capabilities

The Ukraine attackers used existing remote access tools or issued commands from a remote station similar to an operator HMI. One CIP requirement that could have protected the US if a similar attack occurred here is CIP-005. It requires systems covered by the rules to be protected within a regulated utility's "electronic security perimeter," with minimally controlled entry points. If operators need to have remote access to controls, they must go through multifactor

[13] "Ongoing Sophisticated Malware Campaign Compromising ICS." NCCIC/ICS-CERT, March 10, 2016. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

authentication. This means that they must provide two totally different forms of identification, such as a PIN plus a smart card or an iris scan device. [11]

Unlike the regulations set forth by CIP, the Ukraine utilities lacked multi-factor authentication which allowed operators to access grid controls remotely from outside computers and only required a single password. This made it easier for the attackers to gain credential information and move through the system. [11]

US utilities have far more remote access capabilities than the Ukrainian Utilities have. A number of the victims associated with the BlackEnergy campaign were running the Advantech/BroadWin WebAccess software with a direct internet connection.[11] This software is widely used in US utilities. Again, the regulations are set in place but there is no evidence to prove that US utilities are following the multifactor authentication requirement set by CIP. [9]

Serial-to-Ethernet Communications Devices

Moxa UC 7408-LX-Plus and the IRZRUH2 3G were the serial-to-Ethernet converters the attackers updated with their malicious code. The same models are used in the US power-distribution grid and there are many devices susceptible to these types of malicious firmware corruptions. More than five months after the Ukraine cyberattack, DHS posted a warning about a security vulnerability in a 7400-series Moxa device designed to translate serial communications in industrial environments to the modern Ethernet protocol.[14] The advisory ranked the severity of the vulnerability a 5.8 out of 10 stating that "crafting a working exploit for this vulnerability would be difficult". Although this advisory was for the same device that was exploited in the Ukraine attack, there was no mention of the connection to the attacks.

[14] "Moxa UC 7408-LX-Plus Firmware Overwrite Vulnerability." Advisory. Industrial Control Systems Cyber Emergency Response Team. https://ics-cert.us-cert.gov/advisories/ICSA-16-152-01.

Moxa has since stopped producing the UC 7408-LX-Plus device with the critical flaw. There were many in the security field that criticized the DHS's information sharing capabilities and connecting the dots for the general public. SAN's industrial cybersecurity expert Lee views were echoed across the industry," We know for a fact that the adversary took advantage of a vulnerability to overwrite the firmware on a Moxa device during a nation-state cyberattack on the power grid," he said. "And how does DHS classify it? 'It would take a really skilled attacker to do this, and we're giving it a 5 out of 10 for vulnerability rating.' What?"[15] Many of the alerts released by the DHS were inconclusive and provided the industry with a false sense of security following the Ukraine attack.

Telephony Denial-of-Service Attack

The attackers were very impressive in that they were able to attack two critical infrastructure sectors: Energy and Communication. The telephony denial of service attack that was conducted during the Ukraine blackout, was a wakeup call for the DHS to complete the National Cyber Incident Response Plan (NCIRP). A working draft of the plan was released in September 30th, 2016 but feedback is still being solicited.

"The attack in Ukraine gave us a taste of the threat to come," said Paul Stockton, managing director of Sonecon LLC and a former U.S. assistant secretary of homeland defense for the Defense Department. "That is just a small hint of the kinds of cross-sector attacks that may confront the United States."[14]

Proposals in June 2016 called for closer coordination of recovery plans by the communications, electricity and financial sectors. "What we focused on was the wake-up call that the Ukraine attack should provide to the United States, in that it reflected a simultaneous attack on the

[15] Sobczak, Blake, and Peter Behr. "How DHS Fell Silent When a Hack Threatened the U.S. Power Grid." The Hack, July 19, 2016. http://www.eenews.net/stories/1060040460.

communications and energy sectors," said Stockton, a co-chairman of the DHS advisory council subcommittee. "It is the kind of attack that will require very intense cross-sector collaboration, of the sort that the new NCIRP needs to help be able to provide," Stockton said.[16]

The Smart Grid Factor

Because the substations across Ukraine utilities' grid networks still had Soviet-era manual controls, crews were able to restore power by hand within six hours. In other words, it was the Ukraine’s lack of modernization in their grid that ultimately helped them recover quickly. The operators were able to drive out to where the breakers had tripped and fix the problem. The US grid is far more reliable on automation. This modernization could hinder the US’s ability to recover as quickly if a similar attack were to occur.

The damaging KillDisk that was used in Ukraine demonstrated how attackers could conceal malware that could re-emerge unless operators effectively cleansed their control systems. "If they were hiding in other places, they could still be there," Assante said. "If we didn't trust our electric substations and devices anymore, how do we deal with that? How would we bring it back? Those contingencies need to be considered." Michael Assante, Tim Roxey and Andy Bochman wrote a paper titled "The Case for Simplicity in Energy Infrastructure,"[17] published by the Center for Strategic and International Studies in which they argue that returning to older control methods will help protect the US energy infrastructure from cyberattacks.

[16] Braun, Aryn. “Who Is Guarding the Grid?” *US News & World Report*, September 23, 2016. http://www.usnews.com/news/articles/2016-09-23/is-the-energy-grid-in-danger.

[17] Assante, Michael, Tim Roxey, and Andy Bochman. “The Case for Simplicity in Energy Infrastructure For Economic and National Security.” Center for Strategic & International Studies, October 2015. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf.

"The old analog relays and circuit protection devices were as reliable as the day was long," wrote the authors. However, these claims are yet to be validated. The "Securing Energy Infrastructure Act," co-sponsored by Sen. Jim Risch (R-Idaho), chairman of the Senate Energy and Natural Resources Subcommittee on Energy, would task the Department of Energy's national laboratories with testing "analog and nondigital" control systems' ability to withstand remote cyberattacks. The legislation would provide $11.5 million to study the issue. [18]

"For every major piece of grid equipment, hundreds of digital devices have evolved to support it," the authors wrote. "Remote terminal units, intelligent electronic devices, programmable logic controllers, distributed control systems, field programmable gate arrays: these are specialized computers with circuit boards, memory chips, and communications circuits, the parts sourced from innumerable suppliers, and animated via instructions coded in software. And while the hardware brings loads of complexity, it's in software that complexity truly runs wild."

One suggestion that was made in the paper was to put more humans and nonprogrammable backup controls into systems on the most important parts of the power grid. The paper mentioned how utility systems were run by people like "Fred" who used to sleep at the substation with his dog. Give him an instruction to change a setting, and Fred would do it.

To defeat skilled cyber attackers, the most important grid components may need to rehire some "Freds" or create the equivalent with controls that are totally isolated from outside entryways, the authors argue. The authors make a great point, with complexity comes more vulnerabilities. It may be time for the US Utilities and manufacturers to consider slowing down modernization and getting back to the basics to protect the grid from cyberattacks. Unfortunately, the moment a form of connectivity is introduced to a device, its vulnerable to be

[18] Behr, Peter, and Blake Sobczak. "Utilities Look back to the Future for Hands-on Cyberdefense." The Hack, July 21, 2016. http://www.eenews.net/stories/1060040519.

attacked. Protection mechanisms can be put into place to help reduce the likelihood for a successful attack but it’s still vulnerable.

There are also those in the industry that oppose returning to manual mode as a cyberdefense. Cris Thomas, a strategist at Tenable Network Security who also goes by the hacker name "Space Rogue, called the move “a step backward”. "It just seems like we're spinning our wheels looking at this old stuff when we should be looking at the new," he said. This is true there are many practices that can be applied to critical infrastructure systems and those that manufacture the devices. Utility companies can apply better patches and manufacturers can consider security during the development of the devices by deploying Secure Development Lifecycle activities. The activities would include developing cybersecurity requirements, implementing them and testing the devices for robustness.

Scott Aaronson, executive director of security and business continuity for Edison Electric Institute, believes that the history of the grid is what will protect it. "This is a grid that grew up over quite literally 100 years," Aaronson said. "There is any number of redundancies throughout the system, so taking out one or two or 10 nodes is not going to have the impact that you'd think it's going to have where the lights go out for 18 months." However, as noted earlier, if a transformer is taken out, lights out for 18 months could be possible.

Still, vulnerabilities exist throughout the grid. Covering the entire country and parts of Canada, the grid is a network of more than 7,000 power plants, hundreds of thousands of miles of high-voltage transmission lines and upwards of 55,000 substations.[19]

[19] Braun, Aryn. “Who Is Guarding the Grid?” *US News & World Report*, September 23, 2016. http://www.usnews.com/news/articles/2016-09-23/is-the-energy-grid-in-danger.

Criticism of the US Government Intelligence Sharing

An intelligence assessment was released on January 22nd, 2016 by Homeland Security's Office of Intelligence and Analysis with coordination from the Industrial Control Systems Computer Emergency Response Team (ICS-CERT). [20] The assessment concluded that the threat of a damaging or disruptive attack against the US energy sector is low. The assessment went on to state that "advanced persistent threat (APT) nation-state cyber actors are targeting US energy sector enterprise networks primarily to conduct cyber espionage. The APT activity directed against sector industrial control system (ICS) networks probably is focused on acquiring and maintaining persistent access to facilitate the introduction of malware, and likely is part of nation-state contingency planning that would only be implemented to conduct a damaging or disruptive attack in the event of hostilities with the United States." This statement seems to be counterproductive. How can DHS release a statement saying that they believe the threat is low when as noted in the timeline of events, the attackers were in the system for months for reconnaissance purposes which eventually lead to the attack. What is the most disturbing out of this statement that was made by the DHS is the part that says that the US would only get attacked if it becomes hostile with a nation state actor. The US currently has a significant number of nation state actors that have plenty of motives to want to attack the one infrastructure that keeps a country running: The Electric Grid. The threat is not low; it's extremely high. The second key judgement made in the assessment was that "the majority of malicious activity occurring against the US energy sector is low-level cybercrime that is likely opportunistic in nature rather than specifically aimed at the sector, is financially or ideologically motivated, and is not meant to be destructive."[15] They classify that the majority of the malicious activity is considered low level crime because its financially or Ideologically

[20] "DHS Intelligence Assessment: Damaging Cyber Attacks Possible but Not Likely Against the US Energy Sector." Homeland Security, January 27, 2016. https://publicintelligence.net/dhs-cyber-attacks-energy-sector/.

motivated? All it takes is for a nation state actor or even regular hacker sitting in his mother's basement to be financially, ideologically or politically motivated for them to consider attacking United States grid infrastructure.

They clearly stated that the Ukrainian Cyber-attack "does not represent an increase in the threat of a disruptive or destructive attack on US energy infrastructure". Fast-forward a few weeks later and the tone completely changes. The DHS begins releasing a series of warnings to electric utilities and other US critical infrastructure operators. DHS's conflicting messages and drawn out delivery of information to the energy sector, drew criticism of their competency to deliver lessons learned and attacker's technique information in a timely matter to the impacted sectors. Many of those in the cybersecurity community echoed the same stance. "There was a credible threat to the U.S. grid, with realistic mitigations that could have been applied, and instead [DHS] decided to sit on the information," said Robert M. Lee, founder of Dragos Security LLC and a co-author of an influential SANS Institute analysis of the Ukraine case. "In the midst of the first attack on a power grid that was public, there was no public word from the government," he said.

Solutions and Mitigations

Although the DOE and DHS has been criticized for their distribution of information for the Ukraine attacks, they are taking the necessary steps to help improve cybersecurity in the energy sector. In August 2016, the Department of Energy requested up to $34 million in appropriations for 12 projects in nine states, including Washington, to improve grid resiliency through cybersecurity research. [21] A NCCIC/ICS-CERT Incident Alert was released on March 7, 2016

[21] Department of Energy. "Fact Sheet: DOE Award Selections for the Development of Next Generation Cybersecurity Technologies and Tools," August 2016.

where they stated that “critical infrastructure ICS networks, across multiple sectors, are vulnerable to similar attacks. Asset owners should take proactive steps to prevent similar attacks from impacting their own systems.”[13] The alert outlined a number of mitigations.

Employee Cybersecurity Awareness

Notably missing from the mitigations outlined in the alert was employee cybersecurity awareness. Since spearphishing relies heavily on exploiting the human factor, it’s important to educate operators and even corporate personnel to not open emails and click on attachments unless they are 100 percent confident that they trust the content.

Contingency Planning

The Ukrainian companies did not have a contingency plan in place but they were able to recover quickly because of their comfort with manual operation. In contrast, US infrastructure is more reliant on automation so a comprehensive contingency plan should be developed to allow for the safe operation and/or shutdown of operational processes if a cyberattack were to occur.

To help prevent the telephony denial of service attack that blocked communication from customers to the Ukrainian utilities as well as internal communication, organizations should be prepared on how they would respond to such an event. Upstream telephony service providers should be contacted to provide technical controls which decrease the impact of a similar attack. For forensic review, utilities should consider appropriate logging and voice recordings. Network diagrams should be properly documented and safeguarded. Organizations should consider all the devices in the system and which have network connectivity. An inventory of devices,

http://energy.gov/sites/prod/files/2016/08/f33/CEDS%20award%20selections%20August2016%20fact%20sheet%20FINAL_1.pdf.

especially smart devices should be taken and security features of those devices should be considered.

Configure ICS Networks Securely

Unfortunately, many ICS networks add smart devices to their systems without considering the impact these devices might have on the network. Before introducing these devices, organizations should isolate ICS networks from any untrusted networks, especially the Internet as seen in Figure 3. The figure shows the corporate network and the control systems network on separate networks. It also shows that a DMZ or demilitarized zone should be set up for the corporate infrastructure components such as the email and web server as well as a separate one should be set up for the control system network. Any unused protocol ports should be locked down and all unused services turned off. The objective is to decrease the number of entry points that an attacker can use to sabotage the system. Separate credentials should be made for the ICS network and the business network to prevent what happened in the Ukraine

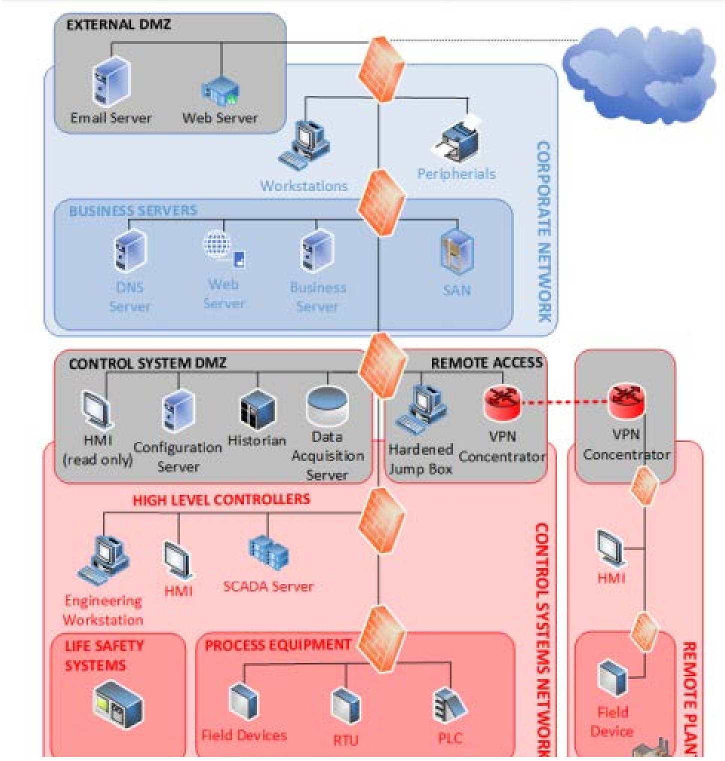


Figure 3: Ideal ICS Network Configuration[1]

attack where the attackers leveraged credentials that they gained from the enterprise network to attack the control system.

Limit Remote Access Functionality

Although it seems the general public and the ICS industry is moving in the direction of modernization which can easily be translated to convenience, one recommended mitigation is to limit remote access functionality. Remote access should be operator controlled, time limited, and logged.

Credential Monitoring

If credential monitoring was a practice used in the Ukraine utilities, it’s possible that the attacker’s presence in the network would have been detected. Credential monitoring should be used to identify compromised credentials being used by unauthorized attackers. One of the Ukraine attackers’ first task when they were in the system was creating new unauthorized domain accounts and granting them certain privileges. If credentials were monitored and the network was monitored for unusual activity, system administrators would have been alerted before the attack took place.

Network Security & Monitoring

Unlike Ukraine’s Soviet era infrastructure, many US utilities use modern IT tools and devices. Firewalls, externally facing interfaces, and wireless access are among the technologies that are widely present in US systems. However, this presence makes US extremely susceptible to a Ukraine-like cyberattack as those components may have security vulnerabilities in them that attackers can leverage. Organizations should consider any newly added devices to the network and ensure the vendor has done the necessary penetration testing to ensure critical vulnerabilities are not present.

The lack of network monitoring in Ukraine assisted the attackers in being able to maintain their presence in the system without being detected. Administrators are encouraged to create a trusted profile of their network traffic and use it as a baseline to detect unusual activity on the network. If there is traffic from an IP address that shows unusual behavior occurring during odd times, special attention should be paid to eliminate access. Intrusion detection systems should be trained to recognize anomalies to normal behavior, and the proper personnel should be notified if abnormal activity is detected, such as local accounts being used to access systems from remote IP addresses. Figure 4 shows an example of a malicious firmware update to an industrial network switch. Even without knowing the baseline of normal activity, which defenders should have, it can be trivial to spot firmware updates in network data. As depicted in the graph, there is a clear spike in abnormal activity that should be investigated further if seen.

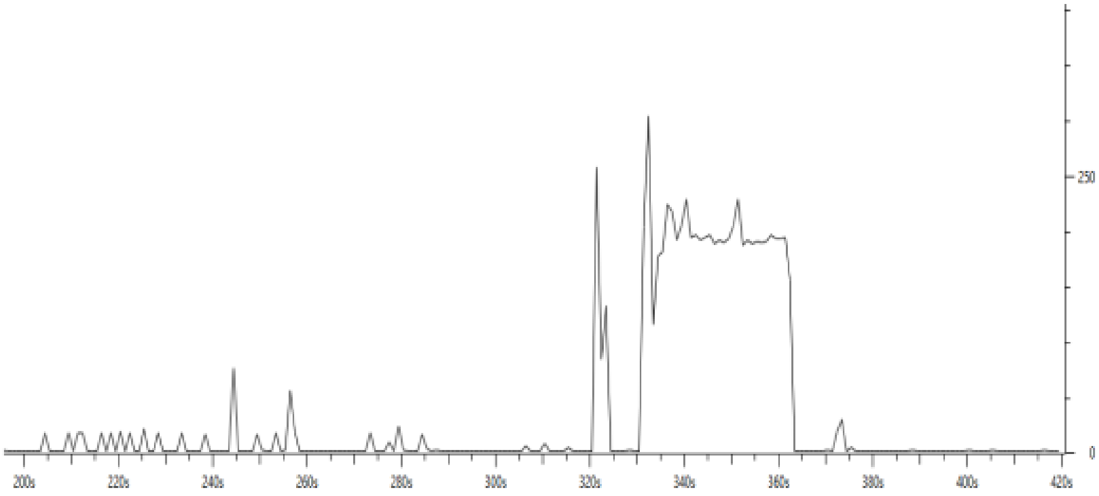


Figure 4: Sample Network I/O Data from a Malicious Firmware Update to an Industrial Ethernet Switch[1]

Security experts believe the US is not utilizing Network Monitoring tools as much as they should be. "A capable monitoring program could have spotted all the abnormal computer traffic secretly traveling back and forth between the attackers and the Ukraine systems they had infected, months before the final attack, said Jake Williams, founder and principal consultant at

Rendition InfoSec LLC, who has analyzed some of the Ukraine attackers' malware. "Few U.S. utilities do it now. It's the exception we see and not the rule." [22]

CIP-007 requires that regulated utilities "deploy method(s) to deter, detect, or prevent malicious code."[23] However, the rules don't specify how. That puts the responsibility on each utility to figure out how to do this and be able to show NERC-approved auditors that they are meeting these requirements. This is a gap that many security experts feel needs to be addressed to include specific detail on how to execute the requirement.

Michael Assante of the SANS Institute is one of them. "You need to look at anything trying to communicate out. We find that isn't very commonplace" in the United States. "There is a requirement to conduct secure monitoring. It's not very prescriptive about what needs to be monitored, and how. So there is a blind spot." [18]

Multifactor Authentication

The Ukraine companies lacked multi-factor authentication mechanisms that allowed attackers to easily gain access to key systems. Strong multi-factor authentication should be implemented whenever possible in the system, especially on externally facing connections. The tokens used should be from different categories (something you know, something you have, something you are). While not a holistic solution, it makes it harder for attackers to gain access because now they need to come up with two forms of credentials.

[22] Behr, Peter, and Blake Sobczak. "Grid Hack Exposes Troubling Security Gaps for Local Utilities." The Hack. Accessed November 28, 2016. http://www.eenews.net/stories/1060040519.

23 "CIP-007-5 Cyber Security — System Security Management." North American Electric Reliability Corporation, n.d. http://www.nerc.com/files/CIP-007-5.pdf.

Firmware Driver Signing

Firmware Driver signing provides an important layer of protection against malicious drive and any firmware overwrite like what was seen in the Ukraine attack. Requiring signed drivers prevents malicious drivers from being loaded on devices, and alerts to malicious activity on a network. New devices that are added to the system should be fully evaluated with the vendor on their security features and ensure that firmware driver signing is a feature offered.

Application Whitelisting

Application Whitelisting (AWL) can detect and prevent malware execution, such as BlackEnergy 3 used in the Ukraine attacks. AWL can be used on database servers and HMI computers. Operators should collaborate with their vendors to baseline and calibrate AWL deployments. If AWL was in place in Ukraine attacks, the spearphishing emails would have been deterred because alerts would have been sent if malicious malware such as BlackEnergy was detected. Alerts should be established when applications commonly used in cyber-attacks are attempted to be loaded on any system. Even if BlackEnergy was not detected, the KillDisk malware was executed as a separate binary and, therefore, would have been prevented from running by AWL.

Conclusion

Unfortunately, the answer is yes. It can be concluded from the literature if there's a nation state actor or even a curious hacker, they will likely be successful in taking down some portion of the United States grid. If physical damage is done to destroy a transformer, logistically most US utilities are not prepared to replace it in a timely matter. The interoperability issues of using legacy communication protocols that don't support authentication, confidentially of reply protection adds to the US susceptibility to a cyberattack. Although the US has set cybersecurity regulations for the energy sector, that doesn't necessary mean they are enforced, monitored and continuously updated to keep up with the maturity of attacks. The regulations set forth also lack details on how to execute which needs to be documented thoroughly. There's also the gap of not catering federal rules specifically to local and regional US distribution utilities which was the targeted segment in the Ukraine attacks. In terms of the US susceptibility from the Ukraine attack TTPs that were used, the Snohomish County Public Utility District test showed that operators are likely to click on malicious attachments, BlackEnergy has been found to be lurking in US utilities, remote access capabilities that lack multi-factor authentication are used frequently in US utilities, the same Serial-to-Ethernet communication devices that were vulnerable to the Ukraine attack are found in many US Utilities, and finally to prevent a telephony denial of service attack requires coordination with the communication, electricity and financial sectors that doesn't currently exist.

In terms of the "Smart Grid Factor", the problem with adding more connectivity and smart devices to the grid is that it's becoming more and more difficult to trust the devices. For instance, the damaging KillDisk used in the Ukraine attack was in the system for months until the hackers executed the call and once it was executed there's no turning back to recover. How can these devices be trusted when they are rigged with malware and a plethora of security vulnerabilities as security wasn't considered when developing the devices? There were two arguments given in terms of the use of smart devices; to modernize more or to take a step back and return to the analog devices with one-way communication that lacked connectivity to the internet. Although, valid points were made that a device can't be hacked if it lacks the "smart" factor, the US has invested billions already in modernizing the grid making it too late to turn back time. There needs to be a balance of modernization and security where security is priority especially in critical infrastructure systems. The DHS also needs to improve their intelligence sharing with the energy sector. The mixed messages, delayed reports and lack of information showed how unprepared and uncoordinated the different US agencies are for an attack.

Overall the US is in better shape than other countries but there is still a long way to go. Everything that humans do is dependent on having electricity and sustaining it. Making devices smarter on the grid help improve efficiency by providing us with two-way communication to assess the environment. It is unfortunate that the same technologies that are hurling us in the direction of modernization could perhaps take us back to the stone ages if a significant cyberattack were to occur.

Literature Criticism

Most of the paper referenced government issued documents or alerts. I found that the *Analysis of the Cyber Attack on the Ukrainian Power Grid* document produced by E-ISAC and SANS was very comprehensive and useful in the breakdown of the attack and with mitigation recommendations. I didn't find literature that showed proof that Russia was involved in the Ukraine attack but that would have been the smoking gun. I could only cite US officials that claimed their involvement and many news article references including the Wired article that I used that used terms like "allegedly". However, that shows how easy it is to get away with a cyber-attack because it's difficult to find accountability when it happens. The Department of Energy released a factsheet title *ARRA GRID MODERNIZATION INVESTMENT HIGHLIGHTS - FACT SHEET* and it highlighted all the great benefits of Smart grid enhancements but as mentioned in the paper, there was no mentioned of how cybersecurity is going to be addressed. I went into detail in the paper about how inconclusive and confusing the alerts that were sent out by Homeland Security. Considering that intelligence sharing is extremely important to help the US mitigate a similar attack, DHS should consider restructuring their alert system and providing more accurate and clear messages to the energy sector. The report that was especially confusing was sent out by Homeland Security titled *DHS Intelligence Assessment: Damaging Cyber Attacks Possible but Not Likely Against the US Energy Sector.* The document had false and mixed messages that I outlined in detail in the section "Criticism of US Intelligence Sharing". There weren't any decent thesis level papers available to reference on the Ukraine attack but that is expected as it is a fairly recent event. I used a lot of quotes from experts in the field which I felt helped support my conclusions and compensate for the lack of thesis work on the topic. The quotes from experts also compensated for the lack of statistical data that was available on the possibility of an attack. A risk assessment that showed the state of the US grid in terms of its cybersecurity posture was also missing. As mentioned in the "Regulations" section of this paper NERC began conducting compliance audits to get more information on the state of the grid in July 2016. It would have been great if NERC would publish a summary of the results from that audit. I would have liked to see research or a study done on comparing a utility that utilizes smart technology versus a utility that doesn't and assessing their susceptibility to a cyberattack. It's difficult to make assumptions that an attack could happen when it hasn't happened yet; literature that provided a risk assessment or included a probability of attack would have supported my conclusions better. It would have been better to find statistics that were catered to ICS; for instance, I wanted to find information on the probability that an operator clicks on a spearphising email. Instead, I was able to find statistics about the broader landscape that wasn't specific to the ICS world but still sufficient enough to prove my point. Likely the omissions of this ICS specific data could be correlated as being part of the problem. Without intelligence and studies on the current state of the sector, US Utilities cannot protect their infrastructure to their utmost ability.

Glossary

Electric Grid: a network of synchronized power providers and consumers that are connected by transmission and distribution lines and operated by one or more control centers. When most people talk about the power "grid," they're referring to the transmission system for electricity a network of synchronized power providers and consumers that are connected by transmission and distribution lines and operated by one or more control centers. When most people talk about the power "grid," they're referring to the transmission system for electricity.

Spearphishing: an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data.

Macros: A symbol, name, or key that represents a list of commands, actions, or keystrokes. Many programs allow you to create macros so that you can enter a single character or word to perform a whole series of actions.

SCADA (Supervisory Control and Data Acquisition): a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery.

Windows Domain Controller: On Microsoft Servers, a domain controller (DC) is a server computer that responds to security authentication requests (logging in, checking permissions, etc.) within a Windows domain.

Virtual Private Network (VPN): a method employing encryption to provide secure access to a remote computer over the Internet.

Uninterruptible Power Supply (UPS): a device that allows a computer to keep running for at least a short time when the primary power source is lost. It also provides protection from power surges.

KillDisk: a powerful and compact software utility that can completely and securely destroy all data on hard drives, removable disks, and flash media devices, without the possibility of future recovery

Telephony Denial of Service: a flood of unwanted, malicious inbound calls.

Distributed Denial of Service: attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.

Remote Terminal Unit (RTU): a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects

Application Whitelisting (AWL): Application whitelisting is a computer administration practice used to prevent unauthorized programs from running. The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for resources.

DMZ or demilitarized zone: a physical or logical subnetwork that contains and exposes an organization's external-facing services to a usually larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.