Cyber-Security Vulnerabilities: Domestic Lessons from Attacks on Foreign Critical Infrastructure

Anthony Moreno

Dr. Petter Lovaas[1]

Abstract:

Technology, and its increasing integration in today's world, have created new threat vectors that were previously unheard of. Although this technology integration streamlines efficiencies and improves communication, its usage can have grave consequences when not properly secured or hardened against cyberattacks. This can be especially true when considering our nation's critical infrastructure systems. Critical infrastructure systems and networks support a vast array of related services that help shape our modern society. Power grids, hospitals, and educational institutions are just some examples of critical infrastructures. Examination of past cyberattacks on foreign critical infrastructure systems will help identify lessons learned and be used to recommend defense in depth approaches and solutions to this challenge.

Keywords: *Cyber security, critical infrastructure*

PRESIDENTIAL POLICY DIRECTIVE (PPD) 21 WAS written to promote the safety and security for the United States' critical infrastructure.[2] Protecting critical infrastructure is increasingly difficult as malicious actors continually pose a threat. In the modern age, nearly all industries and government services now incorporate mission and business critical devices that connect and interact with various public networks. As a society we have come to especially rely on various critical infrastructures that utilize these shared computer networks. Critical infrastructures are formally defined as "the basic facilities, services, and installations needed for the functioning of a community or society".[3]

All United States critical infrastructure sectors currently employ controls over networks for their operation. Supervisory Control and Data Acquisition (SCADA), Internet of Things (IoT) monitors, and other internet-connected computer systems are all used to ensure smooth and efficient operations of their various functions. Countless SCADA systems are deployed worldwide and are used to provide a means to identify and rebound from system faults and other mechanical

[1] Department of Computer Information Sciences (CIS), Niagara University, 5795 Lewiston Rd, New York 14109. amoreno@mail.niagara.edu (Moreno) and plovaas@niagara.edu (Lovaas).

[2] Interagency Security Committee, "Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper," February 2015, https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf.

[3] Wendy Steele, Karen Hussey, and Stephen Dovers, "What's Critical about Critical Infrastructure?," *Urban Policy and Research* 35, no. 1 (2017): 74-86, DOI: 10.1080/08111146.2017.1282857.

failures.[4] The IoT, on the other hand, is not limited to industrial controls, but rather is a general term for various embedded technology devices "and their logical representations [within our] information systems".[5] Frequently these same monitors, systems, and networks, are not sufficiently hardened against cyber threats.

With the internet now connecting numerous countries and malicious actors alike (often without clear attribution), cyberattacks can have a significant impact on political and governmental institutions. Our study is qualitative in nature and explores at depth our nation's critical infrastructures, past successful cyberattacks, and the current steps being taken to harden critical infrastructure networks and computer systems. We conclude by identifying and designing a holistic method for critical infrastructure protection, utilizing a defense in depth approach.

1) Literature Review:

Defining Critical Infrastructures:

Critical infrastructures are responsible for providing the required services and functions that modern life and society have come to rely and depend on. In the United States specifically, the Department of Homeland Security defines 16 critical infrastructure sectors that include a wide range of different industries.[6] Although not an exhaustive list, these industries include the chemical sector, the energy sector, the food and agriculture sector, and the government facilities sector.[7] The importance of each critical sector cannot be understated. The Department of Homeland Security explains that each sector is "so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, [and] national public health [and] safety".[8]

Many of the industries that compose critical infrastructure systems require the constant observation of a myriad of controllers and devices "to ensure [their] proper [and continuous] operation".[9] Operational requirements have transformed critical infrastructure systems "into complex networks that support communication between a central control unit and multiple remote units".[10] These remote units often are not computers, but rather an IoT or SCADA device.

Defining SCADA:

Although IoT devices are primarily found in consumer-based products and homes, SCADA controllers are especially prevalent in the implementation and operation of large Industrial Control System (ICS) devices and processes. In order to provide improved central control and monitoring over great distances, SCADA controllers and the networks they reside on are commonly placed on publicly connected networks.[11] However, the improved communication allotted with connecting SCADA networks to the public internet comes with risks.

---

[4] A. Nicholson et al., "SCADA security in the light of Cyber-Warfare," *Computers & Security*, 31, no. 4 (2012): 418-436, https://doi-org.ezproxy.niagara.edu/10.1016/j.cose.2012.02.009.

[5] Daniel Minoli, *Building the Internet of Things with IPv6 and MIPv6 : The Evolving World of M2M Communications*, (Somerset: John Wiley & Sons, Incorporated, 2013), 2, https://ebook central.proquest.com/lib/niagara-ebooks/reader.action?docID=1216195&ppg=21.

[6] "Critical Infrastructure Sectors," accessed March 30, 2019, https://www.dhs.gov/critical-infrastructure-sectors.

[7] Ibid.

[8] Ibid.

[9] Vinay Igure, Sean Laughter, and Ronald Williams, "Security issues in SCADA networks," *Computers & Security*, 25 no. 7 (2006): 498-506, https://doi-org.ezproxy.niagara.edu/10.1016/j.cose.2006.03.001.

[10] Ibid.

[11] Nicholson et al., "SCADA security in the light of Cyber-Warfare."

Although the improved [and increased] connectivity can aide in the optimization of various manufacturing and distribution processes, it can also expose the safety-critical industrial network to the vast amount of cyber threats found on the global internet today.[12] Concerned with these same shortcomings, a group of researchers in 2012 tested SCADA and ICS devices and networks.[13] In a distressing conclusion, they found significant cyber vulnerabilities in numerous "top industrial control systems… used in critical infrastructure and manufacturing facilities" across the U.S.[14]

The researchers uncovered a "lack of authentication and encryption, and weak password storage" among the SCADA and ICS devices investigated.[15] Alarmingly, the researchers divulged they were able to acquire their access without significant effort.[16] Most concerning was the discovery that allowed the researchers "to interfere with specific critical processes… [including] the opening and closing of valves".[17] The identified vulnerabilities, combined with the large scope and breadth of critical infrastructures, provide evidence that a far-reaching, inclusive, and defense in depth strategy will be required to adequately strengthen overall cyber security.

2) Findings/Discussion:

With the current increase and varying types of cyberattacks, SCADA controllers and their associated networks must be safeguarded and secured. For example, suppose that the researchers in the above-mentioned 2012 study were instead malicious actors that had gained access to a nuclear power generation facility.[18] Remotely turning off critical control valves could have resulted in a catastrophic event that would have put many innocent lives at grave risk.[19] Although this example is only a hypothetical scenario, past cyberattacks have proven that critical infrastructures and their integrated controllers are vulnerable and susceptible to cyber threats.

One such successful cyberattack that targeted a specific type of SCADA controller is the 2010 Stuxnet virus cyberattack.[20] In total, it was found to have impacted more than 60,000 computers in countries ranging from China, the United Kingdom, and even to the United States.[21] However, the Stuxnet virus particularly targeted the country of Iran.[22] More specifically, the virus was found to target Iranian centrifuges that were being used to refine nuclear fuels for power production.[23]

In this case, the virus was able to infect the centrifuges and controllers that were offline and not connected to the public Internet.[24] Further, the malicious code used USB thumb drives as

---

[12] Nicholson et al., "SCADA security in the light of Cyber-Warfare."
[13] Kim Zetter, "Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software," last modified January 19, 2012, https://www.wired.com/2012/01/scada-exploits/.
[14] Ibid.
[15] Zetter, "Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software."
[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Steve Murphy, "The State of Cybersecurity in the Water/Wastewater Market," *InfraGard Journal*, Volume 1, https://www.infragardnational.org/wp-content/uploads/2019/05/The-State-of-Cybersecurity-in-the-WaterWastewater-Market.pdf.
[21] James Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, 53 no.1 (2011): 23-40, https://doi-org.ezproxy.niagara.edu/10.1080/00396338.2011.555586.
[22] Murphy, "The State of Cybersecurity in the Water/Wastewater Market."
[23] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."
[24] Ibid.

the intermediary to gain and establish control of the offline centrifuges.[25] Once the Stuxnet virus had successfully infiltrated the appropriate computer and centrifuge control system or SCADA device, the "Stuxnet worm [then exploited the] Siemens' default password to access Windows operating systems that ran the WinCC and PCS 7 [control] programs".[26]

After the virus had successfully compromised the centrifuge controllers, it then "alternate[d] the frequency of the electrical current that powered the centrifuges".[27] As a result, the centrifuges would then "switch back and forth between high and low speeds".[28] This oscillation "at intervals for which the machines were not designed" rendered the ability to process nuclear fuel inert and physically destroyed the centrifuges themselves.[29] The basic process and steps are outlined in the graphic shown in Figure 1[30]:

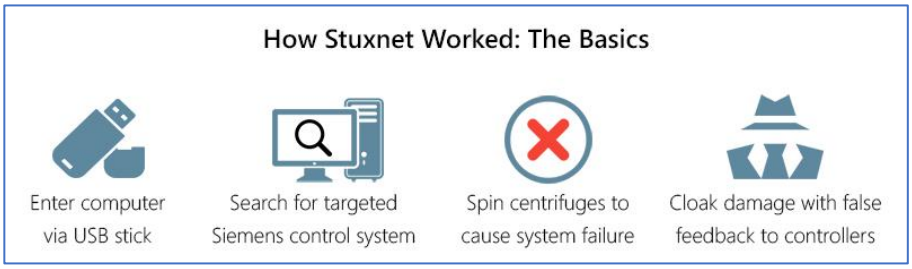

Figure 1

Although an official statement, acknowledgement, or motive of the attack remains elusive, many countries and researchers alike question if the nuclear fuel sought by Iran was in fact being created for power production.[31] Experts speculate that Iran was using the centrifuges with the intention of creating weapons grade nuclear compounds in their unsanctioned pursuit of nuclear weapons.[32] Regardless of the motive or origin, the Stuxnet virus significantly hindered the nuclear program Iran was attempting to develop without any loss of life.[33]

A similar analysis of the Stuxnet attack is warranted in order to determine if the United States own centrifuges and similar systems are vulnerable to a comparable type of an attack. In fact, the U.S. National Nuclear Security Administration (NNSA) in October 2018 announced the desire to expand "domestic uranium-enrichment capabilities".[34] Given the desire to increase the production of the United States' own nuclear fuel supplies, it will be especially important to ensure the ICS and SCADA devices used to moderate these processes are adequately protected.

Although SCADA and other industrial controls themselves can be comprised, the computer networks on which they reside and the users that operate them are also at risk. For example, the

[25] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Matt Puskala, "Industrial Security: 4 Ways to Keep Your Factory Safe from Cyber Attacks," September 23, 2016, https://www.dmcinfo.com/latest-thinking/blog/id/9293/industrial-security-4-ways-to-keep-your-factory-safe-from-cyberattacks.
[31] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."
[32] Ibid.
[33] Ibid.
[34] Frank N. von Hippel and Sharon K. Weiner, "No Rush to Enrich: Alternatives for Providing Uranium for U.S. National Security Needs," July/August 2019, https://www.armscontrol.org/act/2019-07/features/rush-enrich-alternatives-providing-uranium-us-national-security-needs#bio.

Ukrainian power grid was shuttered during a cyberattack in 2015, not necessarily by vulnerabilities in the SCADA and ICS devices themselves, but rather the computer systems and networks to which they were connected.[35] This cyberattack against Ukraine's critical infrastructure power grid ultimately resulted in power outages that affected at least 225,000 people.[36]

The groundwork for the attack was initiated by attackers who were able to successfully employ a form of social engineering.[37] A phishing email containing a malicious Excel attachment executed BlackEnergy malware onto the power company's computer and SCADA control network.[38] When it was time to commence the attack, "the hacker used the preinstalled malware to remotely take control of the HMI [human-machine interface]" for the SCADA controllers.[39] The hacker then switched off switchgears available to them through the interface.[40] The hackers were also perceptive enough to include additional code preventing the user from regaining access to networks and SCADA devices, prolonging the recovery.[41] Although the resulting power outage was relatively short, the control systems took much longer to repair.[42] In fact, more than two months after the attack, the control centers [were] still not fully operational.[43]

In the winter of 2016, Ukraine suffered another crippling cyberattack against their power grid.[44] This time new malware known as Industroyer was unleashed and "shut down the power grid.. [of] Kiev, [the capital of] Ukraine".[45] Industroyer proved to be a substantial evolution from BlackEnergy, in that it was the first malware capable of compromising power grids automatically.[46] With many critical infrastructure sectors relying on electricity, a similar successful attack on the United States power grid would be devastating. A threat actor, according to a Congressional report, would only need to disable or disrupt nine power substations across the United States to cause a 'coast-to-coast blackout.[47]

3) Recommendations/Improvements:

The Stuxnet virus and cyberattacks on Ukraine's power grid demonstrate that the threats faced by our current critical infrastructure systems are vast, ever changing, and should serve as a call to action for the United States. In response, some have suggested that steps be taken to return

---

[35] Patrice Bock et al, "Ukrainian power grids cyberattack," *InTech Magazine*, March/April 2017, https://www.isa.org/intech/20170406/.

[36] Tom Leithauser, "Ukraine grid attack sparks inquiry about U.S. power grid cybersecurity," *Cybersecurity Policy Report*, August 1, 2016, http://link.galegroup.com.ezproxy.niagara.edu/apps/doc/A460465703/ITOF?u=nysl_we_niagarau&sid=ITOF&xid=d17e0252.

[37] Ibid.

[38] Ibid.

[39] Bock et al, "Ukrainian power grids cyberattack."

[40] Ibid.

[41] Ibid.

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

[43] Ibid.

[44] Robert Lipovsky, "Seven years after Stuxnet: Industrial systems security once again in the spotlight," last modified June 16, 2017, https://www.welivesecurity.com/2017/06/16/seven-years-stuxnet-industrial-systems-security-spotlight/

[45] Ibid.

[46] Ibid.

[47] J.M. Porup, "Why America is not prepared for a Stuxnet-like cyberattack on the energy grid," last modified January 28, 2019, https://www.csoonline.com/article/3336061/why-america-is-not-prepared-for-a-stuxnet-like-cyber-attack-on-the-energy-grid.html.

older, non-computerized technologies to service.[48] For instance, legislation that would aim to protect the U.S. electric grid from hackers by studying ways to reincorporate older technologies into control systems was recently introduced in the United States Senate.[49]

Senate Bill S.174 – Securing Energy Infrastructure Act was placed on the Senate Legislative Calendar for further review and discussion on August 16, 2019.[50] Although not yet passed, the Bill outlines the new proposed strategy of the United States power grid operations: to increase the "use [of] analog and manual technology to isolate… important control systems".[51] To achieve this goal, "key devices like computer-connected operating systems that are vulnerable to cyberattacks [would be replaced] with analog and human-operated systems".[52] If the bill passes, the United States power grid would increasingly become disconnected and its component devices would no longer have internet access.[53]

Proponents for this model argue the greater "manual operations offer more control and lower risk" for defending against cyberattacks.[54] Further, the manual control ability was credited as a significant factor in Ukraine's power grid cyberattack recovery in 2015.[55] In contrast, our view is that this model may prove counter-intuitive in the long term. Manual controls reintroduce greater probability of human error, which could ultimately impact the safety and efficiency at which our nation's power grid currently operates.[56] To better combat such a wide and complex challenge, while still utilizing the advantages of technology devices, we recommend the adoption of a defense in depth approach.

A defense in depth scheme can be used to manage risk with diverse defensive strategies.[57] In other words, layering cyber defense controls and techniques is required. One layer to this approach should focus on better user training. In the case of the Stuxnet virus and the BlackEnergy cyberattack, the first line of the failed defense were the operators that introduced the exploits onto the networks and controllers. User-orientated phishing training campaigns can teach users of what to look for in malicious emails and attachments.[58] Promising studies indicate that phishing training helps users identify phishing emails".[59] Additionally, training users of the

---

[48] Tom Leithauser, "Bill would study use of older tech to thwart power grid cyberattacks," *Cybersecurity Policy Report*, June 13, 2016, http://go.galegroup.com.ezproxy.niagara.edu/ps/i.do?p=ITOF&sw=w&u=nysl_we_niagarau&v=2.1&it=r&id=GALE%7CA456351445&sid=summon&asid=90a09485caed686de0b0bf677605aaf5.

[49] Ibid.

[50] "S.174 - Securing Energy Infrastructure Act," accessed October 19, 2019, https://www.congress.gov/bill/116th-congress/senate-bill/174/text.

[51] Kate O'Flaherty, "U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks," last modified June 3, 2019, https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#d6a07d3191d5.

[52] Leithauser, "Bill would study use of older tech to thwart power grid cyberattacks."

[53] O'Flaherty, "U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks."

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] Sean Barnum, Michael Gegick, and C.C. Michael, "Defense in Depth," last modified September 13, 2005, https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth.

[58] Olga Zielinska et al., "One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 58, no. 1 (September 2014): 1466–70, https://doi-org.ezproxy.niagara.edu/10.1177/1541931214581306.

[59] Ibid.

dangers associated with unknown USB devices should be incorporated, as infected USBs are often an overlooked threat.[60]

Another layer in the defense in depth approach is operational, i.e., ensuring firmware and other security patches are applied and up-to-date on all systems and controllers. Planning for system and controller security maintenance will need to be added to other routine mechanical maintenance tasks already in place today. Such operations should occur regardless of whether or not the specific controller is connected to the internet.

An additional area for improvement is the standardization of cyber-security technology in SCADA controllers and networks. One concept under development would interject anti-virus protection onto the SCADA controllers themselves.[61] For example, partnerships like the one between Intel Security's McAfee and Honeywell Industrial Cyber Security Solutions seek to provide "enhanced security software [onboard SCADA devices in order to protect]… control systems from malware and misuse".[62]

Further standardizations could require that the default password be changed when setting up an industrial controller or SCADA device.[63] In regards to IoT devices, the State of California is preparing to enforce similar policies through legislation "mandating [IOT] device manufacturers… create a unique password for each device… or require the user to create one when they interact with the device for the first time".[64] Despite the relatively straightforward approach to implement many of these suggestions, there is currently a lack of central legislation to drive the adoption of such changes.

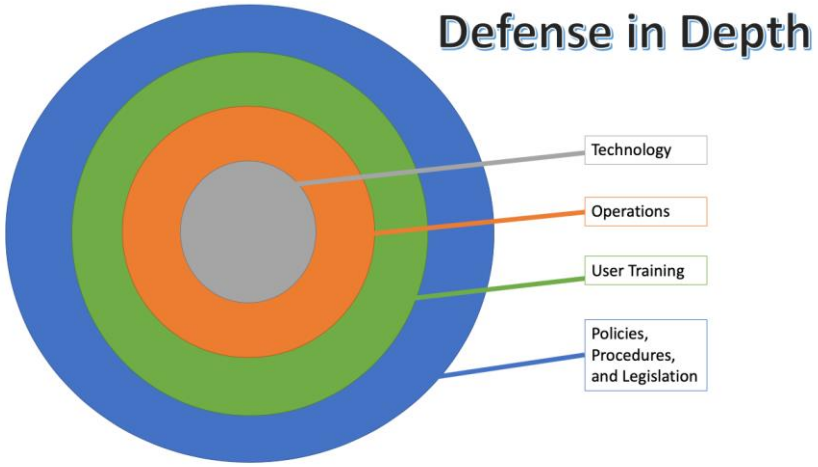

Figure 2

[60] "Wombat security announces mobile-responsive, 508 compliant modules to increase training flexibility and accessibility for end users," *PR Newswire*, September 13, 2016, https://ezproxy.niagara.edu/login?url=https://search-proquest-com.ezproxy.niagara.edu/docview/1818653125?accountid=28213.

[61] "Honeywell and Intel Security collaborates to secure critical infrastructure and Industrial Internet of Things," *Telecom Tiger*, June 27, 2015, http://bi.galegroup.com.ezproxy.niagara.edu/essentials/article/GALE%7CA419572982?u=nysl_we_niagarau&sid=summon.

[62] Ibid.

[63] Andrii Degeler, "California bans default passwords on any internet-connected device," last modified October 5, 2018, https://www.engadget.com/2018/10/05/california-default-password-ban-information-privacy-connected-devices-bill/?ncid=txtlnkusaolp00000616.

[64] Ibid.

As evidenced in Figure 2[65], polices, procedures, and legislation will be a critical first layer to the proposed defense in depth approach. Future legislation requiring integrated cyber-security measures for SCADA and ICS devices should be explored and adopted. Moreover, legislation requiring cyber threat user training for all our nation's critical infrastructure industries should also be implemented. Without regulation, a comprehensive defense in depth approach will be next to impossible to implement. The popular belief that there is "sufficient financial and business incentives currently in place to encourage private firms to protect their own systems and networks," is an outdated mindset in our view.[66] A more hardline approach should be adopted as "governments have a responsibility to intervene in the[ir] national interest".[67]

Lastly, a final recommendation to improve the overall defense in depth strategy is to enhance current partnerships among the United States and its allies. Canada, arguably one of the United States' strongest and geographically closest allies, also shares some critical infrastructure networks and resources. Collaboration should continue to be built and fostered, to "deepen [the] cooperation between U.S. and Canadian cyber emergency response teams".[68] The 2010 Canada-United States Action Plan for Critical Infrastructure was created with exactly this goal in mind.[69]

The Action Plan lays out initiatives to promote cooperation in strengthening the security and resiliency of critical infrastructure for both nations.[70] The cooperation outlined by the plan will "provide for more robust private-sector information sharing and promote better 'public awareness' of the multifaceted cyber threat".[71] The United States and Canada, potentially along with other key allies, should also explore more offensive cyber capabilities as part of their defense in depth strategy to protect critical infrastructures. Trusted partner nations, such as those as part of the Five Eyes Alliance (United States, United Kingdom, Canada, Australia, and New Zealand), may also be considered to be included in such efforts.[72]

4) Conclusion:

Critical infrastructure systems will remain an important asset for the United States. Steps need to be taken to ensure they improve their information security posture to maintain protection from cyberattack and vulnerabilities. With critical infrastructures serving as the backbone of our nation's economy, security, and health, any interruption to their services provided can have dire consequences.[73] The threat faced by critical infrastructure systems is present and ongoing.

---

[65] Vishruta Rudresh, "Securing Industrial Control Systems: A Holistic Defense-In-Depth Approach," last modified April 16, 2018, https://www.powermag.com/securing-industrial-control-systems-a-holistic-defense-in-depth-approach/.

[66] Cath Everett, "Who is responsible for securing critical infrastructure?," *Computer Fraud & Security*, 2010 no. 10 (2010): 5-8, https://doi.org/10.1016/S1361-3723(10)70130-5.

[67] Ibid.

[68] Scott Shackelford and Zachery Bohm, "Securing North American critical infrastructure: a comparative case study in cybersecurity regulation," *Canada-United States Law Journal*, (2016): 61+, http://link.galegroup.com.ezproxy.niagara.edu/apps/doc/A468334914/AONE?u=nysl_we_niagarau&sid=AONE&xid=9fa623da.

[69] Celia Louie, "U.S.-Canada Cybersecurity Cooperation," last modified September 8, 2017, https://jsis.washington.edu/news/cybersecurity-cooperation-u-s-canada/.

[70] Ibid.

[71] Shackelford and Bohm, "Securing North American critical infrastructure: a comparative case study in cybersecurity regulation."

[72] Louie, "U.S.-Canada Cybersecurity Cooperation."

[73] "What is Critical Infrastructure?"

To further illustrate this point, Russia was recently discovered to be making attempts against United States critical infrastructure control systems.[74] As recently as March 15, 2018, the "Russian government [took] actions targeting U.S. Government entities".[75] The Russians in this case specifically targeted "organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors".[76]

Perhaps most alarming is that the Russians targeted areas of weakness that had previously been identified as needing current improvement. The Russian threat actors, "targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks".[77] Additionally, the malicious actors "conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems" and SCADA devices.[78]

Although the Russian hackers in this case were discovered and stopped before any real damage could occur, it helps bring to light the very real and present threat our critical infrastructures face today. In adopting a defense in depth strategy that focuses on users, multi-national partnerships, operations, technology, policies, and legislation, the United States could significantly harden its current critical infrastructure control systems. The cyber security effort surrounding such systems will be required to evolve, match, and overcome any cyber threat of tomorrow.

References:

Barnum, Sean, Gegick, Michael, and Michael, C.C. "Defense in Depth." Last modified September 13, 2005. https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth

Bock, Patrice, Hauet, Jean-Pierre, Francoise, Romain, and Foley, Rober. "Ukrainian power grids cyberattack." *InTech Magazine*, March/April 2017. https://www.isa.org/intech/20170406/.

"Critical Infrastructure Sectors." Accessed March 30, 2019. https://www.dhs.gov/critical-infrastructure-sectors.

Degeler, Andrii. "California bans default passwords on any internet-connected device." Last modified October 5, 2018. https://www.engadget.com/2018/10/05/california-default-password-ban-information-privacy-connected-devices-bill/?ncid=txtlnkusaolp00000616.

Everett, Cath. "Who is responsible for securing critical infrastructure?." *Computer Fraud & Security*, 2010 no. 10 (2010): 5-8. https://doi.org/10.1016/S1361-3723(10)70130-5.

Farwell, James and Rohozinski, Rafal. "Stuxnet and the Future of Cyber War." *Survival*, 53 no.1 (2011): 23-40. https://doi-org.ezproxy.niagara.edu/10.1080/00396338.2011.555586.

Hippel, Frank N. von and Weiner, Sharon K. "No Rush to Enrich: Alternatives for Providing Uranium for U.S. National Security Needs." *Arms Control Association*, July/August 2019. https://www.armscontrol.org/act/2019-07/features/rush-enrich-alternatives-providing-uranium-us-national-security-needs#bio.

[74] Bruce Sterling, "US-Cert: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," last modified March 15, 2018, https://www.wired.com/beyond-the-beyond/2018/03/us-cert-russian-government-cyber-activity-targeting-energy-critical-infrastructure-sectors/.
[75] Ibid.
[76] Ibid.
[77] Sterling, "US-Cert: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors."
[78] Ibid.

"Honeywell and Intel Security collaborates to secure critical infrastructure and Industrial Internet of Things." *Telecom Tiger*, June 27, 2015. http://bi.galegroup.com.ezproxy.niagara.edu/essentials/article/GALE%7CA419572982?u=nysl_we_niagarau&sid=summon.

Igure, Vinay, Laughter, Sean, and Williams, Ronald. "Security issues in SCADA networks." *Computers & Security*, 25 no. 7 (2006): 498-506. https://doi-org.ezproxy.niagara.edu/10.1016/j.cose.2006.03.001.

"InfraGard, Critical Infrastructure Sectors." Accessed October 19, 2019. https://www.infragard.org/Application/General/SectorList.

Interagency Security Committee. "Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper." February 2015. https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf

Leithauser, Tom. "Bill would study use of older tech to thwart power grid cyber Attacks." *Cybersecurity Policy Report*, June 13, 2016. http://go.galegroup.com.ezproxy.niagara.edu/ps/i.do?p=ITOF&sw=w&u=nysl_we_niagarau&v=2.1&it=r&id=GALE%7CA456351445&sid=summon&asid=90a09485caed686de0b0bf677605aaf5

Lipovsky, Robert. "Seven years after Stuxnet: Industrial systems security once again in the spotlight." Last modified, June 16, 2017. https://www.welivesecurity.com/2017/06/16/seven-years-stuxnet-industrial-systems-security-spotlight/.

---. "Ukraine grid attack sparks inquiry about U.S. power grid cybersecurity." *Cybersecurity Policy Report*, August 1, 2016. http://link.galegroup.com.ezproxy.niagara.edu/apps/doc/A460465703/ITOF?u=nysl_we_niagarau&sid=ITOF&xid=d17e0252

Louie, Celia. "U.S.-Canada Cybersecurity Cooperation." Last modified September 8, 2017. https://jsis.washington.edu/news/cybersecurity-cooperation-u-s-canada/.

Minoli, Daniel. *Building the Internet of Things with IPv6 and MIPv6 : The Evolving World of M2M Communications.* Somerset:John Wiley & Sons, Incorporated, 2013. https://ebookcentral.proquest.com/lib/niagara-ebooks/reader.action?docID=1216195&ppg=21.

Murphy, Steve. "The State of Cybersecurity in the Water/Wastewater Market." *InfraGard Journal*, Volume 1. https://www.infragardnational.org/wp-content/uploads/2019/05/The-State-of-Cybersecurity-in-the-WaterWastewater-Market.pdf

Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H. "SCADA security in the light of Cyber-Warfare." *Computers & Security*, 31, no. 4 (2012): 418-436. https://doi-org.ezproxy.niagara.edu/10.1016/j.cose.2012.02.009.

O'Flaherty, Kate. "U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks." Last modified June 3, 2019. https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#d6a07d3191d5.

Porup, J.M. "Why America is not prepared for a Stuxnet-like cyberattack on the energy grid." Last modified January 28, 2019. https://www.csoonline.com/article/3336061/why-america-is-not-prepared-for-a-stuxnet-like-cyber-attack-on-the-energy-grid.html.

Puskala, Matt. "Industrial Security: 4 Ways to Keep Your Factory Safe from Cyber Attacks." Last modified September 23, 2016. https://www.dmcinfo.com/latest-thinking/blog/id/9293/industrial-security-4-ways-to-keep-your-factory-safe-from-cyberattacks.

Rudresh, Vishruta. "Securing Industrial Control Systems: A Holistic Defense-In-Depth Approach." Last modified April 16, 2018. https://www.powermag.com/securing-industrial-control-systems-a-holistic-defense-in-depth-approach/.

"S.174 - Securing Energy Infrastructure Act." Accessed October 19, 2019. https://www.congress.gov/bill/116th-congress/senate-bill/174/text.

Shackelford, Scott and Bohm, Zachery. "Securing North American critical infrastructure: a comparative case study in cybersecurity regulation." *Canada-United States Law Journal*, (2016): 61+. http://link.galegroup.com.ezproxy.niagara.edu/apps/doc/A468334914/AONE?u=nysl_we_niagarau&sid=AONE&xid=9fa623da.

Sterling, Bruce. "US-Cert: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." Last modified March 15, 2018. https://www.wired.com/beyond-the-beyond/2018/03/us-cert-russian-government-cyber-activity-targeting-energy-critical-infrastructure-sectors/.

"What is Critical Infrastructure?" Accessed March 30, 2019. https://www.dhs.gov/sites/default/files/publications/ip-fact-sheet-508.pdf.

"Wombat security announces mobile-responsive, 508 compliant modules to increase training flexibility and accessibility for end users." *PR Newswire*, September 13, 2016. https://ezproxy.niagara.edu/login?url=https://search-proquest-com.ezproxy.niagara.edu/docview/1818653125?accountid=28213.

Zetter, Kim. "Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software." Last modified January 19, 2012. https://www.wired.com/2012/01/scada-exploits/.

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

Zielinska, Olga, Rucha Tembe, Kyung Wha Hong, Xi Ge, Emerson Murphy-Hill, and Christopher B. Mayhorn. "One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58, no. 1 (September 2014): 1466–70. https://doi-org.ezproxy.niagara.edu/10.1177/1541931214581306.