Submitted Statement for the Record of

Kathryn Waldron
Fellow, National Security and Cybersecurity Policy
R Street Institute

Before the

Subcommittee on Energy
Committee on Energy and Commerce
United States House of Representatives

Hearing on

Keeping The Lights On: Addressing Cyber Threats To The Grid

July 12, 2019

KEEPING THE LIGHTS ON: ADDRESSING CYBER THREATS TO THE GRID

Chairman Rush, Ranking Member Upton and Members of the Committee:

Thank you for holding this hearing on the cybersecurity of the United States' power grid. In a world where society is increasingly dependent on electricity to maintain the fabric of daily life, the United States is vulnerable to new methods of attack from hostile actors. A cyberattack that denies service to significant portions of America's population could potentially overwhelm our current ability to respond. Energy companies and electric grid operators must therefore be sufficiently incentivized to install defenses against cyberthreats to the grid, while federal and state government officials must develop better recovery strategies in case a blackout occurs.

My name is Kathryn Waldron, and I am a fellow with the national security and cybersecurity team at the R Street Institute. The R Street Institute is a nonprofit, nonpartisan public policy research organization whose mission is to engage in policy research and outreach to promote free markets and limited, effective government. Our scholars have written extensively on the issues of energy, cybersecurity and the national security implications of today's global supply chain.

The U.S. power grid is the vast network that allows for electricity to be delivered to businesses and individuals across the nation. It includes generators, power stations, transmission lines, distribution lines, and all of the manual and digital systems employed by utility companies. The United States is currently in the process of switching to a smart grid system as different parts of the grid are modernized. (The current grid system was built in the 1890s.) The smart grid would incorporate digital technology that would allow for two-way flows of both electricity and information.[1]

Nations have long recognized the strategic importance of national power grids. For example, countries have frequently targeted a rival's power grid during wartime. The strategy of attacking power grids was discussed frequently in the 1930s by the U.S. Air Corps Tactical School and eventually became the "bedrock upon which the World War II strategic bombing campaigns were first designed."[2] Electrical grids were an appealing target at the time as strategists hoped the loss of electricity would simultaneously reduce production capacity, hinder military ability and dampen civilian morale, eroding support for any war efforts.[3]

[1] Office of Electricity Delivery and Energy Reliability, "What is the Smart Grid?" U.S. Department of Energy, accessed July 9, 2019. https://www.smartgrid.gov/the_smart_grid/smart_grid.html.

[2] Thomas E. Griffith Jr., "Strategic Attack of National Electrical Systems," October 1994, p. 15. https://media.defense.gov/2017/Dec/29/2001861964/-1/-1/0/T_GRIFFITH_STRATEGIC_ATTACK.PDF.

[3] ibid.

The German power grid was a major military target for Allied forces in World War II. While the Allies did not successfully manage to disrupt Germany's access to electricity, power grids continued to be targeted in subsequent military conflicts. In 1952, during the Korean War the United States bombed and destroyed approximately 90 percent of North Korea's power generating infrastructure, leading to a two-week blackout. The U.S. military also attacked the North Vietnamese power grid during the Vietnam War. Destruction of the Iraqi power grid by U.S. forces during the Gulf War lead to devastating civilian casualties, with some reports attributing 70,000 deaths to the blackout.[4]

In today's world, the most pressing threats to the power grid come from malicious cyber actions rather than strategic bombing campaigns. In December 2015, malicious cyber activities against three energy companies in Ukraine left approximately 225,000 people without power for several hours. Spear-phishing emails facilitated intrusions into the computer and supervisory control and data acquisition (SCADA) systems that controlled the Ukrainian systems, allowing intruders to seize control. The intrusion, which occurred as part of the ongoing conflict between Russia and Ukraine, is generally attributed to the Russian group Sandworm.[5] Ukraine's power grid was hacked again the following year, resulting in part of Kiev going without power for approximately an hour. While the 2015 intrusion allowed hackers to infiltrate networks in order to manually shut down an electrical substation, the 2016 intrusion was fully automated.[6]

Although the United States has not seen cyber-instigated power outages like the events in Ukraine, segments of the American energy grid have been targeted frequently by malicious cyber actors. In 2003, the safety monitoring system of a nuclear power plant in Ohio was infected by malware known as "Slammer worm." No damage occurred, as the power plant was offline at the time.[7] In 2008, then-CIA analyst Tom Donahue revealed that hackers compromised the computer systems of utility companies in several U.S. cities, attempting to extort money by threatening to cause blackouts.[8] And just this year hackers launched "denial-of-service" cyber activities that disabled the SCADA component of power grid control systems in Utah, Wyoming and California.[9]

[4] Ibid, pp. 34-47.

[5] "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC, March 118, 2016. https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[6] Andy Greenberg, "'Crash Override': The Malware That Took Down A Power Grid*,"* *Wired*, June 12, 2017. https://www.wired.com/story/crash-override-malware/.

[7] Candid Wueest, "Targeted Attacks Against the Energy Sector," Symantec, January 13, 2014. https://bluekarmasecurity.net/wp-content/uploads/2014/09/Symantec_Targeted-Attacks-Against-the-Energy-Sector_whitepaper.pdf.

[8] Ellen Nakashima and Steven Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *The Washington Post,* January 9, 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277_pf.html.

[9] Blake Sobczak, "Experts assess damage after first cyberattack on U.S. grid," *E&E News*, May 6, 2019. https://www.eenews.net/stories/1060281821.

The U.S. Department of Homeland Security (DHS) has reportedly been warning electrical utility executives about Russian threats for over five years. In 2018, the Wall Street Journal reported that Russian hackers working for the state-sponsored group Energetic Bear had successfully infiltrated the control rooms of some U.S. electrical utility companies. The hackers accessed supposedly secure, "air-gapped" systems by worming their way in through the utility supply chain. Jonathan Homer, chief of industrial-control-system analysis for DHS, stated about the hackers, "They got to the point where they could have thrown switches."[10]

Yet despite continued reports of Russian probing of the U.S. power grid, Russia has refrained from any sort of cyber activity along the lines of the Ukraine outages. This may be due in part to the threat of mutual retaliation from the United States. Last month *The New York Times* reported that U.S. Cyber Command had successfully infiltrated the Russian power grid. While the United States allegedly has put cyber reconnaissance probes into the control systems of the Russian power grid since 2012, this latest move adds a new level of aggression to America's cyber strategy.[11] President Trump, who was not consulted on Cyber Command's actions according to the article, denied American infiltration, tweeting that the article was "NOT TRUE" and calling the New York Times desperate for a story.[12] The U.S. Cyber command is not legally required to inform the president before carrying out cyber activities of this nature. However, the lack of unity among government officials and leaders on this issue makes the United States look weak when it comes to national security and cybersecurity, making the grid a more appealing target for hackers. Therefore, it is all the more important to update the security of the grid.

Smart Grids

The switch to smart grid systems is sometimes touted as adding resiliency to the electric system, since it will increase the flow of information and more easily allow rerouting in the case of limited failures. The U.S. Department of Energy (DOE) has put forth a number of projects and initiatives related to the grid's cybersecurity, including its Cybersecurity for Energy Delivery Systems program and their National SCADA Test Bed, "which provides testing environments to help industry and government identify and correct vulnerabilities in SCADA equipment and control systems."[13] The DOE has also partnered with the National Institute for Standards and Technology (NIST) to issue "Guidelines for Smart Grid Cybersecurity." The guidelines provide

[10] Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *Wall Street Journal*, July 23, 2018. https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110.

[11] David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, June 15, 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

[12] Staff, "Trump calls NYT report on U.S. intrusions into Russia power grid 'virtual act of treason'," *The Japan Times*, June 17, 2019. https://www.japantimes.co.jp/news/2019/06/17/world/trump-calls-nyt-report-russia-power-grid-intrusions-virtual-act-treason/#.XSUiq-hKg2w.

[13] Office of Electricity Delivery and Energy Reliability, "Cybersecurity," U.S. Department of Energy, accessed July 10, 2019. https://www.smartgrid.gov/recovery_act/overview/cyber_security.html.

a framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks and vulnerabilities.[14]

However, increased reliance on digital systems means more access or disruption points for hackers. This has led some politicians to advocate for mandating the inclusion of "retro" technology in the power grid. Last month the Securing Energy Infrastructure Act (SEIA) passed the Senate. The bill's supporters hope the inclusion of analog and manual technology will isolate critical parts of the grid from cyberattacks, arguing that the power outages in Ukraine "could have been worse if not for the fact that Ukraine relies on manual technology to operate its grid."[15]

Industry reaction to SEIA has been mixed. While some experts are not opposed to the concept of analog backup systems, others view the SEIA bill as sidestepping the real issue by proposing a solution that hampers development and superior provision of energy. According to James Scott, co-founder and senior fellow at the Institute for Critical Infrastructure Technology, "Legislation that eschews modern systems in favor of antiquated technologies is a step in the wrong direction because it amounts to significantly crippling the U.S. energy sector instead of addressing the threats."[16]

Worries about the U.S. grid based on the attacks in Ukraine may be overblown, as the Ukrainian grid is far more unified than its American counterpart. Any discussion of the national security of the power grid would be incomplete without acknowledging its uniquely fragmented nature. The U.S. grid is primarily split into three main parts—the Eastern Interconnection, the Western Interconnection and Texas—and each part has its own web of interconnected investor-owned utility companies. As a result, it would be challenging (although not impossible) for any individual, group or nation to cause a complete shutdown of the entire U.S. grid at one time. The private-sector elements of U.S. energy provision thereby strengthen the grid's protection, especially when compared to a unified national system.

Moving Forward

Determining how best to protect the U.S. power grid is a challenging and complex undertaking. In order to reliably and securely provide electrical power to all Americans, it is critically important that Congress play an active oversight and legislative role to better ensure

[14] National Institute of Standards and Technology, "Guidelines for Smart Grid Cybersecurity," U.S. Department of Commerce, September 2014. https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

[15] Angus King, "Senate Passes King Bill Protecting Energy Grid from Cyber-Attacks," June 28, 2019. https://www.king.senate.gov/newsroom/press-releases/senate-passes-king-bill-protecting-energy-grid-from-cyber-attacks.

[16] Alex Crees, "Dumbing down the electric grid: the answer to cybersecurity concerns?" *Choose Energy*, accessed July 10, 2019. https://www.chooseenergy.com/news/article/dumbing-electric-grid-answer-cybersecurity-concerns/.

that the grid can withstand even the most sophisticated cyber intrusion. In the event of a successful intrusion that results in the interruption of electrical service, it is also essential that the operators of the power grid have the capacity to promptly remediate any damage to the system and restore full operability. Below are a few suggestions of ways the United States can strengthen the grid's security.

First, utility companies should be encouraged to carefully vet their own supply chain. Protecting the American power grid is, in part, a matter of supply chain security. Utility companies have their own vendors and suppliers, and these suppliers can carry risks. In the case of Energetic Bear compromising the U.S. power grid discussed above, hackers were able to infiltrate by attacking less secure, yet still trusted vendors.

Second, state governments can also seek to align their security concerns with the incentives of local utility companies. My colleague Travis Kavulla at the R Street Institute has written previously on the need for economic regulation of utility companies to incentivize investment in safety protections against natural disasters like wildfires. This methodology can be applied to cyberthreats as well as natural public-safety risks. In order to align incentives, Kavulla advocates tying regulated utilities' compensation to safety outcomes:

> If safety improvements were obtainable primarily through increased capital spending, it would be reasonable to persist with the status quo, in which a utility's profit is a function of its "used and useful" capital investment. The existing regulatory model, which rewards a utility's equity investment, whether at 10 percent or 17 percent, ensures that. But if safety improvements will result primarily from operational improvements, then the cost-of-service, rate-of-return regulatory model appears misaligned to it. This would seem to be a powerful argument for tying a potentially substantial amount of the corporation's existing or incremental profit opportunity to safety performance.[17]

Cybersecurity inputs can often be difficult to measure and increased spending does not necessarily equal increased security. (Consider, for example, how installing more than one antivirus program often makes a computer system less safe by confusing the programs downloaded.)[18] Tying funding to results instead of merely increasing spending is therefore more likely to send utility companies searching for the right security programs instead of simply adding more security programs.

[17] Opening Statement of Travis Kavulla, California Public Utilities Commission, Forums on Governance, Management, and Safety Culture, April 26, 2019. https://www.rstreet.org/wp-content/uploads/2019/04/Final-edit-Remarks-CPUC-April-2019-PGE.pdf.

[18] "Why Using Multiple Antivirus Programs is a Bad Idea," *Kaspersky Daily*, September 9, 2013. https://www.kaspersky.com/blog/multiple-antivirus-programs-bad-idea/2670/.

Third, U.S. government agencies devise strategies to deal with worst-case scenarios in the case of a successful attack on the grid. While progress has been made in this area, there remains more to be done. Last December the president's National Infrastructure Advisory Council (NIAC) released a report concluding "that existing national plans, response resources, and coordination strategies would be outmatched by a catastrophic power outage."[19] One simple recommendation proposed by NIAC is to clarify emergency authority in the case of a "cyber-physical disaster," which the report states is understood at a high level but not at the level of implementation. (The term "cyber-physical disaster" refers to cyber activities cause damage in the physical world.)

I thank the Committee for its recognition of the importance of ensuring the cybersecurity of the power grid. If I or any of my colleagues at the R Street Institute can be of assistance to members of the Committee, please feel free to contact me.

Kathryn Waldron
Fellow, Cybersecurity and National Security
kwaldron@rstreet.org

[19] The President's National Infrastructure Advisory Council, "Surviving a Catastrophic Power Outage," December 2018. https://www.dhs.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_508%20FINAL.pdf.