Hacking Power Grids: A Current Problem

By: Nir Kshetri and Jeffrey Voas

Kshetri, Nir and Voas, J. (2017)." Hacking Power Grids: A Current Problem ", IEEE *Computer 50*(12), 91-95.

Made available courtesy of IEEE: https://doi.org/10.1109/MC.2017.4451203

Abstract:

Cyberattacks against power grids and other critical infrastructures are increasing in frequency and severity. Government and industry stakeholders must take more active steps to address the problem before a major catastrophe occurs.

Keywords: cyberattacks | hacking | cybersecurity | critical infrastructures

Article:

Cyberattacks are increasingly being waged by state intelligence services or their proxies against other countries' government institutions, corporations, and industrial facilities. National power grids are emerging as a target of choice given their vulnerability and the massive economic and social disruption caused by a widespread and lengthy loss of electricity. A recent contingency planning memo from the Council on Foreign Relations asserted that "disabling or otherwise interfering with the power grid in a significant way could … seriously harm the United States."[1] In testimony before a congressional panel in November 2014, Michael Rogers, director of the NSA and head of US Cyber Command, said that China and "one or two" other countries had the ability to take down the entire US power grid and other critical systems.[2]

A 2016 report by infrastructure engineering and construction consultancy Black & Veatch ranked cybersecurity as the second most pressing issue for electric utilities, only behind reliability—this was up from being the sixth- and fourth-highest concern, respectively, the two previous years.[3,4] Alarmingly, the 2016 report indicated that only 32 percent of electric utilities had integrated cybersecurity systems with the "proper segmentation, monitoring and redundancies" needed to deal with cyberthreats, while 48 percent had no such capabilities.

The US Department of Homeland Security (DHS) has labeled 16 critical infrastructure sectors as vital (www.dhs.gov/critical-infrastructure-sectors). All of these sectors must have electricity, making the energy sector a highly attractive target. A study by the US Cyber Consequences Unit indicated that the costs of a single wave of cyberattacks on US critical infrastructures could exceed $700 billion, approximately the same as that associated with 50 major hurricanes.

US military leaders employ scenario planning to better understand the risks of such cyberattacks—for example, in a confrontation over Taiwan, China might try to cut off the electricity to Fort Bragg, California, to ground US airborne forces.[5] In 2007, a Pentagon cyberdefense analyst testified to Congress that a mass cyberattack could leave up to 70 percent of the US without electrical power for 6 months. Another estimate suggested that a loss of 4 percent of power in North America would disconnect almost two-thirds of the entire grid in the region.[6]

POWER-GRID ATTACKS

As Table 1 shows, there have been several cyberattacks against power companies and grids over the past decade.[7–15] These attacks are becoming more frequent. In 2012, for example, of 200 or so cyberattacks on US critical infrastructures, about half of those targeted a power grid.[16] Power-grid attacks are also increasing in severity. ESET security researchers regarded the Industroyer malware that caused a blackout in Kiev in December 2016 to be the biggest threat to industrial control systems since Stuxnet, which did substantial damage to Iran's nuclear program.[17]

Table 1. Example cyberattacks on power companies and grids.

Date	**Incident**
February 2011	A Brazilian power plant was infected by the two-year-old Conficker worm, causing the plant's management systems to freeze up and not display data.
June 2011	The anarchic hacking group LulzSec shut down the website of Brazilian energy company Petrobras—Latin America's largest energy producer—with a distributed denial-of-service attack for part of a day.
2013-2014	A hacker group linked to the Russian government known as Dragonfly or Energetic Bear used a Stuxnet-like Trojan called Havex to compromise the control systems of more than 1,000 energy fi rms in 84 countries including the US, Germany, France, Italy, Spain, Turkey, and Poland. The goal appears to have been industrial sabotage.
December 2015	A hacker team called Sandworm used the BlackEnergy malware package to hijack the control systems of multiple regional power stations in Ukraine, cutting off electricity to about 225,000 people for many hours. Ukrainian officials blamed Russia for what was the world's first hacker-caused power outage.
December 2016	Sandworm once again targeted Ukraine's power grid, this time a transmission facility outside Kiev, knocking out power in parts of the city and surrounding area for an hour. The perpetrators used Industroyer malware, which enables direct control of circuit breakers and switches.
May 2017	WannaCry ransomware infected four billing offices of India's West Bengal State Electricity Distribution Company, which serve about 800,000 households, and caused bill-payment operations to be suspended for most of a day until backed-up data could be restored.
First half of 2017	Another Russia-based hacking group, called Dragonfly 2.0 by security researchers, targeted dozens of Western energy companies, breaking into more than 20 firms' networks and possibly obtaining operational access to some in the US and Turkey.

Malware like Industroyer is particularly dangerous because it enables hackers to do more than carry out industrial sabotage: it gives them operational access to power companies' networks, which means they can directly control the interfaces used to send commands to equipment such as circuit breakers, switches, and disconnectors and halt electricity flow at will. Such malware could be secretly planted and exploited at an opportune time such as during a conflict.[18]

One factor contributing to the vulnerability of power grids is that industrial communication protocols are often standardized across different infrastructures, which limits security. Malware used against one type of industrial control system can simply be "tweaked" to attack a power grid.[19]

Another factor is the lack of incentivization—at least until recently—to implement defenses against cyberattacks targeting power grids and other critical infrastructure.[20,21] Although a security breach can have catastrophic consequences, existing equipment at many facilities is old and expensive to replace, and upgrades can disrupt service. Many utilities were originally designed to be isolated from other networks to increase resilience; consequently, they often rely on outdated protocols without established security mechanisms such as encryption and authentication, or old software with well-known vulnerabilities such as Windows XP.

Utilities are also heavily regulated, and implementing new technologies often requires navigating a lengthy and complicated approval process involving input from policymakers, government regulators, and power company officials.

Finally, a recent European Commission report noted that a key challenge is the lack of education about cyberattacks and awareness of their dangers among legislators and executives in the energy industry. It argued for greater coordination among all stakeholders to gain the necessary technical expertise to design, build, and maintain smart-grid systems that are secure.[22]

COUNTERMEASURES

Various actors—including policymakers and government regulators, energy companies, and power-grid equipment suppliers—have taken steps to address the growing problem of power-grid attacks.

Government initiatives

In the US, the Department of Energy (DOE) and DHS, in consultation with Obama administration officials and both private- and public-sector experts, developed the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) in 2012 to guide the implementation and management of cybersecurity measures and sharing of best practices by utility companies.[23] In May 2017, President Trump issued an executive order outlining actions for federal agencies to strengthen the cybersecurity of power grids and other critical infrastructures. It instructs the DOE and DHS to work with state and local government agencies to identify risks to the US power grid and assess the potential consequences of cyberattacks.[24]

In recent years, US lawmakers have also proposed legislation to study cyberthreats to the power grid, the impact of a major blackout (especially on the military), and potential solutions, including lower-cost "analog" approaches that involve taking the grid offline.[25] Two pending bills introduced in 2017 include S. 79—Securing Energy Infrastructure Act (www.congress.gov/bill/115th-congress/senate-bill/79) and H.R. 3855—Securing the Electric Grid to Protect Military Readiness Act of 2017 (www.congress.gov/bill/115th-congress/house-bill/3855).

The EU is enacting similar legislation and in some cases is more aggressive than the US by mandating proactive measures. For example, France's 2014 cybersecurity law requires more than 200 entities in the energy and other critical sectors to boost cybersecurity by using certified, domestically manufactured products. Businesses that fail to comply face fines of up to €750,000.[26]

Following the 2014 cyberattacks on the US unit of Sony Corporation, Japan actively took steps to enhance cooperation among the country's 13 critical infrastructure industries, including electricity, by making the Cyber Security Strategy Headquarters part of the cabinet and establishing the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) to work with industry to improve cyberdefenses.[27,28] In 2016, the Ministry of Economy, Trade, and Industry and the Japan Electrotechnical Standards and Codes Committee developed specific cybersecurity guidelines for electric power control systems such as minimizing connections between internal networks and the Internet and encrypting daily network traffic.[29]

Corporate initiatives

Energy providers have responded to recent power-grid attacks with their own initiatives. For example, in August 2012 hacktivists launched a cyberattack against Saudi Aramco using a virus called Shamoon that erased the hard drives of 30,000 computers—85 percent of the oil giant's devices—and shut down the company's business for two weeks at a cost of over $15 million. Following this attack, the Saudi Electricity Company increased their cybersecurity investment by 20 percent, putting special emphasis on protecting electricity generation and transmission.[30]

Equipment suppliers are also more engaged. Siemens and ABB, which dominate the global market for power-grid and industrial equipment, are strengthening their products' cybersecurity. For example, on its website for transformers, ABB publishes advisories and alerts about cybersecurity issues. Siemens monitors cyberthreats and issues warnings for operational technology networks, which monitor and control physical devices, processes, and events. Siemens also has dedicated endpoint protection to stop the execution of malicious applications.[31]

Past cyberattacks were often mounted by criminals seeking economic gain or by disaffected political activists, but state intelligence agencies and their proxies have emerged as the dominant and most dangerous adversaries. These actors have the resources, personnel, and tools to infiltrate government and corporate networks and launch devastating attacks.

Among the most potentially damaging cyberattacks are those against power grids and other critical infrastructures on which modern institutions heavily rely. In the wake of recent alarming incidents, government and industry stakeholders are awake to the problem, but progress remains slow and incremental. Although it's impossible to defend against every cyberthreat, the probabilities of a successful attack can be reduced. In addition to mandating stronger cybersecurity, governments should provide additional economic incentives to energy providers and power-equipment suppliers to implement more robust measures.

REFERENCES

1. Council on Foreign Relations, “A Cyberattack on the U.S. Power Grid,” Contingency Planning Memorandum No. 31, 3 Apr. 2017; www.cfr.org/report/cyberattack-us-power-grid.

2. A. Smith, “China Could Shut Down U.S. Power Grid with Cyber Attack, Says NSA Chief,” *Newsweek*, 21 Nov. 2014; www.newsweek.com/china-could-shut-down-us-power-grid-cyber-attack-says-nsa-chief-286119.

3. A. Neuhauser, “Cybersecurity among Top Energy Industry Concerns,” *U.S. News & World Report*, 12 Aug. 2014; www.usnews.com/news/articles/2014/08/12/cybersecurity-among-top-energy-industry-concerns.

4. “Singapore: The Cybersecurity Act Will Improve Security Culture across Utilities in Asia—Black & Veatch,” *Water & Wastewater Asia*, 15 June 2017; www.waterwastewaterasia.com/en/news-archive/singapore-the-cybersecurity-act-will-improve-security-culture-across-utilities-in-asia-black-veatch/963.

5. C. Mitchell, “Cyberwar: Not If. Not When. Now.,” *Washington Examiner*, 29 Sept. 2014; washingtonexaminer.com/cyberwar-not-if.-not-when.-now./article/2553470.

6. N. Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Springer, 2010.

7. R. McMillan, “A Power Plant Hack That Anybody Could Use,” *PCWorld*, 4 Aug. 2011; www.pcworld.com/article/237347/a_power_plant_hack_that_anybody_could_use.html.

8. R. McMillan, “Brazilian Government, Energy Company Latest LulzSec Victims,” *PCWorld*, 23 June 2011; www.pcworld.idg.com.au/article/391161/brazilian_government_energy_company_latest_lulzsec_victims.

9. S. Khandelwal, “Dragonfly Russian Hackers Target 1000 Western Energy Firms,” *The Hacker News*, 1 July 2014; thehackernews.com/2014/07/dragonfly-russian-hackers-scada-havex.html.

10. N. Perlroth, “Russian Hackers Targeting Oil and Gas Companies,” *The New York Times*, 30 June 2014; www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html.

11. J. Finkle, “U.S. Government Asks Firms to Check Networks after ‘Energetic Bear’ Attacks,” Reuters, 2 July 2014; www.reuters.com/article/us-cybersecurity-energeticbear/u-s-government-asks-firms-to-check-networks-after-energetic-bear-attacks-idUSKBN0F722V20140702.

12. D. Goodin, “First Known Hacker-Caused Power Outage Signals Troubling Escalation,” *Ars Technica*, 4 Jan. 2016; arstechnica.com/information-technology/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation.

13. K. Zetter, “Everything We Know about Ukraine’s Power Plant Hack,” *Wired*, 20 Jan. 2016; www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack.

14. K. Zetter, “The Ukrainian Power Grid Was Hacked Again,” *Motherboard*, 10 Jan. 2017; motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report.

15. “‘WannaCry’ Ransomware: Bengal Power Distribution Company Hit by Cyberattack, Say Officials,” *Hindustan Times*, 15 May 2017; www.hindustantimes.com/india-news/wannacry-ransomware-bengal-power-distribution-company-hit-by-cyberattack-say-officials/story-biqMQN5cPKng36cIyho2oJ.html.

16. Symantec, *Dragonfly: Cyberespionage Attacks against Energy Suppliers*, Symantec Security Response Version 1.21, 7 July 2014; www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf.

17. “Industroyer: Biggest Malware Threat to Critical Infrastructure since Stuxnet,” ESET, 12 June 2017; www.eset.com/int/industroyer.

18. A. Greenberg, “Hackers Gain Direct Access to US Power Grid Controls,” *Wired*, 6 Sept. 2017; www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems.

19. “‘Industroyer’ Virus Could Bring down Power Networks, Researchers Warn,” *The Guardian*, 13 June 2017; www.theguardian.com/technology/2017/jun/13/industroyer-malware-virus-bring-down-power-networks-infrastructure-wannacry-ransomware-nhs.

20. K. Vinton, “Hacking Gets Physical: Utilities at Risk for Cyber Attacks,” *Forbes*, 10 July 2014; www.forbes.com/sites/katevinton/2014/07/10/hacking-gets-physical-utilities-at-risk-for-cyber-attacks.

21. T. Simonite, “Protecting Power Grids from Hackers is a Huge Challenge,” *MIT Technology Rev.*, 27 Feb. 2013; www.technologyreview.com/news/511851/protecting-power-grids-from-hackers-is-a-huge-challenge.

22. European Commission Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids, *Cyber Security of the Smart Grids*, summary report, 02 Dec. 2011; ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=1761.

23. US Dept. of Energy and US Dept. of Homeland Security, *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)*, v1.0, Carnegie Mellon Univ., 31 May 2012; energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf.

24. K. Shallenberger, “Trump’s Cybersecurity Executive Order Calls for Power Grid Assessment,” *Utility Dive*, 12 May 2017; www.utilitydive.com/news/trumps-cybersecurity-executive-order-calls-for-power-grid-assessment/442560.

25. E. Groll, “Preventing a Blackout by Taking the Power Grid Online,” *Foreign Policy*, 10 June 2016; foreignpolicy.com/2016/06/10/preventing-a-blackout-by-taking-the-power-grid-offline.

26. H. Fouquet and M. Mawad, “France Demonstrates Security Savoir Faire as It Enforces New Cyber-Security Law,” *Chicago Tribune*, 7 Oct. 2014; www.chicagotribune.com/sns-wp-blm-news-bc-france-cyber06-20141006-story.html#page=1

27. A. Mie, “Ruling Bloc Readies Bill to Bolster Cybersecurity amid Growing Attacks,” *The Japan Times,* 11 Mar. 2014; www.japantimes.co.jp/news/2014/03/11/national/ruling-bloc-readies-bill-to-bolster-cybersecurity-amid-growing-attacks/#.WdMFN8YVjIU.

28. T. Kelly and K. Nobuhiro, “Japan, Wary of North Korea, Works to Secure Infrastructure after Sony Attack,” Reuters, 24 Dec. 2014; www.reuters.com/article/us-northkorea-cyberattack-japan/japan-wary-of-north-korea-works-to-secure-infrastructure-after-sony-attack-idUSKBN0K20IX20141224.

29. A. Kuwahata, “Cyber Security Regulation for Electric Power Systems in Japan,” presentation, 5th Int’l Workshop on Cybersecurity, 14 July 2017; web.cs.kyushu-u.ac.jp/data/event/2017/04/ak.pdf.

30. A. Allison, “The Hidden Value of IT Departments,” *Middle East Economic Digest*, vol. 57, no. 18, 2013; www.meed.com/the-hidden-value-of-it-departments.

31. “Siemens India Wins First Cyber Security Contract for Power Plant Automation,” *Business Standard*, 15 June 2017; www.business-standard.com/content/b2b-manufacturing-industry/siemens-india-wins-first-cyber-security-contract-for-power-plant-automation-117061500691_1.html.