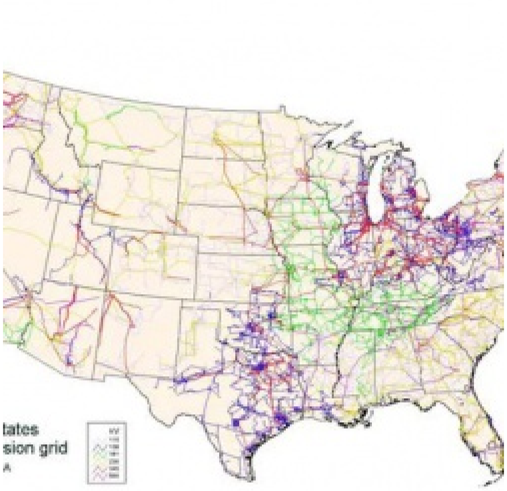
Published on *American Council on Science and Health* (https://www.acsh.org)

As Russians Target Our Electrical Grid, Here's What's Needed To Protect It

By ACSH Staff — August 8, 2018



Credit: Rolypolyman [1]

The U.S. electricity grid is hard to defend because of its enormous size and heavy dependency on digital communication and computerized control software. The number of potential targets is growing as “internet of things” devices, such as smart meters, solar arrays and household batteries, connect to smart grid systems.

As researchers of grid security, we believe that current security standards mandated by federal regulations provide sufficient protection against observed threats. But recent incidents demonstrate the ongoing challenge of ensuring everyone follows the guidelines, which themselves must change over time to keep up with technological shifts.

The threat is real: In late 2015 and again in 2016, Russian hackers shut down parts of Ukraine’s power grid. In March 2018, federal officials warned that Russians had penetrated the computers of multiple U.S. electric utilities [2] and were able to gain access to critical control systems. Four months later, the Wall Street Journal reported that the hackers’ access had included privileges that were sufficient to cause power outages [3].

Specific technical details have not yet been made public, so it’s hard to know exactly what the hackers did or gained access to. What has been revealed is that these breaches were accomplished with common hacking techniques, such as sending spearphishing emails to specific employees [4]. Apparently, and reassuringly, the U.S. attacks didn’t involve more advanced techniques seen in the Ukraine incidents [5], including custom-made software to target specific systems [6].

In addition, human errors will inevitably lead to mistakes that will weaken the security of some of the thousands of digital devices needed to protect the grid. And more sophisticated attackers may still find and exploit currently unknown vulnerabilities. Therefore, it’s important for electric utilities, grid operators and vendors to remain vigilant and deploy multiple layers of defense.

Major players have some protections

There are two main aspects to grid architecture that need defending in different ways. The first element is the bulk power system, often referred to as the “transmission grid.” It connects high-capacity power plants, transmission wires and substations that collectively generate and transport huge quantities of electricity over hundreds or thousands of miles. The rest of the grid is made up of smaller distribution grids – connected with the bulk power system – delivering electricity to homes and businesses around the country. The strongest standards for protection apply only to the bulk power system; though many distribution systems follow the same guidelines, they remain optional.

U.S. federal rules, as well as those set by the agency that governs the North American grid – which also includes large parts of Canada – require companies operating elements of the bulk power system to follow certain basic cybersecurity measures [7], including monitoring their networks to detect intrusions and mandating two-factor authentication for user logins.

Many large utilities do even more, assessing their risks in standardized ways [8] and practicing responses to computer intrusions [9]. These exercises often include hundreds of companies and organizations rehearsing how to collaborate to detect and confine attacks and restore service to customers.

[10]

Companies operating power plants, like this one in Oklahoma, need to remain on top of cybersecurity threats. *AP Photo/Sue Ogrocki* *[11]*

Smaller companies are more vulnerable

Because transmission grid utilities should already have some protections against network intrusions, it is likely that the Russian hackers looked elsewhere, infiltrating smaller distribution utilities. If that's so, any potential power shutdown or other problems in those systems would be confined to smaller areas – like towns or cities. That, in turn, means fewer customers would be affected, with less work needed to get power back on.

But it highlights a worrying reality: Smaller and midsized companies that operate electricity distribution systems often have inadequate resources to invest in full cybersecurity protections. The more than 3,000 utilities in the U.S. [12] have trouble finding sufficiently skilled workers who understand how the computerized and physical components of the grid work together and how to protect them.

In addition, utilities rely on complex supply chains to provide equipment, software, maintenance and other business functions. These external contractors and vendors may not implement protections as rigorous as the utilities. And their computer systems often have connections to the utilities' networks, which may be considered trusted and safe, rather than potential avenues of attack.

Stepping up defenses

Fixing all these potential problems is complex. First, all utility companies – even the smallest – should adopt basic security protections [13] like those required of large utilities. Some states are moving to require this of the power companies serving their residents, but many aren't yet. Further, we recommend all companies that are part of the grid participate in coordinated grid exercises to improve cybersecurity preparedness and share best practices.

In addition, all utility companies need to take steps to ensure the hardware and software they use are from trustworthy sources [14] and have not been tampered with or modified [15] to allow unauthorized users in.

It won't be enough to protect against today's threats. Adversaries are likely to employ increasingly sophisticated techniques that exploit both computer and human vulnerabilities. Companies need to ensure they engage in what might be called sustainable cybersecurity – ongoing processes that let systems and staff adapt over time, to stay ahead of the threats.

Researchers have an important role too, exploring ways that emerging technologies like cloud computing, blockchain and big-data analytics could help reduce risks without introducing any additional weaknesses. Further, researchers should identify more advanced ways to secure the grid, and reduce these systems' complexity, which would limit both current risks and future unknowns.

By Manimaran Govindarasu [16], Professor of Electrical and Computer Engineering, Iowa State University<, and Adam Hahn [17], Assistant Professor of Electrical Engineering and Computer Science, Washington State University. Professor Govindarasu receives funding from US Department of Energy, US National Science Foundation, and US Department of Homeland Security. He is affiliated with Institute for Electrical and Electronics Engineers (IEEE), Power System Engineering Research Center (PSERC), and Illinois Commerce Commission's NextGrid Study Group. Professor Hahn receives funding from the US Department of Energy, US National Science Foundation, and US Department of Homeland Security. He is affiliated with the Institute for Electrical and Electronics Engineers (IEEE), and the Illinois Commerce Commission's NextGrid Study Group. This article was originally published on The Conversation. Read the original article [18]
.

Source URL: https://www.acsh.org/news/2018/08/08/russians-target-our-electrical-grid-heres-whats-needed-protect-it-13281
Links

[1] https://commons.wikimedia.org/wiki/File:UnitedStatesPowerGrid.jpg

[2] https://www.us-cert.gov/ncas/alerts/TA18-074A

[3] https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110?source=acsh.org

[4] https://arstechnica.com/information-technology/2017/07/dhs-fbi-warn-of-attempts-to-hack-nuclear-plants/?source=acsh.org target=

[5] https://dragos.com/blog/crashoverride/CrashOverride-01.pdf?source=acsh.org target=

[6] https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/?source=acsh.org target=

[7] https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx?source=acsh.org target=

[8] https://www.nist.gov/cyberframework

[9] https://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20IV%20Public%20Lessons%20Learned%20Report.pdf

[10] https://images.theconversation.com/files/230606/original/file-20180803-41327-vl41fm.jpg?ixlib=rb-1.1.0&amp;q=45&amp;auto=format&amp;w=1000&amp;fit=clip

[11] http://www.apimages.com/metadata/Index/Tax-Overhaul-Utilities-Things-to-Know/953e50c11cfc49b2ada56fe7ddd37add/67/0

[12] https://www.energy.gov/sites/prod/files/2015/12/f28/united-states-electricity-industry-primer.pdf

[13] https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[14] https://www.nerc.com/pa/Stand/CIP0103RD/Implementation_Plan_Clean_071117.pdf

[15] https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01

[16] https://theconversation.com/profiles/manimaran-govindarasu-339555

[17] https://theconversation.com/profiles/adam-hahn-339561

[18] https://theconversation.com/as-russians-hack-the-us-grid-a-look-at-whats-needed-to-protect-it-100489