Protecting the power grid from cyber attacks

September 25 2018, by Paula Owen

Credit: CC0 Public Domain

As the national power grid becomes increasingly dependent on computers and data sharing—providing significant benefits for utilities, customers, and communities—it has also become more vulnerable to both physical and cyber threats.

While evolving standards with strict enforcement help reduce risks, efforts focused on response and recovery capabilities are just as critical—as is research aimed at creating a well-defended next generation smart grid. The Daily Herd recently sat down with Michael Ahern to discuss the many challenges involved in securing the national power grid against physical and cyber attacks—both now and in the future.

In addition to his role as director in WPI's Corporate and Professional Education and instructor for the Foisie Business School, Ahern also leads a WPI research team supporting BAE Systems as part of the Defense Advanced Research Project Agency's Rapid Attack Detection, Isolation, and Characterization Systems (DARPA RADICS) intitative.

What is being done in the U.S. to protect the power grid from cyberattacks?

Here in the U.S., a lot is being done to protect the power grid from cyberattacks. The power grid, or electric transmission system, is required to meet the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) Standards. These standards include mandatory requirements for specific actions to protect the power grid from both physical and cyberattacks. CIP Standards are updated regularly to address emerging threats and are vigorously enforced by independent auditors backed by Federal Energy Regulatory Commission [FERC] fines for noncompliance.

The result of these regulations and their enforcement is reduced risk of attacks that create widespread power outages.

Even with these evolving standards, cybersecurity is like a race that never ends. Attackers are learning and building their capabilities, too.

Many nation states and rogue organizations are developing their cyberattack capabilities. We've seen attacks against power grid control systems create widespread outages twice in Ukraine. Recently, the U.S. Department of Homeland Security reported attempts to insert malware in our electric power control systems.

The U.S. recognizes the risk that other nations may develop cyberattacks the industry is unable to stop. One initiative DARPA launched several years ago is called Rapid Attack Detection, Isolation, and Characterization Systems [RADICS], research to develop technology that cybersecurity personnel, power engineers, and first responders can utilize to accelerate restoration of cyber-impacted electrical systems.

Overall, the U.S. industry is improving defenses and the U.S. government is conducting research to add new restoration capabilities.

What are the risks if attempts to disrupt the power grid are successful?

Clearly, power grid outages are disruptive. Not only do we lose the lights, after a few days, we may lose water treatment capabilities and also find it difficult to find an open gas station to refuel our cars and trucks. If a nation can do this, it can make coercive threats against other nations without actually going to war.

How can the U.S. better protect against such attacks?

With attackers learning and developing, defenses for all types of critical infrastructure control systems—including water, gas, and transportation—must improve just to keep pace.

On a personal level, we would all do well to learn to protect ourselves

from cybertheft with malware like ransomware. Most of these attacks start with phishing to get us to install their malware and then exploiting an existing software vulnerability. The top few things we should all do to better protect ourselves include hovering over links and checking to see where these links are sending our internet browser before we click; having a questioning attitude about any and all information requests (never give away your ID and password); and quickly installing software patches and updates to apps to eliminate known vulnerabilities.

Provided by Worcester Polytechnic Institute