**Pentagon Up at Night**

A detailed look at why computers running the U.S. electrical infrastructure are so vulnerable to digital threats

By [Michael McElfresh](http://www.scientificamerican.com/author/michael-mcelfresh/), [The Conversation](http://www.scientificamerican.com/author/the-conversation/) on June 8, 2015



[*Scott Wylie/Flickr*](https://www.flickr.com/photos/scotbot/7573955488/in/photolist-cxhv6s-6GWjW6-hM6EQS-bQdz8Z-52J4zu-aLKvn-e8e8zs-5a2qqi-hM6Unv-54bcDZ-pnRU2x-hM7fX1-73ZaKr-b8jCca-hM7Vw2-5297gw-cvf8Ps-mU8rkD-e6LjZq-mUaw7i-hM6kzu-bpnHNo-cxhuz9-sPZfAS-seKU36-bpnLR1-524R7D-q64p8P-p6mWb1-bpnLbb-837bnr-pkPCJL-6PNYma-hM7drX-hM5noR-oP1ADb-pmAysj-hM6gjf-r2GhcV-hM6zFq-mAEnvE-oVx1Uw-hM7mYg-5giNsp-g1N87i-54ftny-g1MEMz-ogYmxs-hM69cu-6QrynR)

Advertisement

The following essay is reprinted with permission from [The Conversation](https://theconversation.com/uk), an online publication covering the latest research.

It’s very hard to overstate how important the US power grid is to American society and its economy. Every critical infrastructure, from communications to water, is built on it and every important business function from banking to milking cows is completely dependent on it.

And the dependence on the grid continues to grow as more machines, including equipment on the power grid, get connected to the Internet. A [report](https://www.thepresidency.org/sites/default/files/Grid%20Report%20July%2015%20First%20Edition.pdf) last year prepared for the President and Congress emphasized the vulnerability of the grid to a long-term power outage, saying “For those who would seek to do our Nation significant physical, economic, and psychological harm, the electrical grid is an obvious target.”

The damage to modern society from an extended power outage can be dramatic, as [millions of people found](http://energy.gov/articles/hurricane-sandy-noreaster-situation-reports) in the wake of Hurricane Sandy in 2012. The Department of Energy earlier this year said cybersecurity was one of the [top challenges facing the power grid](http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf), which is exacerbated by the interdependence between the grid and water, telecommunications, transportation, and emergency response systems.

So what are modern grid-dependent societies up against? Can power grids survive a major attack? What are the biggest threats today?

The grid’s vulnerability to nature and physical damage by man, including a [sniper attack in a California substation](http://www.mercurynews.com/business/ci_26419083/pg-e-substation-san-jose-that-suffered-sniper) in 2013, has been repeatedly demonstrated. But it’s the [threat of cyberattack](http://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system) that keeps many of the most serious people up at night, including the [US Department of Defense](http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).

**Why the grid so vulnerable to cyberattack**  
Grid operation depends on control systems—called Supervisory Control And Data Acquisition (SCADA)—that monitor and control the physical infrastructure. At the heart of these SCADA systems are specialized computers known as programmable logic controllers (PLCs). Initially developed by the automobile industry, PLCs are now ubiquitous in manufacturing, the power grid and other areas of critical infrastructure, as well as various areas of technology, especially where systems are automated and remotely controlled.

One of the most well-known industrial cyberattacks involved these PLCs: the attack, discovered in 2010, on the centrifuges the Iranians were using to enrich uranium. The [Stuxnet computer worm](http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/), a type of malware categorized as an Advanced Persistent Threat (APT), targeted the Siemens SIMATIC WinCC SCADA system.

Stuxnet was able to take over the PLCs controlling the centrifuges, reprogramming them in order to speed up the centrifuges, leading to the destruction of many, and yet displaying a normal operating speed in order to trick the centrifuge operators. So these new forms of malware can not only shut things down but can alter their function and permanently damage industrial equipment. This was also demonstrated at the now famous [Aurora experiment](http://en.wikipedia.org/wiki/Aurora_Generator_Test) at Idaho National Lab in 2007.

Securely upgrading PLC software and securely reprogramming PLCs has long been of concern to PLC manufacturers, which have to contend with malware and other efforts to defeat encrypted networks.

The oft-cited solution of an air-gap between critical systems, or physically isolating a secure network from the internet, was precisely what the Stuxnet worm was designed to defeat. The worm was specifically created to hunt for predetermined network pathways, such as someone using a thumb drive, that would allow the malware to move from an internet-connected system to the critical system on the other side of the air-gap.

**Internet of many things**  
The growth of smart grid – the idea of overlaying computing and communications to the power grid—has created many more access points for penetrating into the grid computer systems. Currently knowing the provenance of data from smart grid devices is limiting what is known about who is really sending the data and whether that data is legitimate or an attempted attack.

This concern is growing even faster with the Internet of Things (IoT), because there are many different types of sensors proliferating in [unimaginable numbers](http://www.pewinternet.org/2014/05/14/internet-of-things/). How do you know when the message from a sensor is legitimate or part of a coordinated attack? A system attack could be disguised as something as simple as a large number of apparent customers lowering their thermostat settings in a short period on a peak hot day.

Defending the power grid as a whole is challenging from an organizational point of view. There are about 3,200 utilities, all of which operate a portion of the electricity grid, but most of these individual networks are interconnected.

The US Government has set up numerous efforts to help protect the US from cyberattacks. With regard to the grid specifically, there is the Department of Energy’s Cybersecurity Risk Information Sharing Program ([CRISP](http://energy.gov/articles/energy-department-releases-new-guidance-strengthening-cybersecurity-grid-s-supply-chain)) and the Department of Homeland Security’s National Cybersecurity and Communications Integration Center ([NCCIC](https://www.us-cert.gov/nccic)) programs in which utilities voluntarily share information that allows patterns and methods of potential attackers to be identified and securely shared.

On the technology side, the National Institutes for Standards and Technology ([NIST](http://www.nist.gov/smartgrid/)) and IEEE are working on smart grid and other new technology standards that have a strong focus on security. Various government agencies also sponsor research into understanding the attack modes of malware and better ways to protect systems.

But the gravity of the situation really comes to the forefront when you realize that the Department of Defense has stood up a new command to address cyberthreats, the United States Cyber Command ([USCYBERCOM](https://theconversation.com/www.stratcom.mil/factsheets/2/Cyber_Command/%0Ahttp:/en.wikipedia.org/wiki/United_States_Cyber_Command)). Now in addition to land, sea, air, and space, there is a fifth command: cyber.

The latest version of The Department of Defense’s [Cyber Strategy](http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf) has as its [third strategic goal](http://www.defense.gov/home/features/2015/0415_cyber-strategy/Department_of_Defense_Cyber_Strategy_Fact_Sheet.pdf), “Be prepared to defend the US homeland and US vital interests from disruptive or destructive cyberattacks of significant consequence.”

There is already a well-established theater of operations where significant, destructive cyberattacks against SCADA systems have taken place.

In a 2012 report, the National Academy of Sciences called for more research to make the grid more resilient to attack and for utilities to modernize their systems to make them safer. Indeed, as society becomes increasingly reliant on the power grid and an array of devices are connected to the internet, security and protection must be a high priority.

This article was originally published on [The Conversation](http://theconversation.com/). Read the [original article](https://theconversation.com/can-the-power-grid-survive-a-cyberattack-42295).