**Five Reasons The U.S. Power Grid Is Overdue For A Cyber Catastrophe**

As other major industries one by one fall victim to hackers, the U.S. electrical-power generation and distribution system seems remarkably insulated from cyber threats. A March 24 story in *USA Today* reported that out of 362 attacks on the power grid over the last four years, only 14 were cyber attacks and “there has never been a successful attempt to cause a power outage through a cyber attack in the United States.”

However, a big attack is coming. The intelligence community has noted a rising incidence of assaults on the industrial control mechanisms used to operate the grid, more and more of which are linked in some fashion to the internet. Industry officials admit that data bases recording the frequency of attacks are unreliable because there is no standard definition of what constitutes a cyber-attack and utilities are reluctant to report vulnerabilities. Chances are, the networks supporting grid operations are probed every day by outsiders, often with nefarious intent.

The balkanized architecture of the current grid — there are actually three grids fed by 7,000 generating plants and 2,000 distribution utilities — provides some protection against widespread outages. Unfortunately, efforts to protect the system are similarly fragmented. So it is just a matter of time before the finger-pointing starts in the aftermath of a cyber-induced blackout. Here are the top five reasons why “the big one” is coming.

**1. Nothing works without the power grid.** When the Army’s Air War Plans Division put together America’s first strategic bombing campaign during nine sweltering days in the summer of 1941, the number-one target on its list of “primary objectives” was the German electrical grid. Steeped in the science of finding bottlenecks in the Axis economy and social fabric, military planners saw that without electricity, every facet of the enemy’s war effort would grind to a halt.

They weren’t so successful at selling that strategy to Army higher-ups or actually hitting electric plants with their primitive bombsights, but those are not issues for today’s hackers. They understand that if you take down the grid, every other network that matters will collapse with it. The Department of Homeland Security identifies 16 “critical infrastructures” supporting the U.S. economy, but the electric grid is the most basic — everything else from medicine to finance to transportation depends on it. Thus, it is the most “lucrative” target for hackers seeking to achieve devastating effects.



*With 450,000 miles of high-voltage transmission lines, the U.S. electrical grid is intrinsically vulnerable to upset from severe weather, mechanical failures and wandering wildlife. But cyber attacks could be the danger that ultimately becomes the grid’s undoing. (Image: Pixabay)*

**2. The current grid has numerous vulnerabilities.** The U.S. electrical grid still reflects its origins as a decentralized network owned by numerous local operators. Security standards vary from utility to utility, as does awareness of cyber threats at the state-level commissions regulating the industry. Regulators at the federal level have traditionally deferred to industry in determining what level of protection is prudent, and even though that is now beginning to change, authorities are limited, standards are nascent, and definitions of who must comply leave out large swaths of the grid.

In other words, the U.S. power grid is full of seams that can be exploited by hackers — especially state-sponsored agents who have the skill and resources to penetrate complex networks. It would be challenging to mount a nationwide cyber assault because Con Edison has different operating features than Pacific Gas & Electric — including different software systems — but even with circuit breakers installed on major interconnect routes, it might be feasible to cause cascading outages across the grid. More permanent damage, such as that wrought by the Stuxnet virus in Iran’s nuclear program, cannot be discounted.

**3. New technologies make the danger worse.** The U.S. power grid is undergoing a renaissance as digital technologies are introduced to enhance reliability and efficiency. However, a June report from the Congressional Research Service warned some of those technologies could make the grid more susceptible to cyber assaults:

*As the grid is modernized and the Smart Grid is deployed, new intelligent technologies utilizing two-way communications and other digital advantages are being optimized by Internet connectivity. Modernization of many [industrial control] systems also has resulted in connections to the Internet. While these advances will improve the efficiency and performance of the grid, they also will increase its vulnerability to potential cyberattacks.*

As in other industries, the increasing use of mobile devices by utility managers and the shift to cloud computing could create new avenues for cyber exploits. Some experts also think the Internet of Things connecting electrical appliances and other equipment could provide opportunities for hackers. Beyond that, the growing contribution of renewable energy sources to electricity generation adds to the complexity of grid operations. With so many internet-connected innovations being introduced across a decentralized network and diverse workforce, it is nearly impossible to enforce the kind of consistent security standards that would minimize danger from cyber attacks.

**4. Industry financial incentives are weak.** Historically, the main threats to the U.S. power grid have come from bad weather, mechanical failures, human error, wandering wildlife and physical attacks (like the vandals who recently shot up an electrical substation near Silicon Valley). Cyber attacks have not been a big concern. In fact, I heard one industry executive say that squirrels were a bigger threat to the system. So it shouldn’t come as a surprise that few investor-owned utilities have implemented cyber protections beyond the minimal standards required by current regulation.

The federal government’s 2011 *Roadmap to Achieve Energy Delivery Systems Cybersecurity* noted that “making a strong business case for cybersecurity investment is complicated by the difficulty of quantifying risk in an environment of rapidly changing, unpredictable threats with consequences that are hard to demonstrate.” Because power companies typically operate as state-regulated utilities whose profits are closely scrutinized, industry executives have to be convinced it makes sense to invest in protection against a threat that looks largely hypothetical today. The high cost of installing necessary hardware and software, coupled with the challenge of training workers in good network “hygiene,” is a powerful disincentive to addressing the danger.

**5. The regulatory structure dilutes oversight.** The lead national agency for enforcing power-grid cybersecurity standards is the Federal Energy Regulatory Commission, which also oversees interstate transport of oil and gas. FERC in principle can mandate measures for securing critical infrastructure recommended by the North American Electric Reliability Corporation, an industry organization established after a major blackout in 1965. However, according to the June congressional report, “FERC still asserts that it does not have the authority to act quickly in the event of a major cyber event.” Even before such an event unfolds, FERC must reconcile its regulatory exertions with those of other federal agencies (such as the Department of Homeland Security), powerful state-level commissions, and industry bodies.

So the regulatory standards for cyber defense of the grid are a bit uneven. For instance, the protections required in the core assets of the bulk energy system are more demanding than those imposed on some local distribution facilities, even though the local assets are connected to the bulk system. Richard Campbell, the author of the congressional study, observes that “because there are no mandatory standards of protection for distribution facilities below the bright-line threshold, these potentially ‘less protected’ seams of the [bulk energy system] may provide a backdoor to cyber intrusions to the grid.”

The bottom line is that the U.S. power grid will remain vulnerable to cyberattack for the foreseeable future, and may become more vulnerable as new technologies couple it more closely to the internet. It is ironic that the grid’s decentralized architecture may be its best defense against a nationwide blackout, but that same feature impedes the ability of managers to see when a major attack is under way, and respond appropriately. It probably will not be long before the weaknesses in the current structure lead to some sort of cyber catastrophe. But don’t count on hearing about it quickly, because you may not have any electricity.