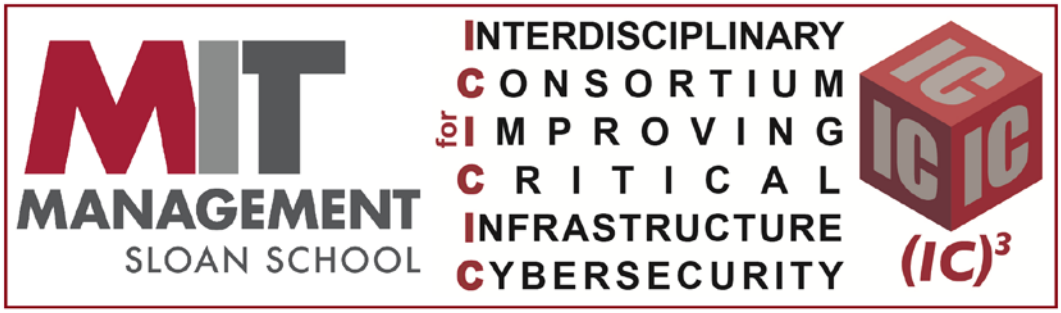


Preparing for the Cyberattack That Will Knock Out U.S. Power Grids

Stuart Madnick

Working Paper CISL# 2017-07

May 2017

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

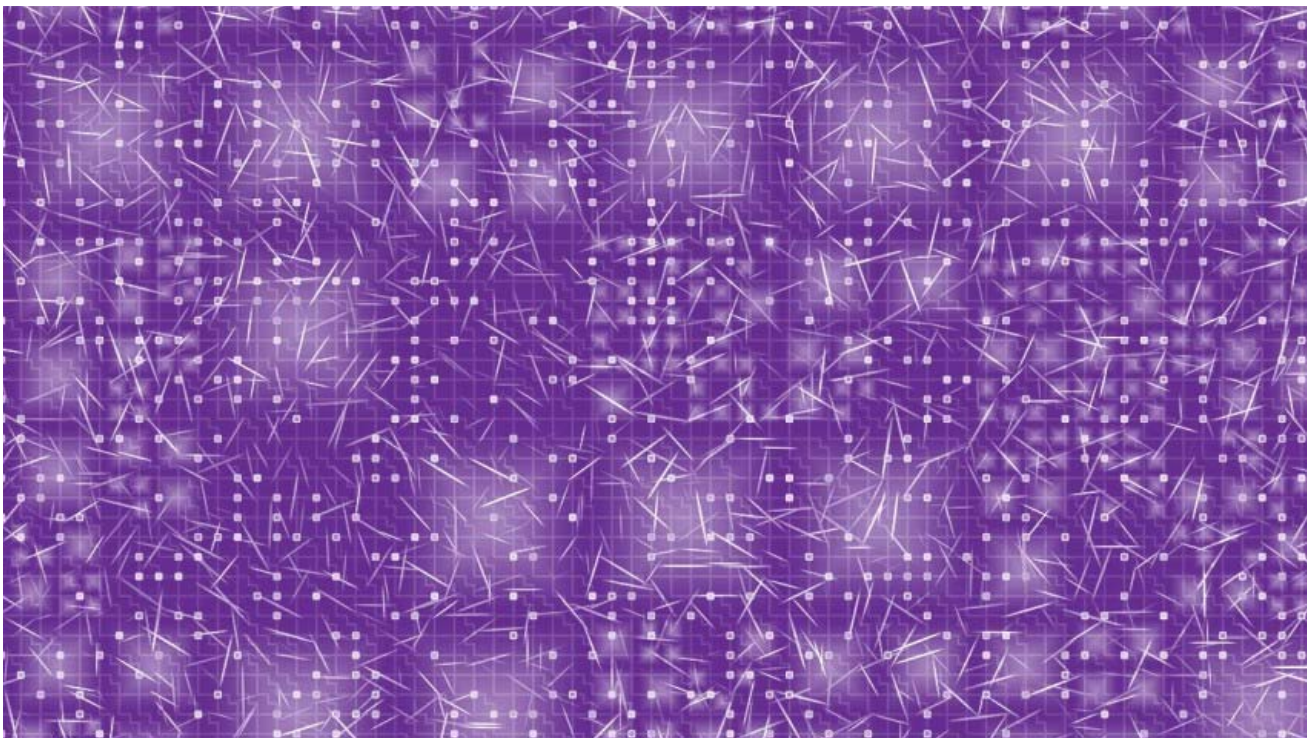
Harvard Business Review

GOVERNMENT

Preparing for the Cyberattack That Will Knock Out U.S. Power Grids

by Stuart Madnick

MAY 10, 2017



Cyberattacks are unavoidable, but we're not going to stop using computerized systems. Instead, we should be preparing for the inevitable, including a major cyberattack on power grids and other essential systems. This requires the ability to anticipate not only an unprecedented event but also the ripple effects that it could cause.

Here's an example of second-order effects (though not caused by a cyberattack, they're a good way to think through what could happen in an attack). In February 2017, an area of Wyoming was hit by a strong wind storm that knocked down many power lines. It took about a week to restore power, due to heavy snow and frozen ground. Initially, water and sewage treatment continued with backup generators. But the pumps that moved sewage from low-lying areas to the treatment plants on higher ground were not designed to have generators, since they could hold several days' worth of waste. After three days with no power, they started backing up. The water then had to be cut off to prevent backed-up waste water from getting into homes. The area had never lost power for so long, so no one had anticipated such a scenario.

Now think about what would happen if a cyberattack brought down the power grid in New York, for example. New Yorkers could manage for a few hours, maybe a few days, but what would happen if the outage lasted a week or more? For an example of the kind of disruption such an attack could cause, consider the 2011 Japanese tsunami. It knocked out both the power lines and the backup generators at the same time. Either event could have been managed, but both

occurring at the same time was a disaster. Without power, the cooling systems in three nuclear reactors failed, resulting in massive radiation exposure and concerns about the safety of food and water. The lesson: We need to prepare not only for an unexpected event but also for the possible secondary effects.

Based on conversations I've had with experts in the field, preparedness for a major cyberattack like this is low, regardless of whether you're talking about the regional or city level, or the private sector. As Lawrence Susskind, a professor in MIT's urban systems department, described it to me, "Millions...could be left with no electricity, no water, no public transportation, and no waste disposal for weeks (or even months) .... No one can protect critical urban infrastructure on their own. Nobody, though, is showing any leadership."

In our research consortium at MIT Sloan, we have been studying ways that massive physical damage can happen to power grids and other industrial control systems through a cyberattack. The potential for massive damage is alarming, to say the least. The scenario of losing power for a long time — weeks or even months — is not unthinkable. We went through this recently at MIT when the institute's cogeneration facility had a turbine failure. It wasn't due to a cyberattack, but rather to a mechanical failure from a defective nozzle. It took three months to source the necessary parts from Germany and fix the turbine, even though the possibility of such a failure was more likely to be expected than a first-of-its-kind cyberattack might be.

You may be wondering why a major cyberattack of this nature hasn't already occurred. There are three necessary conditions for it to happen: opportunity, capability, and motivation. There are

plenty of opportunities to launch a cyberattack, as Iran learned when its uranium enrichment facility was attacked by Stuxnet. There is also plenty of capability out there. As I sometimes say, "The good guys are getting better, but the bad guys are getting badder faster." The tools to accomplish attacks are increasingly available on the dark web at decreasing costs, including troves of cyber tools stolen from the NSA and CIA. Just look at the Ukraine power grid attack in 2015, where the attackers used several different techniques, such as spear phishing and denial-of-service attacks, that were all readily available on the black market of the internet.

So, our saving grace at the moment is motivation. While there are some state actors who might *want* to shut down a major power grid in another country, the possibility of retaliation acts as a deterrent. But that equation changes when you consider actors like North Korea or ISIS, or any disgruntled group in the world that might proceed regardless of the consequences. Even criminals are an increasing risk. Here in the Boston area, we have seen ransomware attacks on local police departments. How much "protection" might the governor pay to prevent a state-wide shutdown of essential services like power generation? Questions we should all be asking include: If the power grid is breached and all the electric-start generators fail too, what do we do? What's the backup plan for the backup plan? What happens to our food supply? Our water supply? Our sewer systems? Our financial systems? Our economy?

When it comes to being prepared for a significant cyberattack, there are three essential elements. Some are actions that we can take on our own, such as having backups in place for key systems and for secondary systems. Some are actions best undertaken by government, such as guidance on the important steps to take

when a major cyberattack happens. Finally, there are things that require public-private collaboration. For example, the NIST Cybersecurity Framework provides companies with guidelines on cyber protection, but companies need to determine what actions to take. Much more is needed, beyond the current NIST framework, to address the specific threats that I have described.

This isn't rocket science. But it does involve systems-level thinking about how everything is connected, and considering the layers of interdependencies. For example, hospitals might have backup generators, but what about the supply line for refueling? If the refueling stations need electricity to operate pumps, what is the plan? A few states, including Florida, have introduced regulations to address this concern, but only for outages of 72 hours.

We need innovative, systems-level thinking – and a sense of urgency – to mitigate the impact of a major cyberattack. And we need it now.

Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, a Professor of Engineering Systems in the MIT School of Engineering, and the academic director of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, aka (IC)^3. He is also a frequent speaker at the MIT Sloan CIO Symposium.