NATIONAL CENTER FOR POLICY ANALYSIS

Cyber Threats to the Texas Electric Grid

Issue Brief No. 199 by David Grantham and Luke Twombly September 21, 2015

Texas plays a unique role in America's infrastructure as the only state with a self-contained electric grid. [See Figure I.] The entire U.S. electric power system is a prime target of cyberattacks from hostile governments and terrorist organizations, but the Lone Star State is in a unique position to act.

Dallas Headquarters:
14180 Dallas Parkway, Suite 350
Dallas, TX 75254
972.386.6272

www.ncpa.org

Washington Office:
202.830.0177
governmentrelations@ncpa.org

The Consequences of a Vulnerable Grid. The Northeast blackout in 2003 left nearly 55 million residents of the United States and Canada temporarily without power. Crews traced the cause to a software error at a utility control room in Ohio and restored power after two days to most of those affected. But the blackout disrupted transportation in many areas, cut off city water in several locations, and hampered emergency services. Experts attributed 10 deaths to the blackout, which cost more than $10 billion.[1]

Remember: For many, this blackout only lasted a few days. And there was no significant damage to sensitive infrastructure. However:

- Any serious injury to important power equipment could create a blackout lasting for at least one year "given the nation's current state of unpreparedness," argues Peter Pry, a former executive of the Task Force on National and Homeland Security.[2]
- The Obama administration remains "unwilling to empower competent authorities to combat the adversaries within the grid environment," according to the assessment of George Cotter, the founding director of Department of Defense Computer Security Center.[3]
- The Pentagon's current information security strategy is nothing more than "patch and pray," said Arati Prabhakar, the Director of Defense Advanced Research Projects Agency (DARPA), in 2015.[4]

The Cost of Cyber Attacks. Malicious cyber activity costs the U.S. economy upward of $100 billion and over half a million jobs every year. According to Keith Burkhardt, vice president of Kraus-Anderson Insurance, 60 percent of companies that suffer a data breach are out of business within six months.[5]

The grid remains a prime target of this cyber offensive. A Ponemon Institute report explains that the annualized cost of cybercrime for the energy and utilities sector averaged approximately $21 million from 2009-2014. That number increased roughly 28 percent in 2015 to $27 million.[7] The jump in costs came in second only to the financial services industry, which saw the average annual cost of cyberattacks jump from $19.37 million to $28.33 million (a 30 percent increase). [See Figure II.] [8]

The ubiquity of cyberattacks suggests a strike against the Texas grid is far more probable than an electromagnetic pulse (EMP) attack or physical assaults against substations. A report from the Institute for Critical Technology Infrastructure argues that Islamic terrorists and antagonist governments are more likely to employ cyberattacks against vital infrastructure simply because malicious code can achieve an impact similar to physical assault with fewer costs and less logistical coordination.[9]

The Evolving Cyber Threat. Russian intelligence infected 1,000 power plants in Western Europe and the United States in July 2004 with a so-called "dragonfly" computer virus. Cyber experts found that the malware was not designed to damage power stations, leading them to believe Russia was merely probing western grid defenses.[10] Skeptics pointed to the lack of physical damage as evidence that malicious cyber capabilities remain largely incapable of physical damage and, thus, unlikely to cause a major electric shutdown.[11]

Russian Attack on Ukraine. In December 2015, a watershed moment occurred when Russian hackers successfully triggered a massive blackout in Ukraine that left 300,000 people without electricity and water for several hours.[12] Researchers from antivirus specialist ESET reported that multiple Ukrainian power authorities were infected by "BlackEnergy" — malware that can destroy fundamental parts of a hard drive and industrial control centers, while providing the attacker permanent access to infected computers.[13]

The improved sophistication in the 11 years separating the two attacks proved that the intent and capability of malicious code had graduated from data manipulation and disruption to physical damage.

Stuxnet Attack on Iran. Adam Segal writes in the *Hacked World Order* that malicious code capabilities more and more aim to cause material injury, especially state-sponsored cyber weapons.[14] For instance, the Stuxnet worm — allegedly developed and deployed by the U.S. and Israeli governments — launched against the Natanz nuclear site in Iran in 2010 caused 1,000 centrifuges to spin uncontrollably at high rates of speed until they tore themselves apart. The creators of the malware achieved an effect that previously could only have been accomplished through a bombing campaign.[15]

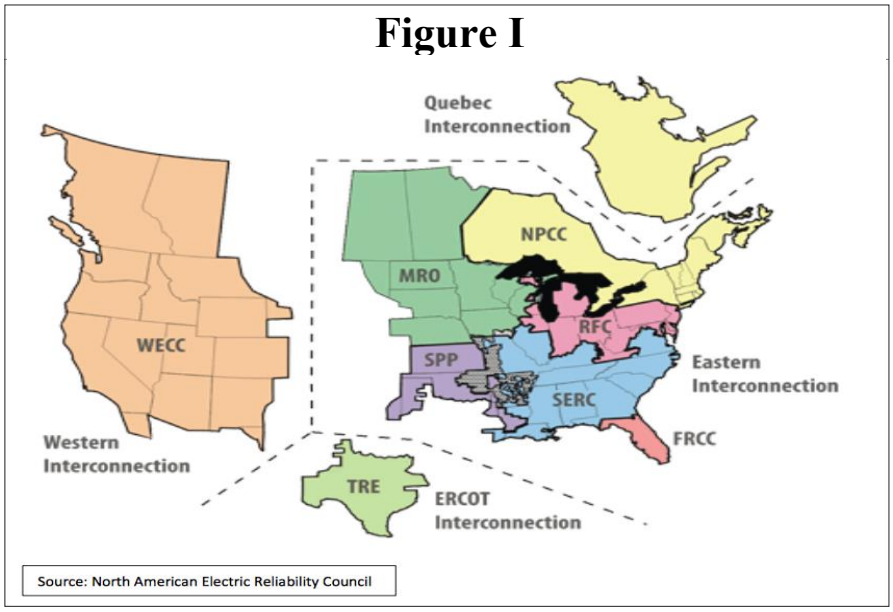
Stuxnet was subsequently released globally after an unwitting engineer at the Natanz site hooked up his infected computer to the web. The "escape" allowed experts to examine the sophisticated worm, and potentially gave bad actors the opportunity to replicate it or learn its intricacies in order to defend against it.[16] This exposure brings up a more important concern: the compressed time between the development of a sophisticated malicious code and its availability on the black market.

ISIS's Cyber Development. The Islamic State places great emphasis on the illicit acquisition of the latest malicious cyber tools and actively recruits well-trained information technology specialists for its Islamic State Hacking Group — a faction of the organization that coordinates cyberattacks against Western targets. ISIS also hosts a 24-hour cyber help desk for its less skilled followers and affiliates to learn hacking techniques.[17] The strategy appears to be working. A digital intelligence expert claimed recently that ISIS capabilities are "1,000 times what they were four years ago."[18]

ISIS hackers have also attempted to penetrate the U.S. grid. Although the attack failed miserably due to a lack of capabilities, the FBI fears ISIS could simply purchase the necessary malicious software on the black market.[19] More to the point, the Islamic State's interest in the grid underscores the vulnerability of America's infrastructure. In fact, the attempt on the grid should call into question its protections since terrorist organizations ordinarily focus their efforts on soft targets.

Vulnerabilities of the Texas Grid. The cyber threat to the Texas grid is specifically focused on the network's supervisory control

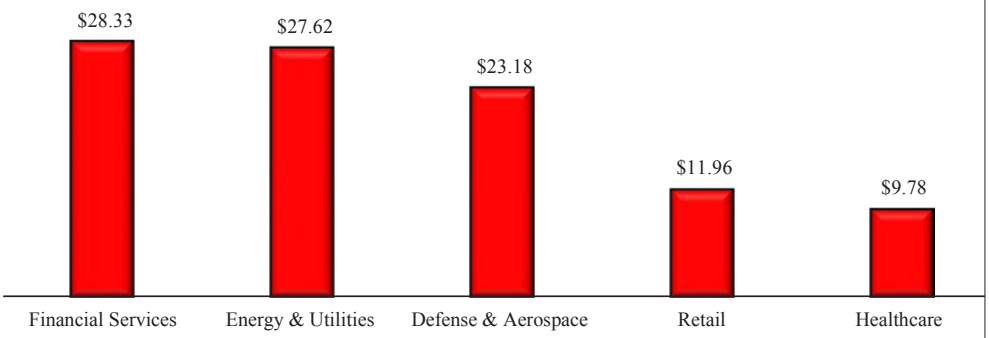
Figure I



Source: North American Electric Reliability Council

and data acquisition (SCADA) systems — small computers that run the electric grid and other critical infrastructure. SCADA systems, for instance, regulate the electric current that flows through transformers, the natural gas or water that runs through pipelines and the data traveling through communications and financial systems, among a host of other things.[20]

Figure II
Average Annualized Cost of Cyber Attacks by Industry, 2015 (millions of dollars)



Source: "2015 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2015, page 10.

The problem remains that experts have gradually incorporated 21st-century digital platforms into a grid system that is "older than the average car." This integration layered advanced technology atop an aged infrastructure, which exposed the grid to relentless cyberattacks and destructive malicious code — threats it was never designed to defend against.[21] Moreover, the older parts needed to repair the grid should destructive code cause damage are becoming more and more scarce.

Despite antivirus software and numerous firewalls, even the most basic cybercrime tactics can circumvent the current network protections and wreak havoc on the dated system. For instance, the delivery of an official-looking yet infected email that targets a specific user can trick the recipient into downloading a malicious attachment or convince them to visit a compromised website. This could be the only opening a hacker needs to co-opt and compromise the entire grid.

How Texas Can Protect Against Cyber. The state government and the Electric Reliability Council of Texas (ERCOT), the utility organization that manages the grid, could come together to craft policies to protect the grid. The most effective and affordable way to protect from cyberattack would also protect against both EMPs and solar storms.

Surge protectors — equipment that prevents electrical overloading of transformers — moves the solution beyond the expensive "digital arms race" of antivirus software to an affordable, long-lasting solution.[22] The installation of surge protectors nationwide would cost roughly $2 billion, according to the EMP Commission — a 2008 congressional committee established to examine the threat of EMP to the United States.[23] Given that Texas consumes almost 13 percent of the nation's electricity, it should cost roughly $260 million to equip the state's grid with the same protection.[24] Those costs equate to as little as 3 percent of the total cash currently held in Texas' so-called "rainy day fund."[25]

Newer technologies aimed at protecting the grid specifically from cyberattacks are also coming to market. Alex McEachern, president of Power Standards Lab, a California-based firm that evaluates energy and power quality, and collaborators at the University of California Berkeley and Lawrence Berkeley National Laboratory, developed a Rapid Attack Detection, Isolation and Characterization program: It is an independent and automated power grid defense system that watches from outside the network for "irregularities in the physical behavior of the grid itself."[26] The so-called phasor measurement unit (PMU) can synchronize and compile voltage and energy distribution data into a big-picture, real-time reading that could help identify harmful anomalies in the system. Workers could then isolate and defeat the problem before it compromises larger portions of the network.[27]

Conclusion. Texas legislators and utilities can no longer rely on reactive antivirus and intrusion detection policies pushed down from the federal government. They have the opportunity to craft comprehensive, state-level policies that would fortify the Texas grid against an advanced cyberattack. To borrow from Keith Burkhart, vice president and cyber risk strategist at Kraus-Anderson Insurance, the Texas grid must become cyber resilient. After all, Texas remains an integral part of the nation's security and economy.

David Grantham is a senior fellow and Luke Twombly is a research associate with the National Center for Policy Analysis.

Notes

1. "The Economic Impacts of the August 2003 Blackout," Electricity Consumers Resource Council, February 9, 2004; and David Grantham, "The Texas Grid and U.S. National Security," National Center for Policy Analysis, Backgrounder No. 182, May 2016.
2. Peter Pry, *Apocalypse Unknown: The Struggle to Protect America from an Electromagnetic Pulse Catastrophe* (CreateSpace Independent Publishing Platform, 2013), page 3.
3. Quoted from George R. Cotter's "Security in the North American Grid: A Nation at Risk," a white paper presented at the Data Center World Security Conference, April 8, 2015.
4. Mohana Ravindranath, "DOD's Current InfoSec Strategy Is Patch and Pray," DefenseOne, October 1, 2015.
5. Paul Taylor, "Cybercrime Costs US $100bn a year, report says," *Financial Times*, July 23, 2013.
6. L. Keith Burkhart, "The Intelligence of Cyber Resilience," *CIO Review*, June 12, 2015.
7. "2015 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2015, page 10.
8. Ibid.
9. James Scott and Drew Spaniel, T*he Anatomy of Cyber-Jihad: The New Great Equalizer*, Institute for Critical Infrastructure Technology, report, June 2016.
10. Peter Pry, "The EMP Threat: The State of Preparedness Against the Threat of a Electromagnetic Pulse (EMP) Event," Statement for the Record, Joint Hearing Before the Subcommittee on National Security and Subcommittee on the Interior, House Committee on Oversight and Government Reform, May 13, 2015.
11. Several experts believe different parties have hyped the threat. See Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013); and Kelsey D Atherton, "GOP Platform Vows to Protect U.S. From a Fantasy Weapon: An EMP Is an Empty Threat," *Popular Science*, July 11, 2016.
12. Katie Collins, "Ukraine Blackout is a Cyberattack Milestone," CNET, January 5, 2016.
13. Dan Goodin, "First known hacker-caused power outage signals troubling escalation," *Ars Technica*, January 4, 2016.
14. Adam Segal, *Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate* (New York: PublicAffairs, 2016), page 79.
15. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *International New York Times*, June 1, 2012.
16. Ibid.
17. James Scott and Drew Spaniel, *The Anatomy of Cyber-Jihad.*
18. Tim Johnson, "Computer hack helped feed an Islamic State Death List," McClatchyDC, July 20, 2016.
19. Jose Pagliery, "ISIS is attacking the U.S. energy gird (and failing)," CNN Money, October 16, 2015.
20. Peter Vincent Pry, "The EMP Threat: The State of Preparedness Against the Threat of a Electromagnetic Pulse (EMP) Event."
21. Matthew E. Luallen, "SANS SCADA and Process Control Security Survey," SANS Institute, February 2013; quoted in an interview with Melissa Ventrone, partner and cybersecurity expert, Thompson Coburn LLP.
22. Peter Vincent Pry, ed., Blackout Wars: State Initiatives to Achieve Preparedness Against an Electromagnetic Pulse Catastrophe, Task Force on National and Homeland Security, collection, page 72.
23. R. James Woolsey and Peter Vincent Pry, "The Growing Threat From an EMP Attack," *Wall Street Journal*, August 12, 2014.
24. "Guide to Electric Power," Houston Advanced Research Center, January 2003; authors' estimates.
25. Authors' estimates based on the number provided in Robert T. Garrett, "Texas rainy day fund overflows – and divides legislators," *Dallas Morning News*, March 20, 2015.
26. Peter Fairley, "Detecting Cybersecurity Threats by Taking the Grid's Pulse," *IEEE Spectrum*, July 12, 2016.
27. Ibid.