Lights Out: Securing National Infrastructure from Cyber Threats

Cellular and landline telephones service are overloaded or unavailable. Television and radio stations are off the air or running on generators. The water supply in several cities may be contaminated. Interstate passenger and commuter rail service is shut down. Gas stations are unable to pump fuel, causing numerous traffic and transport problems. Scores of factories are forced to close, creating larger supply problems. Disruptions to air transport, financial markets and hospitals are widespread.

This is not a emergency exercise scenario. It is what happened during the August 2003 blackout that brought life to a standstill for 55 million people in eight Northeast states and Canada. Strained power lines and overgrown trees in Ohio, and a previously unknown software flaw at one utility triggered a domino effect, forcing 100 power plants to shut down.[1] The blackout showed the extensive consequences of an accidental disruption to U.S. infrastructure. But what if the disruption had been intentional?

"The next world war might not start with a bang, but with a blackout."[2] Disabling a country's critical infrastructure can be an effective asymmetric threat tactic or part of a physical attack. According to a 2010 survey, more than half of IT security executives at 600 critical infrastructure providers reported their organizations being hit by large-scale cyber attacks or infiltrations.[3] "China and Russia routinely probe our industrial networks, looking for information and vulnerabilities to use as leverage in any potential dispute."[4] Additionally, the Stuxnet worm represents the next generation of cyber threats to critical infrastructure because it can change control systems and steal data, while undetected by infrastructure operators.

Critical infrastructure is vulnerable because of its massive scale, scope, and internet connectivity. The North American bulk power system, for example, is composed of more than 5,300 power plants that serve over 334 million people. In one survey, 62 percent of North American critical infrastructure providers reported that "their control systems were directly connected to an IP-based network or the Internet."[5]

Most critical infrastructure technology is challenging to protect and improvements will be slow going. Better equipped to deal with threats to facilities, most industrial control systems were developed when cyber security was not a priority. Architecture varies by operator and is often made up of various legacy systems. Critical infrastructure operations are uninterruptable and in real-time, making significant network security upgrades difficult. Vulnerabilities from COTS software in proprietary industrial control systems also present a threat. At this time, the electric sector is only critical infrastructure sector with cyber security standards. With over 85% of critical American infrastructure owned by private sector, public-private partnerships will be necessary to identify problems, share information, and create solutions.

"[I]t is imperative that organizations prepare for the instability that cyber attacks on critical infrastructure can cause," says McAfee CEO Dave DeWalt. "From public transportation, to energy to telecommunications, these are the systems we depend on every day. An attack on any of these industries could cause widespread economic disruptions, environmental disasters, loss of property and even loss of life."[6]

---

[1] Kevin Poulsen, "Software bug contributed to blackout," *SecurityFocus.com*, February 11, 2004, http://www.securityfocus.com/news/8016.
[2] Glenn Derene, "How vulnerable is U.S. infrastructure to a major cyber attack?" *Popular Mechanics*, October 1, 2009, http://www.popularmechanics.com/technology/military/4307521.
[3] Warwick Ashford, "Critical infrastructure under continual cyber attack, says report," *ComputerWeekly.com*, January 28, 2010, http://www.computerweekly.com/Articles/2010/01/28/240112/Critical-infrastructure-under-continual-cyber-attack-says.htm.
[4] Derene, op. cit.
[5] "Critical infrastructure is not prepared for cyber attacks," *Help Net Security*, November 11, 2008, http://www.net-security.org/secworld.php?id=6727.
[6] http://cacm.acm.org/news/69921-report-reveals-critical-infrastructure-under-constant-cyber-attack/fulltext