U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT
SUBCOMMITTEE ON ENERGY

HEARING CHARTER

Thursday, July 30, 2015
9:00 a.m. – 11:00 a.m.
2318 Rayburn House Office Building

PURPOSE

The Subcommittees on Oversight and Energy will hold a joint hearing titled *Examining Vulnerabilities of America's Power Supply* on Thursday, July 30, 2015, starting at 9:00 a.m. in Room 2318 Rayburn House Office Building. The purpose of this hearing is to examine the vulnerabilities of the national electric grid and the severity of various threats to the power supply if those threats are not adequately assessed and managed. The hearing will discuss various threats to the national electric grid, including: severe weather or other natural events; cyber, physical, or coordinated attacks; space weather; and electromagnetic pulse (EMP) attacks.

WITNESS LIST

- **Mr. Richard Lordan**, Senior Technical Executive, Power Delivery & Utilization Sector, Electric Power Research Institute
- **Ms. Nadya Bartol**, Vice President of Industry Affairs and Cybersecurity Strategist, Utilities Telecom Council
- **Dr. Daniel Baker**, Distinguished Professor of Planetary & Space Physics; Moog-BRE Endowed Chair of Space Sciences; Director, Laboratory for Atmospheric and Space Physics, University of Colorado Boulder
- **Dr. M. Granger Morgan**, Hamerschlag University Professor, Departments of Engineering and Public Policy and of Electrical and Computer Engineering, Carnegie Mellon University

BACKGROUND

The electricity infrastructure of the United States consists of power plants generating electricity, transmission and distribution lines, and transformers and substations, which all work together to bring power to American homes and businesses.

The stability, reliability, and security of the electric grid are important components to prevent extensive power outages that could interfere with the everyday lives of millions of Americans. However, the electric grid is vulnerable to a wide range of threats that could cut off power to families and businesses, including physical, cyber, EMP, and space weather threats.

Physical Threats

In August of 2003, a tree branch in Ohio – with the help of software issues and human error – caused a major power outage across the northeastern portion of the United States and part of Canada. The blackout was blamed for directly contributing directly to 10 deaths with further indirect impact on the surrounding population.[1] Even with one isolated incident, it took two days to return electricity to the entirety of the affected area.[2] After Superstorm Sandy in 2012, millions of people were left without power. Despite broad disaster relief efforts, it took thirteen days to restore power to at least 95 percent of customers in New York and eleven days to restore power to 95 percent of customers in New Jersey.[3]

In addition to natural events, man-made physical threats exist for the national grid. In 2013, unknown individuals led an attack on a Pacific Gas & Electric's Metcalf substation in California – severing six underground fiber optic lines and firing over 100 rounds of ammunition at transformers. The attack caused over $15 million in damage, but did not lead to any loss of power or life.[4]

Cybersecurity Threat

As the electric grid continues to be modernized and become more interconnected, the threat of a potential cybersecurity breach significantly increases. While there has been no reported cyber-attack that has resulted in widespread loss of power, there have been many attempted attacks. An investigation completed by USA Today earlier this year found that the United States' power grid "faces physical or online attacks approximately 'once every four days.'"[5] In addition, it appears that these cyber threats could be highly sophisticated. In 2014, the National Security Agency (NSA) reported that the agency had tracked intrusions into [industrial control] systems by entities with the technical capability "to take down control systems that operate U.S. power grids, water systems and other critical infrastructure."[6]

One area of potential vulnerability within the grid is the Supervisory Control and Data Acquisition (SCADA) systems, which have been in use since the 1970s. While, these systems have historically consisted of remote terminal units, which were often connected to a mainframe computer via telephone lines or radio connections, SCADA systems were not typically connected to central IT networks. These systems were also not designed with digital security features, so as SCADA systems were modified to connect to digital networks, potential access points for cybercriminals were created.

---

[1] Steve Reilly and Ryan Sabalow, "Power Grid Security Solutions and Ideas Arose After 2003 Blackout," USA Today, March 24, 2015, available at: http://www.nbcnews.com/news/us-news/power-grid-security-fears-surge-2003-blackout-n329381
[2] Ibid.
[3] Fahey, Johnathan, "Hurricane Power Outages After Sandy Not Extraordinary According To Report Analyzing Katrina, Past Storms," AP, available at: http://www.huffingtonpost.com/2012/11/16/hurricane-power-outages-after-sandy_n_2146393.html
[4] Reilly, Steve, "Bracing for a big power grid attack: 'One is too many,'" USA Today, March 24, 2015, available at: http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/
[5] Ibid.
[6] Campbell, Richard J., "Cybersecurity Issues for the Bulk Power System," Congressional Research Service, June 10, 2015, available at: http://www.crs.gov/pdfloader/R43989

Electromagnetic Pulse

An electromagnetic pulse (EMP) is a burst of high power electromagnetic radiation that results from the detonation of nuclear weapons, or from non-nuclear devices that are designed to disrupt or destroy electronic equipment.[7]

In 2000, the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 established a Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (EMP Commission).[8] The EMP Commission was tasked with assessing the nature and magnitude of potential high-altitude EMP threats from hostile state or non-state actors that acquired a nuclear weapon; the vulnerability of the U.S. military and civilian infrastructure to EMP attacks; U.S. capability to repair and recover from damage inflicted by a domestic EMP attack; and the feasibility and cost of hardening select military and civilian systems against EMP attacks.

After the EMP Commission was reestablished in the National Defense Authorization Act for Fiscal Year 2006[9], it released a 2008 report that included recommendations on the preparation, protection and recovery of U.S. critical infrastructure against a possible EMP attack.[10] According to recent testimony from the Government Accountability Office, however, while the Department of Homeland Security has worked to address some of the vulnerability issues addressed in the 2008 report, it "has not fully coordinated with stakeholders in certain areas such as identifying critical assets or collecting information necessary to assess electromagnetic risks."[11]

Space Weather

In addition to manmade EMPs, a geomagnetic disturbance (GMD) brought on by naturally occurring solar weather events can cause an electromagnetic impact that can adversely impact the electric grid. In 1989, a GMD caused millions of Canadians to lose their power for approximately nine hours. During that incident, the electric grid collapsed within 92 seconds of the GMD event.[12]

Specifically, space weather is the term used to describe severe disturbances of the upper atmosphere and of the near-Earth space environment that can be caused by the magnetic activity of the sun.[13] Major occurrences that lead to space weather include solar wind; solar flares and

[7] GAO-15-692T, United States Government Accountability Office, Testimony Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, July 22, 2015, available at: http://www.gao.gov/assets/680/671554.pdf
[8] PL 106-398, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001. October 30, 2000. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-106publ398/content-detail.html
[9] PL 109-163, National Defense Authorization Act for Fiscal Year 2006. January 6, 2006. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-109publ163/content-detail.html
[10] GAO-15-692T, United States Government Accountability Office, Testimony Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, July 22, 2015, available at: http://www.gao.gov/assets/680/671554.pdf
[11] Ibid.
[12] Ibid.
[13] National Research Council, Severe Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report (2008), 2008, available at: http://www.nap.edu/openbook.php?record_id=12507

coronal mass ejections; eruptive prominences; corotating interacting regions; and solar energetic particle events.[14]

Space weather can have an effect on everyday life, including: high-frequency radio communications, astronaut health, satellite function, and aircraft electronic systems. When a coronal mass ejection (a large explosion of "magnetic field and plasma from the Sun's corona"[15]) interacts with the Earth's magnetic fields it "creates colorful aurorae at high latitudes. More ominously, it can drive disturbances in the Earth's upper ionized atmosphere (ionosphere) that interfere with global navigation and communication systems, and can endanger electrical power grids through geomagnetically-induced currents (GICs)."[16]

There is also the potential of extreme space weather events, like the Carrington event of 1859, which resulted in failure of telegraph communications around the world and bright, colorful auroras in the sky.[17] A geomagnetic storm also occurred in May 1921, which suggests that while these extreme space weather events are rare, they could happen again in the future, with significant impact for modern, electricity-based technology.[18]

The "Smart Grid"

The nation's electric infrastructure is aging, and the electric power industry is in the process of modernizing it with its transformation to the "smart grid," or technology that provides an increased use of digital information and control technology to improve reliability, security, and efficiency of the electric grid. Research and development and private sector coordination towards incorporating smart grid technology was authorized in the Energy Independence and Security Act of 2007 (EISA) in order "to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth."[19]

In practice, the "smart grid" generally refers to a technology used to modernize utility electricity delivery systems using computer-based remote control and automation. These systems consist of two-way communication technology and modify computer processing that has been used for decades in other industries to functions on the electric grid.[20] In contrast, that vast majority of today's electric grid primarily delivers electricity in a one-way flow from generator to outlet, without automatic two-way communication between distribution and consumption sites.[21]

---

[14] McMorrow, Dan, "Impacts of Severe Space Weather on the Electric Grid," The MITRE Corporation, November 2011, available at: https://fas.org/irp/agency/dod/jason/spaceweather.pdf

[15] Space Weather Prediction Center, Coronal Mass Ejections, National Oceanic and Atmospheric Administration, available at: http://www.swpc.noaa.gov/phenomena/coronal-mass-ejections

[16] Gibson, Sarah, "Living with Space Weather (Baby, It's Charged Outside), The Blog, The Huffington Post, April 1, 2015, available at: http://www.huffingtonpost.com/sarah-gibson/living-with-space-weather_b_6981168.html

[17] Klein, Christopher, "A Perfect Solar Superstorm: The 1859 Carrington Event," History, March 14. 2012, available at: http://www.history.com/news/a-perfect-solar-superstorm-the-1859-carrington-event

[18] National Academy of Sciences, "Severe Space Weather Events – Understanding Societal and Economic Impacts Workshop Report (2008)," 2008, available at: https://www.nap.edu/download.php?record_id=12507#

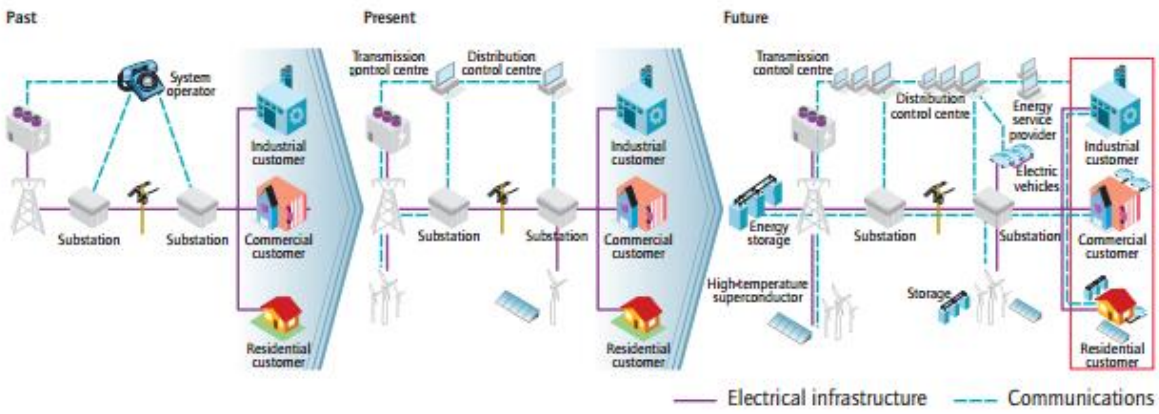
[19] PL 110-140, Energy Independence and Security Act of 2007. December 19, 2007. Available at: http://www.gpo.gov/fdsys/pkg/PLAW-110publ140/content-detail.html

[20] Department of Energy, Office of Electricity Delivery & Energy Reliability, "Smart Grid," available at: http://energy.gov/oe/services/technology-development/smart-grid

[21] National Institute of Standards and Technology, "Smart Grid: A Beginner's Guide," available at: http://www.nist.gov/smartgrid/beginnersguide.cfm

The concern with the two-way communication aspect of the "smart grid" is that it opens up potential points of unauthorized system access and can present potential cybersecurity vulnerabilities. In addition, there are concerns with the security and privacy of smart electricity meters, which send data about energy use wirelessly to electric distribution companies and control the flow of power to customers.[22]

Figure 1. Smarter electricity systems



Source: International Energy Agency[23]

Complicating matters, components of the smart grid are controlled by software programming, which may make these devices and functions subject to manipulation over a network. Recent reports of cyber intrusions and malware found on industrial control systems are known to control energy flows on the electric grid, and include: BlackEnergy, HAVEX, and Sandworm.[24]

[22] Campbell, Richard J., "The Smart Grid and Cybersecurity – Regulatory Policy and Issues," Congressional Research Service, June 15, 2011, available at: http://www.crs.gov/pdfloader/R41886
[23] International Energy Agency, "Technology Roadmap: Smart Grids," 2011, available at: https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf
[24] Ibid.