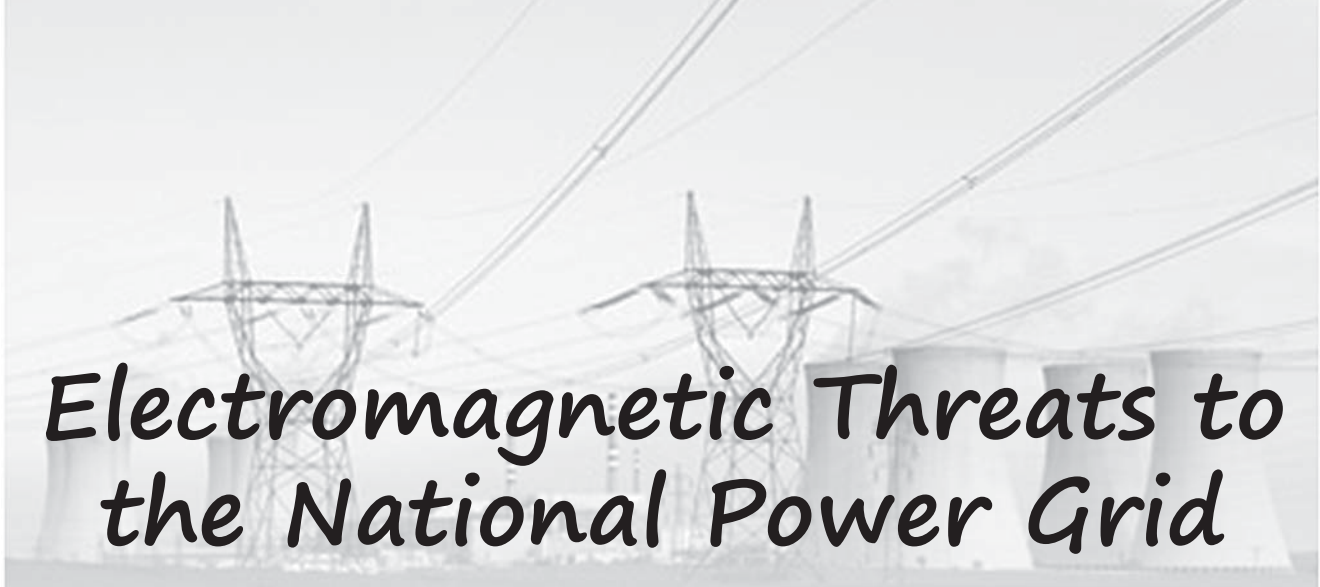

# Electromagnetic Threats to the National Power Grid

*By Mr. Robert Pfeffer*

**Editor's Note:** *This article reflects the findings and opinions of the author and is not meant to identify the position of the Department of Defense (DOD), Federal Energy Regulatory Commission (FERC), or electric power industry. First, the article describes a typical power grid. Next, it identifies the basic elements of the national power grid (NPG). Then, it identifies potential NPG vulnerabilities and discusses the importance of protection options for specific types of electromagnetic (EM) threats. The vulnerability of the NPG is also discussed from a political standpoint.*

The NPG is now so fundamental to U.S. infrastructure that, without it, the national economy would collapse and the health of the civilian population would be at risk. This scenario is possible, given that the NPG is vulnerable to several natural threats and an ever-growing number of man-made ones. Damage to key nodes in just a single region could take months—even years—to resolve. During that time, the damaged grid would be unable to provide the power necessary to process and refrigerate food and medicine; pump water, fuel, and sewage; assure the availability of public transportation and communication; maintain bank and stock market records and other critical databases; and provide light, heat, and air conditioning. In other words, society within the region would rapidly disintegrate. If the threat were multiregional, as it clearly could be, a national disaster could result.

But is the NPG too big to fail? This simple question does not have a simple answer. The Nation has been at war with unconventional enemies who have already attacked military and civilian personnel, businesses, and religious structures worldwide. They generally do not fight in uniform—preferring, instead, to blend in with the civilian population and operate as terrorists. Their first major attack against civilian property and people on U.S. soil occurred more than 15 years ago, with the bombing of the World Trade Center in New York on 26 February 1993. This attack was followed by others against U.S. targets worldwide—

- **4 October 1993:** U.S. troops gunned down in Somalia.
- **26 June 1996:** U.S. Airmen bombed in Saudi Arabia.
- **7 August 1998:** U.S. Embassies bombed in Africa.
- **12 October 2000:** U.S. Ship Cole bombed in a Yemeni harbor.
- **11 September 2001:** World Trade Center brought down by two hijacked U.S. aircraft in New York; Pentagon damaged by a hijacked U.S. aircraft in Washington, D.C.; and the deliberate crash of a hijacked U.S. aircraft in Pennsylvania.

Since 11 September 2001, terrorist leaders have continued to wage war against military and civilian targets. Therefore, it is reasonable to assume that fundamental elements of our infrastructure, such as the NPG, will remain high-priority targets.

Because the NPG is so massive and potentially vulnerable, it would not be practical to protect the entire NPG against every possible threat. A risk assessment identifying the most serious natural and man-made threats and the most vulnerable NPG elements represents a more reasonable alternative. Based on the risk assessment, protection options and their costs can be developed to protect only those portions of the NPG that support the minimum-essential services to military and civilian personnel until the damaged portion of the grid can be repaired and brought back on line.

## Power Grids

A power grid is an enormous power generation, transmission, and distribution system. It could consist of coal, hydroelectric, natural gas, and nuclear power plants that generate medium-voltage (1–100 kilovolts [kVs]) electric power and send it to nearby step-up transformer substations. High-voltage transmission lines then take the stepped-up, now high-voltage (greater than 230 kV) electric power and pass it long distances to step-down transmission substations or distribution centers with collocated substations. These substations reduce (or step down) the voltage and redistribute the electric power via aboveground or belowground, medium-voltage or low-voltage (less than 1 kV) lines to end users such as military facilities, homes, and businesses. A typical grid is illustrated in Figure 1, page 6.

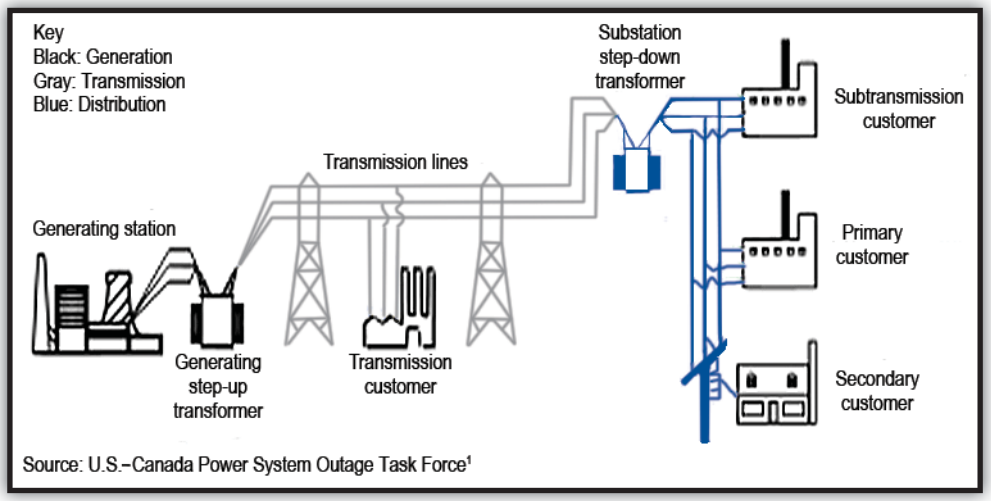


**Figure 1. Typical Power Grid**

In its simplest form, a power grid does not store the power it generates; rather, all generated power is immediately distributed throughout the system. For example, electricity obtained from a wall socket is generated less than a millisecond before it is actually used. This means that power plants must constantly generate an enormous amount of power to accommodate grid losses and power usage spikes. These grid conversion and transmission losses could be substantial; for power generation plants that have high combustion and heat losses due to the use of older boilers and turbines, as little as one-third of the total power produced might eventually be delivered to the user.

## The NPG

The term "NPG" is commonly used to refer to the U.S. power grid—probably the world's largest network. The NPG consists of about 10,000 independently owned and operated power generation plants, about 157,000 miles of high-voltage transmission lines, and hundreds of thousands of miles of lower-voltage lines running from distribution substations to individual users' meters. Although this network is not owned by the U.S. government, it is a national monopoly that is regulated by the government. This means that the government has the authority to regulate electric power as a commodity and to ensure network reliability.

The NPG has expanded through the years to accommodate an increasing population with a growing appetite for electrical energy. Today, 40 percent of the energy consumed in the United States is used by the NPG to produce electricity. (In 1940, it was 10 percent; in 1970, it was 25 percent.)[2] The NPG now consists of a patchwork of old and new power plants, transmission lines, and distribution centers tied together to form the following separate, but interdependent, networks—Eastern Interconnection, Western Interconnection, and Electric Reliability Council of Texas Interconnection (see Figure 2).

In addition to their internal connections, these three networks are also connected to the Canadian and Mexican grids, forming the North American Power Grid. The continued expansion of the grid to meet increasing power needs has resulted in the unintended consequence of slowly increasing grid vulnerability.

## NPG Vulnerability

NPG vulnerability has been studied and documented by numerous DOD and private sector organizations. The Armed Services Committee, U.S. House of Representatives, began studying NPG vulnerability to a specific type of nuclear-generated electromagnetic pulse (EMP) in 2001. Other studies focused on actual regional shutdowns due to several

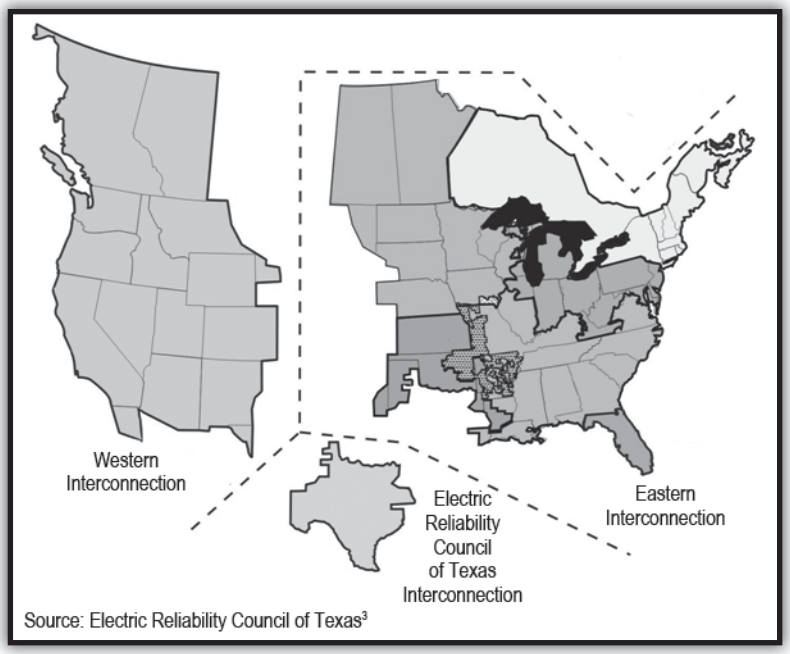


**Figure 2. NPG Networks**

types of threats, including naturally occurring EMPs and personnel error. The conclusions are all the same: Upgrade the existing NPG, or start over.

Each of the three most recent regional NPG shutdowns was the result of a different threat—a naturally occurring EMP created by multiple lightning strikes on transformers (New York, 1977), a localized solar storm (Quebec, 1989), and an operational control problem (the "Lake Erie Loop," Midwestern United States, Northeastern United States, and Southern Canada, 2003).

The first two shutdowns were of modest severity, and the loss of power was somewhat controlled. Nevertheless, portions of the grid were down for weeks and the financial cost reached hundreds of millions of dollars. A congressional study indicated that, during the 1-day, 1977 New York City blackout, the damage from looting and vandalism alone was more than $300 million. The 1989 Quebec solar storm directly cost two large utility companies (Hydro-Quebec in Canada and Public Service Electric and Gas [PSE&G] in New Jersey) an estimated $30 million. In addition, Hydro-Quebec also spent $1.2 billion on the installation of protection devices to block future storm-induced currents. In one recent assessment, the Quebec solar energy field strength (about 5 volts/kilometer [V/km]) and duration (several minutes) compared favorably to the late-time field strength and duration characteristics of a nuclear-generated, high-altitude electromagnetic pulse (HEMP).[4] This means that HEMPs are also capable of knocking out portions of the NPG. If natural or nuclear-induced EMPs were to damage some of the key, custom-ordered, 500-kV, 1,200-megavolt-ampere transformers, it would likely take more than a year to replace them, since most of these hand-wound, extra-high-voltage transformers are currently made in China, India, Japan, and Europe.

During the 2003 Lake Erie Loop incident, blackouts occurred in many large cities, including New York City, just a little more than two hours after the first Ohio generating plant shut down and just one hour after controllers noticed a voltage dip and did nothing. "The . . . blackout, although set off by specific chance events, became the logical outcome of these trends. Controllers in Ohio, where the blackout started, were overextended, lacked vital data, and failed to act appropriately on outages that occurred more than an hour before the blackout. When energy shifted from one transmission line to another, overheating caused lines to sag into a tree. The snowballing cascade of shunted power that rippled across the Northeast in seconds would not have happened had the grid not been operating so near to its transmission capacity."[5] This 2-day blackout left 50 million people without power, contributed to 11 deaths, and cost an estimated $6 billion.

Some of the more obvious NPG sensitivities that could have widespread social and economic impacts are summarized in Table 1. Those recently receiving the most publicity are EM in nature. Collectively, EM threats have the largest impact on the grid. Most of the five EM sensitivities listed in the table can be resolved through hardware protection, but some (including various forms of cyber attack) are best addressed through software protection.

Consider the specific case of a severe solar storm. Unlike nuclear-generated, HEMP events, which are unpredictable, solar storms are cyclical. Solar activity occurs on an 11-year cycle. Many times during each cycle, the sun ejects a stream of charged particles known as a "coronal mass ejection." Some coronal mass ejections are recaptured by the sun, while others stream into space. Those that travel toward the Earth in the enhanced solar wind are eventually captured by Earth's magnetic field and are bent, resulting in the flow of

| Threats | Generation Node Sensitivities | Transmission Node Sensitivities | Distribution Node Sensitivities | Local/Regional NPG Threat Impact |
|---|---|---|---|---|
| **EM Threats** | | | | |
| Lightning | Transformers | Lines | Transformers | Local+ |
| Solar flares | Transformers | Low sensitivity | Transformers | Regional+ |
| HEMP | Transformers, C4 | Low sensitivity | Transformers, C4 | Regional+ |
| IEMI | C4 | No known sensitivity | N/A | Local+ |
| Cyber attack | C4 | None | C4 | Local+ |
| **Other Threats** | | | | |
| Operator error | C4 | None | C4 | Local+ |
| Explosives | Substations | Towers, lines | Power poles, civilians | Local+ |
| CBRN* | Facilities, substations | Towers, lines | Facilities, substations, civilians | Local+ |

Legend:
C4: command, control, communications, and computers
* In this table, CBRN does not include HEMP.

**Table 1. Potential NPG Sensitivities to Various Threats**

charged particles downward toward the lower ionosphere, where they eventually produce a horizontal current flow. As these particles travel downward, they undergo various ionization processes that result in a visible glow. This aura, known as the Northern Lights, can be seen in the northern hemisphere. The phenomenon is similar to the glow that is visible in the upper atmosphere due to the flow of charged particles from a high-altitude nuclear detonation.

The current solar cycle (Number 24, as designated by the sunspot number) is predicted to peak around 2013. While it is impossible to forecast how serious this solar cycle might become, it is reasonable to assume that it or a future solar cycle will produce a storm that could rival or exceed the 1–2 September 1859 storm, which is sometimes referred to as the "Solar Superstorm" or "Carrington Event." This killer storm was the strongest ever recorded; it has been estimated to be several times stronger than the 1989 Quebec solar storm. And although the 1859 storm caused less damage to the rugged, primitive electrical systems than the 1989 storm caused to electronics and electrical systems in Quebec, it resulted in fires and telegraph system failures throughout North America and Europe. In addition, auroras that were generated by the 1859 storm were visible around the world. The glow in the sky over the Rocky Mountains was so bright that it woke gold miners.

Another major threat to the existing NPG is a cyber attack or other form of information attack. Unlike natural and nuclear-generated EMPs—which cause detectable, catastrophic damage or unacceptable upset to the NPG—an information attack can go undetected for some time. And the number of attacks continues to increase: The Department of Homeland Security documented that cyber attacks against the United States tripled between 2006 and 2008 (Figure 3). Furthermore, some national security officials believe that one or more nations deliberately infiltrated the NPG on 8 April 2009, leaving behind software programs that could be used to disrupt the system.

In the interest of minimizing protection costs, cyber attacks should be treated as other EM threats. To do this, the EM environmental effects and electronic warfare protection communities must work together to develop a unified protection scheme for each new system design. This protection must then be maintained throughout the lifetime of the NPG.

### Political Assessment of NPG Vulnerability

While the vulnerability of the NPG to various threats has long been the subject of technical assessments, it has only recently become a national political issue. EM threats are of particular concern to Congress.

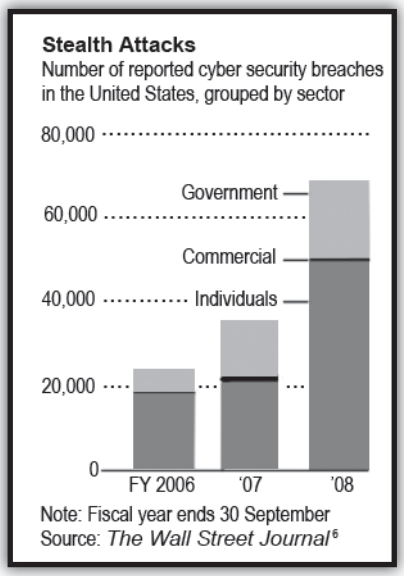


**Figure 3. A summary of documented cyber attacks on U.S. assets.**

Congress now has the political will to address the NPG vulnerability issue in separate House and Senate bills that explicitly identify the most serious EM threats as cyber attacks, naturally occurring EMPs caused by solar storms and lightning, nonnuclear EMPs (also known as intentional electromagnetic interference [IEMI]), and nuclear EMPs. Congressional members no longer believe that a major EM event *might* materialize; they now agree that it is only a matter of time until such an event brings down the grid. And political support for NPG protection is growing. Bills were pushed forward in the Senate and the House in late 2009. Representative Yvette D. Clarke (Democrat–New York), Chairwoman, Subcommittee on Emerging Threats, Cyber Security, Science and Technology, and Representative Roscoe G. Bartlett (Republican–Maryland), member of the Armed Services Committee, supported House Resolution (H.R.) 2195. Senator Joseph Lieberman (Independent–Connecticut) supported Senate (S.) 946. Both bills propose "To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack and for other purposes."[7] Other EM threats emphasized in the bills include EMP caused by solar storms and nuclear detonations.

The House Energy and Commerce Committee's Subcommittee on Energy and Environment held a legislative hearing on H.R. 2195 and another bill (H.R. 2165), which were intended to protect the NPG from cyber security threats. This hearing was followed by a classified briefing to members of the Energy and Commerce Committee. Since then, Energy and Commerce Committee staff members have developed a bipartisan discussion draft to amend the Federal Power Act to ". . . give the FERC new authorities to protect the electric grid against cyber security and other threats, as well as from geomagnetic storms created by solar flares."[8] This bill (H.R. 5026, which passed the Energy and Commerce Committee by a vote of 47–0 on 9 March 2010) is sometimes referred to as the "Grid Reliability and Infrastructure Defense Act" or the "GRID Act."

Should Congress approve a single bill, the question of how robust the entire NPG—or at least the most critical parts of it—should be will need to be addressed. Several ideas have been proposed, including the redesign of the NPG as a commercial, digital smart grid that is capable of energy storage and regulated by the FERC; however, the cost would be significant. Until a permanent solution is funded, DOD must consider different options to ensure the continued ability to complete critical missions. One of these options involves the isolation of military posts, bases, and facilities from the civilian NPG. This isolation could be achieved with the development and deployment of

small (10–25 megawatt [MW] electric), modular nuclear power reactors (NPRs) at each site. This is not a new idea; at one time (about 50 years ago), the U.S. Army installed fixed NPRs to provide electrical power to Fort Belvoir, Virginia, and Fort Greely, Alaska. In addition, mobile NPRs were temporarily used at Sundance, Wyoming; Camp Century in Greenland; and McMurdo Sound in Antarctica. A 10-MW (electric) NPR mounted on a floating barge also provided electricity to the Panama Canal Zone for 8 years (1968–1976).[9] The proper integration of small, secure NPRs into a comprehensive military and civilian EM hardware and software threat protection scheme could protect Army sites from cyber attack and other forms of EM threats.

## Conclusion

The technical community and congressional policy makers recognize the vulnerability of the NPG to various threats. Potential weak points have been identified through technical assessments, and protection options have been developed for some of the more serious EM threats. Congressional bills identify cyber attack, severe solar storms, IEMI, and nuclear EMPs as significant EM threats. These threats can only be addressed by integrating hardware and software protection into an overall, end-to-end system design. The integrated protection must then be maintained throughout the lifetime of the NPG. Although the least expensive approach to hardware and software protection involves its inclusion in the original system design, the existing NPG requires a retrofit, which involves the support and participation of many private businesses. Consequently, there must be one civilian organization—possibly the Office of Electric Reliability, FERC—that is responsible for overseeing such a massive protection scheme.

**Endnotes:**

[1]"Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," U.S.-Canada Power System Outage Task Force, April 2004.

[2]*GridWorks*, "Overview of the Electric Grid," U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, undated.

[3]*NERC Interconnections,* Electric Reliability Council of Texas, *<http://www.ercot.com/content/news/mediakit/maps/NERC_Interconnections_color.jpg.html>*, accessed on 24 August 2010.

[4]William Radasky, John Kappenman, and Robert Pfeffer, "Nuclear and Space Weather Effects on the Electric Power Infrastructure," *NBC Report*, Fall/Winter 2001, pp. 37–42.

[5]Eric J.Lerner, "What's Wrong With the Electric Grid?" *The Industrial Physicist, <http://www.aip.org/tip/INPHFA/vol-9/iss-5/p8.html>*, accessed on 24 August 2010.

[6]Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *The Wall Street Journal*, 8 April 2009, *<http://online.wsj.com/article/SB123914805204099085.html>*, accessed on 24 August 2010.

[7]H.R. 2195: *To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes*, introduced 30 April 2009, and S. 946: *Critical Electric Infrastructure Protection Act of 2009*, introduced 30 April 2009.

[8]"Grid Security Legislation: March 9, 2010 Bipartisan Discussion Draft Summary," *<http://empcouncil.org/images/upload/media/Grid%20Security%20Discussion%20Draft%20Summary%20(3-9-10)_1.pdf>*, accessed on 24 August 2010.

[9]Robert A. Pfeffer and William A. Macon Jr., "Nuclear Power: An Option for the Army's Future," *Army Logistician*, September–October 2001, pp. 4–8.

**References:**


Jeff Brady, "An Aged Electric Grid Looks to a Brighter Future," *National Public Radio*, 27 April 2009, *<http://www.npr.org/templates/story/story.php?storyId=103327321>*, accessed on 24 August 2010.

Marshall Brain, "How Power Grids Work," *How Stuff Works*, *<http://www.howstuffworks.com/power.html>*, accessed on 24 August 2010.

"Electromagnetic Pulse & Geomagnetic Storm Events," Executive Brief, North American Electric Reliability Corporation, 24 August 2009, *<http://www.nerc.com/fileUploads/File/CIP/EMP-Geomagnetic-Exec-Brief(1).pdf>*, accessed on 24 August 2010.

William R. Forstchen, *One Second After*, Forge Books, 2009.

*High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*, North American Electric Reliability Corporation, June 2010.

H.R. 2165, *Bulk Power System Protection Act of 2009*: *To amend Part II of the Federal Power Act to address known cyber security threats to the reliability of the bulk power system and to provide emergency authority to address future cyber security threats to the reliability of the bulk power system, and for other purposes*, introduced 29 April 2009.

H.R. 5026, *Grid Reliability and Infrastructure Defense Act*, 9 June 2010.

David Lindley, "Smart Grids: The Energy Storage Problem," *Nature News*, 6 January 2010, *<http://www.nature.com/news/2010/100106/full/463018a.html>*, accessed on 24 August 2010.

"North American Electric Reliability Corporation (NERC) Regions," *U.S. Energy Information Administration: Independent Statistics and Analysis*, U.S. Energy Information Administration, *<http://www.eia.doe.gov/cneaf/electricity/chg_str_fuel/html/fig02.html>*, accessed on 24 August 2010.

Personal conversations with Dr. William Radasky, Metatech Corporation, April 2010.

Robert Pfeffer, "The Need to Redefine Electromagnetic (EM) Protection: A Think Piece," *Combating WMD Journal*, Issue 5, Spring/Summer 2010.

"Solar Storms Cause Significant Economic and Other Impacts on Earth," *NOAA Magazine*, 5 April 2004, *<http://www.magazine.noaa.gov/stories/mag131.htm>*, accessed on 24 August 2010.

"Solar Superstorm," *NASA Science: Science News*, National Aeronautics and Space Administration, 23 October 2003, *<http://science.nasa.gov/science-news/science-at-nasa/2003/23oct_superstorm/>*, accessed on 24 August 2010.

"Update 2—U.S. Concerned Power Grid Vulnerable to Cyber-Attack," *Reuters*, 8 April 2009, *<http://www.reuters.com/article/idAFN0853911920090408>*, accessed on 24 August 2010.

U.S. Code, Title 16, Chapter 12, *Federal Power Act*.


---


*Mr. Pfeffer is a physical scientist with the U.S. Army Nuclear and Combating Weapons of Mass Destruction Agency, Fort Belvoir, Virginia. He holds a bachelor's degree in physics from Trinity University, San Antonio, Texas, and a master's degree in physics from The Johns Hopkins University, Baltimore, Maryland.*