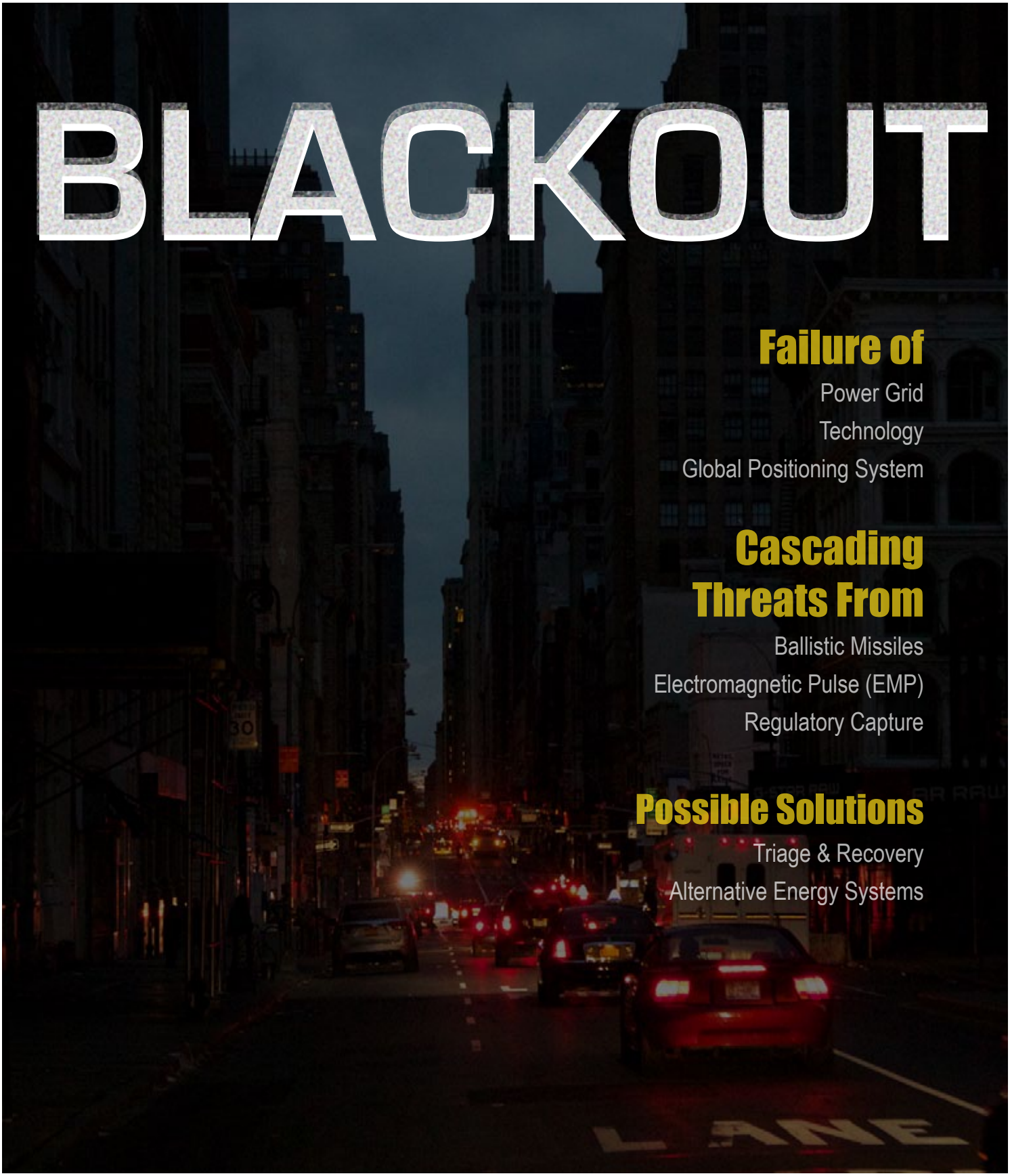
domestic preparedness .com

DomPrep Journal

Subscribe Volume 10 Issue 11, November 2014



Not If, But When?

Prepare Now

For Chemical & Biohazard Emergencies

AP4C

Handheld Chemical Detector

- Unlimited, Simultaneous Detection
- Continuous Detection for Fix Locations
- Low Maintenance and Operation Cost
- Compact Design for Tight Locations

PROENGIN

Chemical and Biological Detection System

PROENGIN, inc.
140 S. University Dr, Suite F
Plantation, FL 33324 USA
Ph: 954.760.9990
contactusa@proengin.com
www.proenginusa.com

Business Office
517 Benfield Road, Suite 303
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Advertisers in This Issue:

American Military University (AMU)

BioFire Defense Inc.

FLIR Systems

International Disaster Conference & Expo 2015

PROENGIN Inc.

DomPrep Journal is electronically delivered by the IMR Group Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

Articles are written by professional practitioners in homeland security, domestic preparedness, and related fields. Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher. Text is the opinion of the author; publisher holds no liability for their use or interpretation.

IMR GROUP

Featured in This Issue

About the Cover: An uncommon blackout in lower Manhattan, New York City, on 31 October 2012. Hurricane Sandy and subsequent Nor'easter left 8.6 million customers without power across 21 states. (iStockPhoto)

RADIATION DETECTION & IDENTIFICATION

SMALL. SIMPLE. SPECIFIC.

Confident decision-making is critical when lives are at stake. Emergency responders must have fast and accurate threat information where they need it the most - in the field.

FLIR is focused on delivering advanced threat detection and identification tools that are more affordable and easier to use than ever before.

For example, the identiFINDER® R300 is the world's first pager-size radiation instrument that can detect, locate and identify radioactive isotopes.

Worn on a belt similar to a personal radiation detector (PRD), the identiFINDER® R300 provides the operator with all the information necessary to respond with confidence in the most hazardous and stressful environments.

To learn more about the identiFINDER® R300 and our other laboratory-caliber products visit www.flir.com/r300

FLIR®

THE WORLD'S SIXTH SENSE™

/flirhq @FLIRdetection

Editorial Remarks

By Catherine Feinman

"We are like Ireland the month before discovering there was a potato blight in August 1845. We have giant technology monocultures with all our technology eggs in one basket or another. We need to diversify and create more local resilient communities," says this month's guest editor, Charles Manto, founder and lead of the InfraGard National's Electromagnetic Pulse Special Interest Group (EMP SIG). Despite warnings by groups such as the EMP SIG, many policymakers and emergency planners do not fully grasp the magnitude of threats to the electric power grid.

Leading this month's issue is George H. Baker, who addresses common misconceptions about electromagnetic pulses, which can be generated by manmade or natural events. If the electric grid were to be significantly damaged or destroyed, electronic components across the grid that provide life-supporting services may cease to function. It is critical to understand the realistic effects of a "blackout" and remove any misconceptions. Results of a related flash poll of DomPrep readers are conveyed in "Em-Powering Communities to Prepare."

In another article, Ambassador Henry F. Cooper warns the nation about the potential for ballistic missile attacks against the homeland. "If we fail to take advantage of straightforward remedies, we dramatically increase the likelihood that our adversaries will take advantage of our vulnerabilities," says Manto. Dana A. Goward discusses the nation's interdependencies with satellite navigation and timing, both good and the bad news.

Mary D. Lasky describes potential cascading effects following the loss of the electric power grid. To avoid such effects, Charles Manto presents immediate and long-term steps to plan for, triage, and shield against electromagnetic pulse before an incident occurs. In addition, William Kaewert shares alternative energy resources that work despite long-term power outage threats. As communities plan for major disasters, they also will be better prepared for not-so-major incidents. If all else fails, Joseph Cahill reminds responders to be ready to perform their tasks "old school."

State representative Andrea Boland and Rodrigo Moscoso round out this issue by describing efforts in their respective states. Boland shares a journey through Maine's grid-protective legislation and the threat of regulatory capture, while Moscoso describes how Washington, D.C., is prepared to fail gracefully, but recover quickly from a major power outage.

All-hazards planning necessarily includes protection of the electric power grid and communications networks from electromagnetic pulse, geomagnetic storms, ballistic missile attacks, and other threats that could damage or destroy power-generation sources. A special thanks goes to Charles Manto for soliciting much of the content in this month's issue.

Electromagnetic Pulses – Six Common Misconceptions

By George H. Baker

Many misconceptions about electromagnetic pulse (EMP) effects have circulated for years among technical and policy experts, in press reports, on preparedness websites, and even in technical journals. Because many aspects of EMP-generation physics and its effects are obscure, misconceptions from those who do not perceive the seriousness of the effects to those who predict a doomsday chain of events are inevitable. However, not all EMPs are the same, with the most significant effects being caused by E1 and E3 fields.

Nuclear bursts detonated at altitudes above 40 km generate two principal types of EMPs that can debilitate critical infrastructure systems over large regions:

- The first, a "fast-pulse" EMP field, also referred to as E1, is created by gamma ray interaction with stratospheric air molecules. The resulting electric field peaks at tens of kilovolts per meter in a few nanoseconds, and lasts a few hundred nanoseconds. E1's broadband power spectrum (frequency content from DC to 1 GHz) enables it to couple to electrical and electronic systems in general, regardless of the length of their cables and antenna lines. Induced currents range into the thousands of amperes and exposed systems may be upset or permanently damaged.
- The second "slow-pulse" phenomenon, is referred to as magnetohydrodynamic (MHD) EMP, or E3, and is caused by the distortion of Earth's magnetic field lines due to the expanding nuclear fireball and the rising of heated, ionized layers of the ionosphere. The change of the magnetic field at the Earth's surface induces a field in the tens of volts per kilometer, which, in turn, induces low-frequency currents of hundreds to thousands of amperes in long conducting lines only (a few kilometers or longer) that damage components of long-line systems, including the electric power grid and long-haul communication and data networks.

By over- and under-emphasizing realistic consequences of EMPs, policymakers may delay actions or dismiss arguments altogether. The six misconceptions about EMPs that are perhaps the most harmful involve: (a) exposed electronic systems; (b) critical infrastructure systems; (c) nuclear weapons; (d) cost of protection; (e) type of EMPs; and (f) fiber-optic networks.

Misconception 1:
EMP Will Cause Every Exposed Electronic System to Cease Functioning.

Based on the U.S. Department of Defense (DOD) and Congressional EMP Commission's EMP test databases, small, self-contained systems, such as motor vehicles, hand-held radios, and unconnected portable generators, tend not to be affected by EMPs. If there is an effect on these systems, it is often temporary upset rather than component burnout.

On the other hand, threat-level EMP testing also reveals that systems connected to power lines are highly vulnerable to component damage requiring repair or replacement.

Because the strength of EMP fields is measured in volts per meter, the longer the conducting line, the more EMP energy will be coupled into the system, and the higher the probability of damage. As such, the electric power-grid network and landline communication systems are almost certain to experience component damage when exposed to an EMP with cascading effects to most other (dependent) infrastructure systems.

Misconception 2:
EMP Effects Will Have Limited, Easily Recoverable, "Nuisance" Effects on Critical Infrastructure Systems.

Although an EMP would not affect every system, widespread failure of a significant fraction of electrical and electronic systems will cause large-scale cascading failures of critical infrastructure networks because interdependencies among affected and unaffected systems. Mathematician Paul Erdos's "small-world" network theory applies, which refers to most nodes – equipment attached to a network – being accessible to all others through just a few connections. The fraction of all nodes changes suddenly when the average number of links per single network connection exceeds one. For example, a single component failure, where the average links per node is two, can affect approximately half of the remaining "untouched" network nodes.

For many systems, especially unmanned systems, loss of control is tantamount to permanent damage, in some cases causing machinery to self-destruct. Examples include:

- Lockup, or not being able to change the "on" or "off" state, of long-haul communication repeaters;
- Loss of remote pipeline pressure control in supervisory control and data acquisition (SCADA) systems, which communicate with remote equipment;
- Loss of generator controls in electric power plants; and
- Loss of machine process controllers in manufacturing plants.

Misconception 3:
Megaton-Class Nuclear Weapons Are Required to Cause Serious EMP Effects.

Due to a limiting atmospheric saturation effect in the EMP-generation process, low-yield weapons produce a peak E1 field similar in magnitude to high-yield weapons if they are detonated at altitudes of 50-80 km. The advantage of high-yield weapons is that their range on the ground is affected less significantly when detonated at higher altitudes.

Nuclear weapons with yields ranging from 3 kilotons to 3 megatons (a 3 order of magnitude difference in yield), when detonated at their optimum burst altitudes, exhibit a range of peak E1 fields on the ground differing by only a factor of ~3, viz. 15-50 KV/meter. With respect to the late-time (E3, or low-amplitude, low-frequency components) EMP field, a 30-KT nuclear weapon above 100 km would cause geomagnetic disturbances as large as solar superstorms, although over smaller regions. It also is worth noting that peak currents on long overhead lines induced by E1 from 10 kiloton-class weapons can range in the kiloamperes with voltages reaching into the hundreds of kilovolts.

The six electromagnetic pulse "knots" addressed here are common misconceptions and perhaps the most important to "untie."

Misconception 4:
Protecting the Critical National Infrastructure Would Be Cost Prohibitive.

Of the 14 critical infrastructure sectors, EMP risk is highest for electric power grids and telecommunication grids because of their network connections and criticality to the operation and recovery of other critical infrastructure sectors. Attention to hardening these infrastructure grids alone would provide significant benefits to national resilience.

The electric power grid is essential for sustaining population "life-support" services. However, some major grid components could take months, or years, to replace if many components are damaged. The primary example is high-voltage transformers, which can irreparably fail during major solar storms and are thus likely to fail during an EMP event. Protection of these large transformers would reduce the time required to restore the grid and restore the necessary services it enables.

According to Emprimus, a manufacturer of transformer protection devices, the unit cost for high-voltage transformer protection is estimated to be $250,000, with the total number of susceptible large, high-voltage units ranging from 300 to 3,000, according to Oak Ridge National Laboratory. The requirement and cost for generator facility protection are still undetermined but are likely to be similar to transformer protection costs. To protect SCADA systems, replacement parts are readily available and repairs are relatively uncomplicated. Protection costs for heavy-duty grid

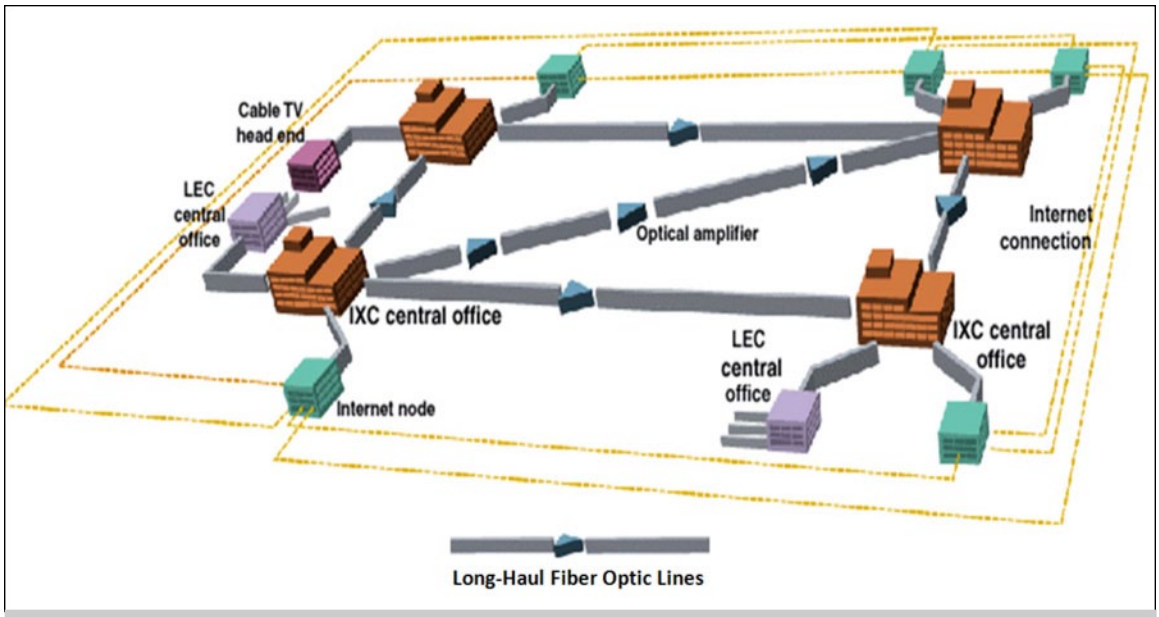


Figure 1: Regional Fiber-Optic Network Components

components are in the $10 billion range, which is a small fraction of the value of losses should they fail. When amortized, protection costs to consumers amount to pennies per month.

Misconception 5:
Only Late-Time EMP (E3) Will Damage Electric Power-Grid Transformers.

Oak Ridge National Laboratory's January 2010 report on its E1 tests of 7.2-KV distribution transformers produced permanent damage to transformer windings in seven of the 20 units tested. The failures were due to transformer winding damage caused by electrical breakdown across internal wire insulation. As an important side note, transformers with direct-mounted lightning surge arrestors were not damaged during the tests. Similar tests of high-voltage transformers are needed.

Misconception 6:
Fiber-Optic Networks Are Not Susceptible to EMP Effects.

In general, fiber-optic networks are less susceptible than metallic line networks; however, fiber-optic multipoint line driver and receiver boxes, which are designed to protect against ground current, may fail in EMP environments. Long-haul telecommunication and regional Internet fiber-optic repeater amplifiers' power supplies are particularly vulnerable to EMP environments (Figure 1). Terrestrial fiber-optic cable repeater amplifier power is provided by the electric power grid and thus vulnerable to grid failure as well as to direct EMP/E1 effects.

Undersea cable repeater amplifiers also are vulnerable to EMP/E3 effects since they are connected to a coaxial metallic power conductor that runs the length of the line. Because of its low-frequency content, E3 penetrates to great ocean depths, which subjects undersea power amplifiers to high risk of burnout. On the positive side, line drivers/receivers and repeater amplifiers are relatively easy to protect using shielding, shield-penetration treatment, and power-line filters and/or breakers.

Standardized Solutions

From a risk-based priority standpoint, the electric power grid is a high priority for EMP protection. Hardening this infrastructure alone would have major benefits for national resilience – the ability to sustain, reconstitute, and restart critical services. EMP engineering solutions have been implemented and standardized by DOD since the 1960s and are well documented:

- MIL-STD-188-125-1 – "DOD Interface Standard – High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions – Part 1 – Fixed Facilities" (17 July 1998);
- MIL-STD-188-125-2 – "DOD Interface Standard – High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions – Part 1 – Transportable Systems" (3 March 1999); and
- MIL-HDBK-423 – "Military Handbook – High-Altitude Electromagnetic Pulse (HEMP) Protection for Fixed and Transportable Ground-Based C4I Facilities Vol. 1 – Fixed Facilities" (15 May 1993).

With respect to the power grid, the installation of blocking devices in the neutral-to-ground conductors of large electric distribution transformers will significantly reduce the probability of damage from slow EMP/E3. Transformer protection against E1 overvoltages is achievable by installing common metal-oxide varistors (control elements in electrical circuits) on transformers from each phase to ground. Costs for protecting the power grid are small compared to the value of the systems and services at risk.

George H. Baker is professor emeritus at James Madison University (JMU) and directed JMU's Institute for Infrastructure and Information Assurance. He consults on critical infrastructure assurance, specializing in EMP and other nuclear effects. He is the former director of the Defense Threat Reduction Agency's critical system assessment facility. He also led the EMP group at the Defense Nuclear Agency responsible for development the DoD EMP standards. He served as principal staff on the Congressional EMP Commission and now serves on the board of directors of the Foundation for Resilient Societies and the Congressional Task Force on National and Homeland Security advisory board. He holds a Ph.D. in engineering physics from the U.S. Air Force Institute of Technology.

Em-Powering Communities to Prepare

By Catherine Feinman

Modern society has become dependent on electrical resources that sustain communications, transportation, agriculture, finance, water, sanitation, and other aspects of daily life. As such, a catastrophic failure of the electric power grid likely would have devastating cascading effects. In this month's survey, 58 DomPrep readers replied to a flash poll that addressed the topic of electric power-grid resilience. This article is a compilation of these responses.

Most of the emergency preparedness professionals who responded agree that:

- The U.S. electric power grid is not secure (85 percent);
- The current policy, regulation, and/or oversight of utility companies are not effective in protecting the grid from long-term outages lasting one month or more (83 percent); and
- Corporate utility protocols are not sufficient to sustain this critical infrastructure in light of threats to the power grid (66 percent).

A community's tolerance level during a power outage before civil unrest ensues and possible solutions to close gaps in electric-grid protection vary. However, by examining past incidents and determining where gaps exist, communities can increase resilience for their critical infrastructures.

Power Disruptions & Civil Disobedience

Three examples described by the U.S. Department of Energy illustrate the far-reaching effects that power outages can have across jurisdictions:

- On 14 August 2003, the largest power blackout in North American history affected an area with an estimated 50 million people in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, and New Jersey, and the Canadian province of Ontario.
- In 2005, Hurricane Katrina contributed to 2.6 million reported outages in the states of Louisiana, Mississippi, Alabama, Florida, and Georgia.
- In 2012, Hurricane Sandy and subsequent Nor'easter affected 21 states – from North Carolina to Maine, and as far west as Illinois – and left 8.6 million customers without power for varying lengths of time.

One respondent recounted, "I have been through a power outage situation for many days, living in a totally electric home. It was not pretty. It was in North Carolina, during the winter of 1968. We had a snow/ice storm, which resulted in 3-4 inch radial ice

on the overhead power service lines…. Back then, people were not prepared for these types of situations. I was on an Air Force Base, and it too was not prepared, at the time."

Unfortunately, almost 50 years later, many communities remain unprepared for widespread power outages. Some may argue that the nation is even less prepared. One respondent noted that, although some members of the public trust that policymakers have "solved society-threatening issues like grid vulnerability," policymakers should "be honest and admit when there is no plan and people need to make their own." A lack of information sharing with the public could exacerbate the incident's impact on society.

In addition to the level of information sharing, many other factors also would affect the length of time between an incident's occurrence and civil disobedience within the affected communities. These include: time of year; weather conditions; homeowners' ability to self-sustain; extent of the outage; location; degree of urbanization; distance between the affected area and alternate power sources; and amount of social and economic capital. By providing adequate warning for a potential incident and demonstrating efforts to restore power following an incident, community leaders and emergency planners can help mitigate the threat of civil unrest.

"On 14 August 2003, the largest power blackout in North American history affected an area with an estimated 50 million people in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, and New Jersey, and the Canadian province of Ontario."

Greater planning, of course, often leads to longer periods of sustainability following a disaster. For example, small communities that are accustomed to losing power during thunderstorms are more likely to have contingency resources such as generators and water/food storage. Residents in large urban areas, though, may not have the same levels of resources, plans, and storage capabilities, which could lead to civil unrest in a much shorter time than in communities that are more prepared.

Issues & Possible Solutions to Power-Grid Failure

Large, interconnected power grids increase the risk of communities experiencing a sudden single point of failure. Electromagnetic pulse (EMP), geomagnetic disturbance (GMD), and cyberthreats are all significant threats to the nation's critical infrastructure. Addressing the threat requires a whole community approach – from putting the issue at the forefront of the public's attention to taking governmental action.

However, several respondents expressed concern that U.S. Federal Energy Regulatory Commission (FERC), whose mission is to provide reliable, efficient, and sustainable energy for customers, and North American Electric Reliability Council (NERC), whose mission is to assure the reliability of the bulk power system in North America, have

BioFire Defense has led

the industry for over 15 years

in pathogen identification

technologies.

Now, more than ever

we remain committed

to providing the industry

with superior products,

unsurpassed customer support,

and a solid future of

innovation and design.

Follow us, we'll show you how.

BIOFIRE™

DEFENSE

Follow us at www.BioFireDefense.com

not been effective in protecting the power grid. One respondent expressed concern that, "Since the definitive 2008 congressional EMP report, there have been no substantive plans in place … that have even started to effectively deal with any high-impact threats and hazards to the electric power grid."

"Ideally, the power companies would harden the grid," said one respondent, but everyone has a role to play. Suggestions for protecting power sources from a variety of threats include:

- Gathering better data and surveillance, as well as monitoring individuals or groups that could threaten the grid;
- Instituting state grid protections using independent experts and established professionals;
- Creating more microgrids, which are small-scale centralized electricity systems;
- Promoting personal preparedness measures – for example, bottled water, nonperishable food supplies, and generators;
- Creating standards to effectively deal with high-impact threats and hazards to the electric power grid (one respondent noted there have been no substantive federal plans in place since the April 2008 Congressional EMP report);
- Facilitating conversations with the public; and
- Providing public service announcements about personal opportunities and responsibilities to prepare.

One respondent defended the preparedness efforts of electric utility companies, "I work for a major electric utility. We are better than the media and the public give us credit for." This comment illustrates the need to bring this issue to the forefront of discussion and planning efforts, and open lines of communication between the government, private utility companies, and the public.

Catherine Feinman joined Team DomPrep in January 2010. As the editor, she works with writers and other contributors to build and create new content. With more than 25 years experience in publishing, she previously served as journal production manager for Bellwether Publishing Ltd. She also volunteers as an emergency medical technician, firefighter, secretary of the Citizen Corps Council of Anne Arundel County and City of Annapolis, and a Community Emergency Response Team (CERT) trainer.

Maine – A Journey Through State Grid-Protective Legislation & the Threat of Regulatory Capture

By Andrea Boland

What happened in Maine when the state legislature, receiving testimony from national experts, resolved to protect the electric transmission system from severe geomagnetic disturbances (GMD) and manmade electromagnetic pulse (EMP) weapons is a study in the stresses imposed by appointed regulatory bodies on legislative policy-making bodies. Here is a sketch of actions by the state and electric utilities, operating at both the federal and state levels.

The Maine Legislation

Legislative Document 131 (LD 131), "An Act to Secure the Safety of Electrical Power Transmission Lines," initially required all current and future transmission system upgrades to include protections against both solar storms (GMD/geomagnetic disturbance) and manmade electromagnetic pulse (EMP) weapons and terrorist devices. The Joint Standing Committee on Energy, Utilities, and Technology (EUT) of the Maine State Legislature held the public hearing in February 2013, and work sessions thereafter.

The electric industry initially opposed the legislation claiming that it was not needed. After compelling, data-driven testimony by independent experts showing big gaps in the security of the Maine grid, the EUT decided the whole grid needed to be protected. They turned LD 131 into a "resolve" that required the Maine Public Utilities Commission (PUC) to examine the vulnerabilities of the transmission system and identify options for mitigation measures – including low-, mid-, and high-cost options, and a time frame for adoption.

The committee approved the bill unanimously as "emergency" legislation. Then, the House approved LD 131 unanimously; the Senate approved by a 32-3 vote; and the resolve became law on 11 June 2013. Its preamble states:

> "Whereas, in the judgment of the Legislature, these facts create an emergency within the meaning of the Constitution of Maine and require the following legislation as immediately necessary for the preservation of the public peace, health and safety; now, therefore, be it." (See the full text of the June 2013 Maine legislation on GMD and EMP)

It was a very clear directive. The Maine legislation called for a report from the Maine PUC due by 20 January 2014. Thomas Welch, chair of the Maine PUC, anticipated an on-time report; he noted that, as chair of the PUC, he could approve the reliability upgrades without awaiting the report. Representative Barry J. Hobbins (D-Saco) had promised at the close of the public hearing of the EUT, "I don't know what we are going to do, but I can tell you this – we are going to do something!" The legislative intent was clear: provide the information needed to protect Maine's electric grid. This was landmark legislation, heralded nationally and internationally. A single state had done what Washington, D.C., never has – passed legislation for GMD and EMP protections.

Inadequacy of Federal Protection

Efforts seeking GMD and EMP grid protections at the federal level have been frustrated. The Federal Energy Regulatory Commission (FERC) has no legal authority to initiate "reliability standards" for the electric utilities. Only the North American Electric Reliability Corporation (NERC), the industry association, has that authority.

When FERC tells NERC they must set those standards, NERC writes weak standards, say the standards are not needed, or argue for more time. With effective lobbying, the utility industry has repeatedly blocked federal legislation that would give FERC power to require higher reliability standards than those NERC proposes.

The electric utilities comprise the only national infrastructure that is self-regulated. Some independent experts worry about the degree to which FERC seems to accommodate them. William R. Harris, secretary and counsel to the Foundation for Resilient Societies, on 1 November 2014, compared the regulatory capture problem at FERC with that at the Federal Reserve in a shared email among interested parties, responding to a publication article.

What a contrast: the Fed [Federal Reserve Bank] has extraordinary information subpoena powers, sanctions authority, and standard-setting that is not subject to veto by the regulated banks. Yet the Fed acts as if they must "get along" with the regulated firms even when they place society at great risk.

A fortiori, far weaker FERC Commissioners act as if they need to ingratiate themselves to the electric utility industry that operates with monopoly power to initiate reliability standard-setting.

The behavioral aspects of "regulatory capture" appear paramount. With FERC, Cheryl LaFleur (Chair of FERC) acts as if she has a psychological "need" to be in sync with the NERC culture, and to act as if scientifically-defective NERC reliability standards are OK because, as members of the NERC Board keep repeating: "Reliability is in our DNA."

The key difference between FERC and the Maine PUC is that the PUC, like the Federal Reserve Bank, has the authority to require the utilities to employ specific protections, even without waiting for a study. Also, like the Federal Reserve Bank, the PUC has come under scrutiny by Maine's Government Oversight Committee for a possible "culture problem," otherwise described above as "regulatory capture."

Protecting Maine's transformers, which would be irreplaceable for years in the event of a widespread blackout, conservatively is estimated at $7.2 million, or about $2.80 per household per year for about 5 years. If shared across all the states within the target area of ISO New England – the independent, not-for-profit company authorized by FERC to perform grid operation, market administration, and power-system planning roles for the region – that cost would drop to about $0.35. The protective equipment should last at least two decades, so the average cost over the life of the equipment would then be either $0.70 or $0.09 per household, respectively.

The Maine Public Utilities Commission Takes Over

From a hopeful start, in which the PUC provided an online docket for the study (Maine PUC docket 2013-00415, available online), it devolved into a draft report in December 2013 that showed utility bias, recommending: do nothing; wait for Washington. Reaction to the report was quick, professional, and condemnatory. National experts again turned their attention to the report and detailed errors, omissions, and shortcomings, and made corrective recommendations. Dr. Peter Pry, executive director of the Task Force on National and Homeland Security, conducted analysis that found the report to be "dishonest." His analysis is on the online Maine PUC docket 2013-00415.

When Welch presented the final report to the EUT in January 2014, he acknowledged GMD and EMP were serious problems, hence the PUC needed more time. Delay was reminiscent of NERC/FERC history. Welch proposed a task force with Central Maine Power Company (CMP) as coordinator. CMP had a convenient location, but had been unable to answer legislator questions during hearings. At one point, Chair Hobbins said, "I feel if we ask you one more question, you'll throw up your hands and say, 'guilty'." The sponsor and experts welcomed the revived focus, and inclusion of outside expertise.

Professional report – using independent modeling, real-world data, and NASA probabilities shows protection against 100% probable blackouts lasting months or years would cost pennies per household per year. Maine PUC dismisses, argues, "too costly."

Two independent experts were invited to participate: John Kappenman of Storm Analysis Consultants; and Thomas Popik, president of the Foundation for Resilient Societies. EMPrimus, a research and development company that had offered expert docket input, also was invited to participate. The monthly meetings focused predominantly on GMD. CMP's Brian Huntley's leadership seemed strong, but there was some worry that, as with NERC/FERC processes, the report would be sabotaged before it was complete.

In September 2014, Huntley left CMP, and the task force meeting was canceled. On September 24, Welch assured the Government Oversight Committee that the report would be out by December, EMP would be covered, and staffers were working with EMPrimus. Later that day, he announced his early retirement for 31 December 2014. [Note: As the bill's sponsor, I made phone calls to CMP that were not answered.]

Central Maine Power Company Finds No Protective Equipment Is Needed – The Grid Could Withstand Any Threat Their Model Could Conceive

The last study group meeting was on 27 October 2014. Justin Michlig, lead engineer of system planning at CMP, who became the new CMP project manager of the study in late September, invited EMPrimus to present its report. EMPrimus utilized independent (PowerWorld Corporation) modeling, real-world historical data, mitigation equipment, and NASA probabilities for a 100-year solar storm (12 percent within a decade, 50 percent within a 30-year period). The EMPrimus report found that "reactive

power" equipment might temporarily stabilize grid voltage in a solar storm. However, there would be five-minute periods necessary to reset key equipment, during which the grid would be at risk of collapse. During prior solar storms, Maine's reactive power equipment had become inoperable on multiple occasions. EMPrimus proposed the installation of 18 neutral ground blocking devices. These would protect transformers and keep geomagnetically induced currents out of the high-voltage Maine transmission system.

Then, Michlig presented CMP's analysis. The modeling relied on the technically dubious NERC "GMD Benchmark Event" methodology in the still unapproved standard and did not use CMP's own recorded data for validation. The CMP scenario assumed that "reactive power" equipment always worked, despite outages in past solar storms. CMP found no need to install any protective equipment. Michlig gave no answers to questions of why they ignored their own historical data. Lisa Fink, PUC staff attorney and project manager of the PUC work, backed up Michlig. The CMP Draft Report will be available later in November 2014 for comment.

It was surreal, appearing that Maine's PUC exhibited the kind of "regulatory capture" that has troubled the Maine public and its legislature. Like NERC, the PUC had cordially supported the mission, opened an online docket, and then manipulated data and assumptions to avert protection of the Maine grid.

The emergency legislation did not ask for the recommendation of the Maine task force and its PUC staffers. It asked them to identify vulnerabilities, options for protections, and costs, so that the legislature, on behalf of the people of the State of Maine, could make their own decisions on protections. [Note: As sponsor, I reminded them of that at the meeting and asked them to be sure to read the legislation; they said they would.]

At the time of this writing, the nation still awaits the draft report. However, the PUC has taken down the online docket – a recent change that blocks public view.

Update (11/21/14): Representative Boland, working with others, was able to get the docket back up online.

State Representative Andrea Boland is completing her eighth year in the Maine legislature. She is considered a leader in safety issues of electromagnetic radiation, especially from cellphones and smart meters. She became involved in electric grid protection against electromagnetic pulse and geomagnetic solar storms (GMD) at the suggestion of her regular scientific advisor. Her work is supported by several national experts. She has a B.A. degree from Elmira College and an MBA from Northeastern University, and studied at the Sorbonne and Institute of Political Studies in Paris. She was awarded the 2011 Health Freedom Hero Award by the National Health Federation for her work on health freedom and safety. Her legislative work has led to confronting major corporate interests on matters of transparency and regulatory capture, and public protections.

Challenge: Defeat Ballistic Missile Attacks From the South

By Henry (Hank) F. Cooper

October 22 marked the 52nd anniversary of President John F. Kennedy's television announcement that Soviet ships were transporting nuclear weapons and ballistic missiles to Cuba – constituting a mortal threat to the United States. Miami was only 90 miles away and those missiles could have reached much farther.

Actually, the situation was worse than President Kennedy knew. After the Cold War, former Soviet authorities revealed that 100 nuclear weapons were already in Cuba and Fidel Castro wanted to keep them. Soviet General Secretary Nikita S. Khrushchev overruled Castro and removed them as the crisis wound down. Notably, the United States removed its nuclear-armed missiles from Turkey.

Many believe this crisis was the closest America came to nuclear war during the Cold War. The United States now confronts another existential threat from the South, in at least two ways.

A Modern Nuclear Missile Crisis

As illustrated in Figure 1, a North Korean freighter was caught in June 2013 smuggling military cargo from Cuba through the Panama Canal, into the Gulf of Mexico. Included were two SA-2 missiles, each capable of carrying a nuclear weapon, as the Soviets designed during the Cold War. They could have been launched to attack the United States from that freighter – or Cuba, Venezuela, or some other country – and currently there is little or no defense against them.

Such nuclear weapons need not be exploded in U.S. cities. Indeed, their effects would be far more devastating if detonated at high altitude to produce an electromagnetic pulse (EMP) to debilitate major segments of the currently unhardened U.S. electric power grid – with cascading disastrous effects over much of the nation.

This threat was identified by the congressionally mandated EMP Commission in 2004 and 2008 and reiterated by many informed authorities, but the grid is still unhardened against such attacks. In addition, the United States operates no missile defense against such threats, although the U.S. government could rapidly and inexpensively deploy one.

Figure 1 also illustrates that Iran and North Korea launched their satellites southward such that they passed over the South Polar region before approaching the United States from the South. North Korea is reportedly again preparing to launch a satellite, no doubt with Iranian scientists and engineers present as in the past.

If such a satellite carries a nuclear weapon, it can be detonated over a hundred miles above the United States in its first orbit to produce an EMP that could take down the unhardened U.S. electric grid for an indefinite period. Such an attack would return America's current just-in-time economy to that of the 19th century and leave many millions more people at risk without the life support and security of the agrarian society of that era.

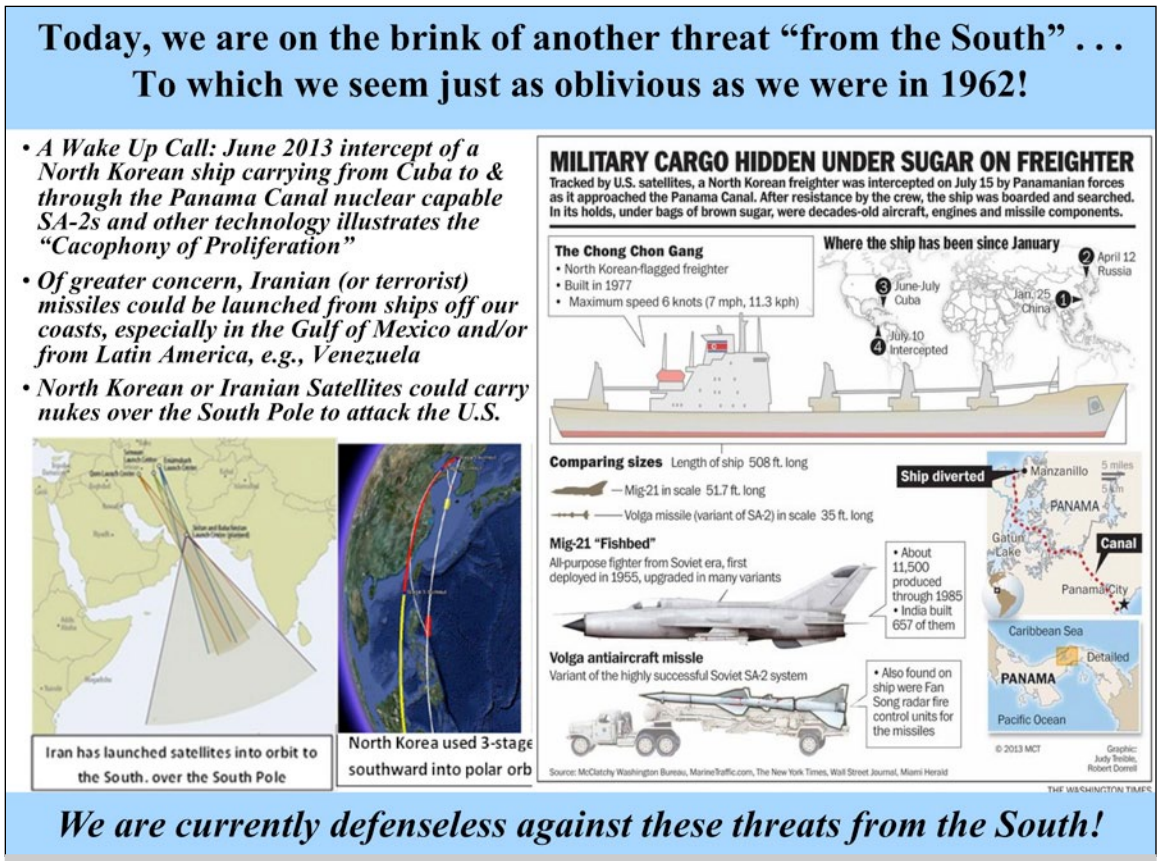


Figure 1: Illustration of Iranian and North Korean actions that could have U.S. consequences.

Credible estimates suggest most of the over 300 million people in the United States would die within the next year from starvation and the consequent chaos. For example, Dr. William R. Graham – former director of the White House Office of Science and Technology Policy and chairman of the EMP Commission – so testified before the House Armed Services Committee on 8 July 2008, and numerous others echo his and the commission's statements.

Response: Upgrade U.S. Missile Defenses

U.S. homeland ballistic missile defense (BMD) sites in Alaska and California provide a limited defense against North Korean and Iranian intercontinental ballistic missiles (ICBMs) that approach the United States from the North. The government currently plans to deploy another ground-based site in the northeastern United States to increase that capability, especially against Iranian ICBMs. However, the threat from over the South Polar region has largely been ignored.

In particular, Americans are defenseless against ballistic missiles launched from vessels in the Gulf of Mexico or against a "satellite" attack from the South. That condition could be rapidly rectified by employing existing relatively inexpensive missile defenses.

To counter ballistic missiles launched from offshore vessels, the United States could employ its sea-based defenses, deployed on over 30 cruisers and destroyers at sea around the world. If prepared to engage, such defenses are inherently capable of shooting down missiles launched from almost anywhere.

The U.S. Navy has repeatedly demonstrated that the Aegis BMD system is capable of shooting down attacking missiles while they are ascending from their launch points and above the Earth's atmosphere on their way to their targets. However, the ships must be appropriately located, with crews trained and ready, to shoot down missiles intended to attack the United States.

On a random day in 2013, there were four to six Aegis BMD ships along the eastern seaboard or in an east coast port. Under this condition, the east coast can be defended if the Aegis BMD ships are appropriately located and their crews are trained and ready to engage. Those in charge of homeland defenses can assure these conditions are met.

Since Aegis ships usually do not traverse the Gulf of Mexico, threats from the Gulf likely would remain. The United States could affordably purchase and deploy on military bases around the Gulf the same Aegis Ashore system it is building in Romania (to be operational within months) and Poland (to be operational in 2018). No new development is required, just the agreement of the local and state authorities for placing these systems on bases such as Tyndall Air Force Base in the Florida panhandle – the location of First Air Force, the command responsible for the air defense of the continental United States.

This country is building Aegis Ashore bases to protect NATO allies against Iranian ballistic missiles, surely it can build the same "football-size" installations to protect U.S. citizens. There already is a site for testing in Hawaii, so additional sites around the Gulf of Mexico, and possibly along other coasts, could close operations gaps in defense coverage provided by the normally operating Aegis BMD ships.

Furthermore, the first generation Aegis system was used in 2008 to shoot down a dying satellite before it could spread its toxic waste on populated regions on Earth.

Today's improved Aegis BMD system retains an improved inherent capability to support homeland defense missions involving threats from satellites approaching North America from the South. What is required technically is sensor information to launch the Aegis interceptors on the right track to complete the intercept with their on-board sensors – a continuously improving global sensor capability.

If a satellite is at an altitude that exceeds the Aegis interceptor's altitude range, then ground-based interceptors on Vandenberg Air Force Base, California, can complete the intercept, provided they have the needed upstream sensor cues. Aegis BMD ships also can help with this capability, as well as other sensors such as forward-based radar and space-based sensor systems.

Bottom Lines

Other initiatives to help counter the existential EMP threat are discussed in a 3 October 2014 *Investor's Business Daily* article and elaborated in High Frontier's email message on 8 October 2014. The above discussion simply emphasizes the reality of the manmade, ballistic missile threat and possible, essentially off-the-shelf, means to defend against it.

The electric grid also should be hardened against nuclear EMP effects because no defense is perfect. If that is done, the grid also will be hardened against nature's EMP threat, which is produced by solar storms. No defense will protect against natural EMP from a solar storm that will one day occur, but defenses can be built faster than the grid can be hardened. Both remedies to the nation's current vulnerability should be initiated without further delay.

Finally, hardening the grid against only the solar storm-produced EMP will not assure the grid is hardened to the shorter wavelength EMP threat posed by a high-altitude nuclear explosion. If, for political reasons, the solar threat is taken as the primary reason for hardening the grid, that hardening effort should accommodate the entire EMP spectrum to protect against nuclear EMP attack.

Ambassador Henry (Hank) F. Cooper is chairman of High Frontier and a former acquisition executive for all U.S. ballistic missile defenses. He also served in several other senior U.S. government acquisition and policy positions, including as President Ronald Reagan's chief negotiator at the Geneva Defense and Space Talks with the Soviet Union and U.S. Air Force deputy assistant secretary for strategic and space systems. He currently is focused on helping local, state, and federal authorities protect against the natural and manmade electromagnetic pulse threat by building effective ballistic missile defenses and hardening the electric grid. This article is adapted from his 22 October 2014 presentation at a South Carolina InfraGard Members Alliance Conference on Sullivan's Island.

Grid Power Failure – Alternative Energy Systems That Work

By William Kaewert

The conventional utility power grid is vulnerable to a number of threats that can cause failure over wide areas. Most people understand that power failure can be caused by frequent, low-impact events such as ice storms and hurricanes. Less well understood are high-impact, low-likelihood events on the power grid, such as geomagnetic disturbance (GMD) caused by solar storms, or deliberate cyber or electromagnetic pulse (EMP) attack.

In fact, the Congressional EMP Commission and others have warned multiple times of the probability of widespread, long-duration power outages in the wake of a large GMD or EMP attack. Some of the failure mechanisms identified by the Congressional EMP Commission include permanent damage to extra high-voltage (EHV) power transformers and damage to electronic controls in multiple networks, including electric power distribution, fuel pipelines, transportation, communications, and other critical infrastructures. The extent and duration of these failures would be without precedent.

One question sometimes asked by people contemplating long-duration failure of the power grid is, "Are alternative energy systems such as home solar photovoltaic (PV) power systems or wind farms viable sources of electricity should a widespread grid outage occur?"

The bad news, and shortcoming of many small alternative energy systems, is that most alternative energy systems would not be able to deliver power after a power grid outage. The good news, though, is that, with planning and knowledge, some of these systems can be designed ahead of time, or retrofitted, to operate in "off-grid" or "island" mode, such that they can deliver power after a grid failure.

"Island Mode" & Power Grid

Most emergency generators and microgrids – networks of two or more generating sources, such as photovoltaic, wind, and combustion engines – are capable of operating either independent of, or in conjunction with, the conventional utility power grid. When the power fails, these sources serve as "islands" of electric power – hence, the terms "island mode" and "off grid." Two pieces of equipment are essential to island operation: (a) a prime mover (solar panels, wind turbine, combustion engine); and (b) a transfer switch to isolate the "island" from the utility grid. Even large microgrids such as university campuses, airports, and other large facilities are equipped with the means to connect to, and disconnect from, the utility grid.

What differentiates "islanding" capability from other generating sources – alternative or otherwise – is that a generating "island" is designed to operate independently from the conventional power grid. Unless the owner of a particular generating asset such as wind farm or home PV system clearly specified that the system must operate in "island mode," the asset is unlikely to function after a grid outage. In other words, just because solar panels are installed on a roof does not mean that the power they generate

is available when the power grid fails. Before discussing why rooftop PV systems stop running when the grid fails, it is necessary to understand how and why the power grid functions.

Known as the most complex machine ever built, the U.S. power grid is a vast network of generating plants, EHV transformers, high-voltage transmission lines, substations, a low-voltage distribution system and computer controls throughout. Assuming that one power plant in a network of thousands goes offline, all remaining plants in the system will make up the difference such that no customers lose power. If power were unavailable from multiple plants simultaneously, demand for electricity would greatly exceed supply. The result of this imbalance is a collapse of alternating current frequency and voltage.

To prevent this collapse of frequency and voltage from propagating across a wide region, including to customers whose local power plants and transmission resources are not damaged, automatic protection systems in the power grid isolate areas where demand exceeds capacity. Normally these systems function quickly and seamlessly, but sometimes they fail in spectacular fashion. When a tree limb fell on a transmission line in Ohio in August 2003, for example, power was lost across large portions of the mid-Atlantic region and into Canada. Failure to isolate intact power grid assets from the failed regions causes an almost immediate cascading failure.

Alternative Energy Systems & Power Grid Failures

Unless specified as an "off-grid" or "island" system, most home solar PV systems – including rooftop solar power systems – are synchronized to the alternating current frequency of the power grid. This enables seamless import of utility power to the home at night and export of power from the solar panels during times of peak production. When failure of the power grid in the PV-equipped home's neighborhood occurs, protective systems in the solar power inverter shut down the home system for two reasons:

- To prevent damage to the system inverter from massive overload when one home system attempts to power an entire neighborhood; and
- To eliminate the risk that power produced by the PV system will energize downed utility lines and expose repair crews to dangerous voltage – these power systems are subject to the Underwriters Laboratories standard (UL 1741) and to the National Electrical Code (NFPA 70).

The cheapest and simplest way to perform these tasks is to just shut off the home inverter unless grid power is present. Unfortunately, this solution leaves the homeowner literally in the dark, *unable to access the power generation resource on his roof* during a utility power failure.

A similar mechanism is designed into wind farms, including even the largest farms with hundreds of megawatt-rated or larger turbines. When the power grid fails, each turbine is designed to feather its blades such that the turbine stops turning. Even though output of the wind farm might be large by household standards, the suddenly massive load applied to the wind farm by the wide area grid is just as overwhelming to the wind farm as the neighborhood was to the homeowner's small PV system. The turbines

shut down to protect from this overload, and to insure that transmission lines are de-energized and thus not a threat to repair crews.

Specifying a Residential Microgrid

Although technical specifications are beyond the scope of this article, the following guidelines provide important considerations when specifying a new, or retrofitting an existing, alternative energy source, such that electric power will be available in the event of a utility outage:

- *The system must be specified to operate completely independently of the power grid.* One test to determine whether an existing power system is capable of off-grid operation is to shut off the main power feed to the home or facility in question. If the alternative source cannot deliver power when it ought to – for example, during midday for a solar PV system – the system is not independent of the power grid.
- *There is a manual or automatic transfer switch installed at the utility entrance point that enables the alternative energy source to be disconnected, either automatically or manually, from the utility grid.* The transfer switch protects the home system from the relatively infinite load presented by the grid, and prevents the home system from energizing neighborhood power lines. Transfer switches add cost and complexity to alternative energy system, but are essential for safe off-grid operation.
- *The alternative energy system includes either on-site energy storage assets, such as a battery, or a fuel-consuming generator, such as a gas or diesel engine or a fuel cell.* Without either of these elements, power will not be available from the alternative energy system during times when the alternative energy source is nonproductive – for example, darkness for a PV system and lack of wind for a windmill.

It is not difficult to specify a new alternative energy system, or convert an existing one to operate "off grid." It does, however, demand sufficient knowledge about distributed energy and alternative energy systems and a contractor experienced in building "off-grid" energy systems. Some suppliers are even able to harden off-grid energy systems to the effects of EMP attacks and geomagnetic storms. During a utility power grid outage, people who properly specified and built their own "off-grid" system will stand a good chance of enjoying the many benefits of electric power, and will be in a position to help their less-prepared neighbors in a time of need.

William Kaewert is founder of two power protection companies and has over 30 years' experience applying technology-based solutions that assure continuity of electrical power to critical applications. He is currently president and chief technology officer of Colorado-based Stored Energy Systems LLC (SENS), an industry leading supplier of nonstop DC power systems essential to electric power generation and other critical infrastructures. The company also produces COTS-based power converters used in EMP hardened military systems including ground power for Minuteman III ICBM and THAAD ballistic missile interceptor. He received his AB in history from Dartmouth College and MBA from Boston University. He serves on the board of directors of the Electrical Generation Systems Association (EGSA) and on the management team of the Federal Bureau of Investigation's InfraGard Electromagnetic Pulse Special Interest Group.

Electromagnetic Pulse Triage & Recovery

By Charles (Chuck) L. Manto

Emergency medical technicians and paramedics triage patients for mass-casualty incidents. Hospital emergency rooms have triage nurses to determine the level of care needed. Community Emergency Response Team (CERT) participants are taught how to quickly sort and tag victims so they can focus on the seriously injured and sustain them until help arrives. Conversation about high-impact disasters should convey hope. Without the hope of recovery and the management capacity implied in the word "triage," the problem may seem overwhelming. One sign of hope is that an economic impact assessment on electromagnetic pulse (EMP) showed that protecting even 10 percent of the most critical infrastructure could avoid up to 60 percent of losses. Triage helps identify that 10 percent.

Triage is especially helpful in the case of a high-altitude nuclear burst EMP or severe solar storm. Depending on who is in charge and where the impacted organization is located relative to the event, actions will range from relatively easy to nearly impossible. Knowing the difference makes it possible to begin developing and deploying plans now in order to manage and recover from such incidents in the future.

How EMP Works

Large solar storms create ground-induced currents similar to the slow-rise time pulse of a large high-altitude nuclear EMP burst, known as E3. Currents can connect with conductors in the ground to damage equipment connected to ground wires, including large transformers that may take over a year to replace.

A high-altitude nuclear burst from even a small weapon could disrupt or damage electronics at nanosecond speeds within a specific region and, under the right circumstances, across the continental United States. Smaller electronic hand-held or vehicle-mounted electromagnetic interference (EMI) devices only act on equipment that is at fairly close range and require a number of people to cause interruption in a large area, but can pose serious threats like other coordinated physical attacks. Protecting equipment from high-altitude EMP also protects against smaller EMI weapons.

Manmade EMP creates both a radiated pulse through the air and a conducted pulse along cables. See the article by George Baker, professor emeritus at James Madison University, for more-detailed explanations and discussions of common misperceptions about EMP.

For any triage scenario, sometimes the most difficult tasks are ultimately "written off." For example, although protecting large power utility generators and transformers is relatively inexpensive, a moderately difficult activity for utilities would be nearly impossible for an outside firm to impose on these utilities. At this time, only a few utilities have begun the process of protecting their most critical assets and earning certification by independent testing authorities to prove they meet objective standards of protection from either EMP or a hundred-year solar storm. The InfraGard National EMP Special Interest Group's (SIG) conference proceedings of 2012 and 2013 include technical, economic,

policy, and emergency management resources, which help corporate as well as local and state government officials to assess: (a) what can and is being done (or not done) at the federal and industry-wide levels; and (b) what, in this class of threats, requires an all-of-nation response.

Benefits of EMP-Protected Microgrids & Local Networks

From a triage perspective, scenarios involving a nationwide collapse of centralized infrastructures for 1-12 months or longer would highlight the need for companies and organizations to avoid total dependence on large centralized systems outside of their own control and plan. For this reason, the EMP SIG is creating a workshop and tabletop exercise package along with background technical and engineering information that it will make available to state and local government emergency management after the completion of its workshop and facilitated discussion on 4 December 2014.

As organizations face the prospective collapse of centralized infrastructure, they may become motivated to discover how to make and store enough power locally to continue to operate indefinitely without a centralized power grid and communications network. In fact, protected microgrids and local networks would make the centralized grids more resilient because those islands of sustainable power would minimize the domino effect of cascading failures inherent in a regional or nationwide incident.

Industries and communities that produce some of their own power would save or make money by avoiding peak load charges. Local communities that already produce their own power will find it easier to protect their assets than with larger systems. Fortunately, for those wanting to produce and store power for their own facility or campus, technologies are available and new technology in the near future will make it more cost competitive with centralized systems, especially given the resulting improved sustainable reliability. There are some companies including utilities that are offering systems integration services for microgrids. In time, they also could provide EMP-rated microgrids.

Local EMP Protection – The Easy Part of EMP Triage

Fortunately, organizations can take some relatively easy and inexpensive steps on their own. For example, since EMP and intentional EMI are either radiated through the air or conducted through power or communication lines, one easy and nearly free action any organization can take to reduce the probability of EMP disrupting or damaging critical equipment would be to unplug equipment that is not being used. Emergency operations centers, which are often reserved for emergencies and not used much of the time, have multiple computer and communication stations connected to power and communication lines 24/7. If unused subsystems were to be unplugged when not in use, then the conducted pulses would not be as likely to couple with the systems through those conductors.

Circuit breakers or plug connections could be deployed in easy-to-see locations at eye level so facility managers can walk into rooms and see at a glance whether unused systems are plugged in. Requiring managers to walk around and crawl under desks to see if something is plugged in is not a sustainable maintenance method. Unplugged systems still would be vulnerable to EMI through the air, but unplugging them when not used

would increase the chances of survival. In addition, less power used for standby capability would actually save money for organizations. The savings then could be used to purchase EMP-rated surge protectors or electronic filters for electric distribution systems so those particular lines would be able to pass through power while filtering excess EMI during operation. Filtered lines also deliver "cleaner" power to devices, minimizing the impacts of small day-to-day surges and fluctuations that reduce equipment health and lifespan.

Perhaps the simplest and least expensive measure to protect equipment from radiated EMI would be to place spare equipment into EMP-shielded containers or rooms. In this case, solid metal containers that are independently EMP rated are the most reliable solutions. Homemade solutions also may be effective, especially for those who are required to have fire-rated steel safes for files, equipment, or firearms. In these cases, there should be no holes into the safe, and doors should have metal gaskets around all of the edges so signals do not travel through the seams or edges of the closed door.

Similarly, steel or aluminum garbage cans for this use should have metal tape applied to the seams and metal gaskets of the same or compatible metal as the can around the inside of the lid. Aluminum tape or gaskets applied to an iron or steel surface, for example, would result in corrosive interactions between the different metals, which would degrade the shielding. In addition, the inside needs to be lined with a nonconducting insulation layer to protect equipment from the metal layer that will hold or pass a charge.

Somewhat More Difficult Local EMP Protection – Moderate EMP Triage

Shielding operating equipment and rooms from airborne EMI is a little more complicated and expensive because these rooms have power, communications, and air circulation that make shielding more difficult but not impractical. Business arrangements prove that even cash-poor organizations among counties, hospitals, or universities can acquire equipment at no monetary cost by providing in-kind resources to business continuity parks that would provide protection to organizations as they create EMP and cyber-resilient local networks supported by local power generation and energy storage systems.

Some buildings constructed entirely of steel may have enough inherent shielding properties built in that could be modified to provide a small measure of EMP protection. For example, some all-steel buildings may have enough shielding value in their material that could provide as much as 30 decibels (dB) of the 30-100 dB of protection required by military specifications if those buildings were to be modified as a consistent shield. Even a lower level of shielding such as this will improve the odds that equipment might survive a given EMP event. (Every 20 dB of protection reduces the amount of EMI passing through the shield by a factor of 10.)

Meeting the Military Standard Tests

The military standard 188.125 for EMP protection currently requires a minimum reduction of the pulse by a factor of 1000 or 80 dB – that is, the reduction deemed necessary to allow otherwise vulnerable equipment to operate without disruption while under an EMP attack. Even these levels of protection do not have to be cost-prohibitive, especially if built into infrastructure in the beginning of the planning process.

Operating equipment can be shielded from radiated pulses by placing equipment into cabinets or rooms that are shielded on all six sides by either welded (best) or bolted (next best) metal to ensure protection at a given level. These rooms and equipment also must be protected from conducted pulses since cables either act as antennae that promulgate the pulse into the room or provide direct pathways into the equipment they connect. All power and communication wires must be filtered from excess electromagnetic energy. Conductors of any sort must be placed into a shielded space with proper filtering and connections.

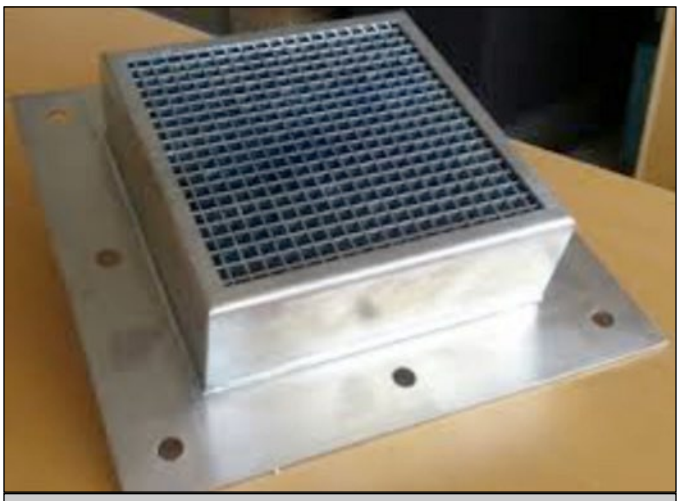


Figure 1: An EMP-rated waveguide for airflow.

In addition, waveguides can protect air passageways by capturing the electromagnetic waves and connecting them back to ground connections (see Figure 1). EMP-rated doors and sally ports need to be tested to ensure that they do not compromise the rooms (see Figure 2). Ideally, management will support and determine that continued maintenance and testing will be performed on the most critical infrastructure deserving this level of protection.

It is critical that subsequent changes do not damage the shielding effectiveness. Business continuity, security, change management (i.e., a management process used to make systems, usually information technology and infrastructure, to ensure consistency with overall requirements), and maintenance systems should all be integrated to ensure the alignment of management objectives and day-to-day practice. More than once, multimillion dollar facilities have been compromised because someone decided to casually drill a hole through a shielded room to place antennas through the shield for a better communications signal. Experienced contractors could ensure that the work is tested against objective standards and the desired EMP protection is maintained over time.

Simplifying a Civilian Critical Infrastructure EMP Rating System

Civilian critical infrastructure managers would be better served by a simple and understandable EMP rating system such as the one used by the Uptime Institute for data centers, which ranks them from low (Level 1) to high (Level 4) based on their resilience. One industry practice proposed by Instant Access Networks takes a similar approach by providing objective standards against which EMP-protected facilities and equipment could be measured. In this approach, Level 3 would be a way to meet all harmonized military standards for EMP and Tempest (signal emitting protection) at a 100-dB level. For those who want a greater level of protection, Level 4 provides 140 dB of protection, while Level 1 provides 30 dB and Level 2 provides 60 dB.

This is especially useful in a systems approach to civilian critical infrastructure that can be composed of rooms, systems, facilities, campuses, and networks spanning regions or continents. Not all components or systems will require the same amount of protection and not every system is equally valuable. An overall design approach to business continuity will require different levels of protection depending on the importance of the system element being protected and its vulnerability. Instant Access Networks LLC devised the following way to show ranges of protection that may be relevant to various elements – power, data, and communications – in a 4-level, system-wide protection method where Level 3 meets or exceeds various military specifications for EMP and Tempest requirements.

Large data center and control rooms have been constructed to meet EMP standards for the military for decades. In the past year, a U.S.-based utility created an EMP-protected control room in Texas and an insurance company built an EMP-protected data center in Pennsylvania. Mass producible EMP-protected equipment such as cabinets, transportable 8 x 20 foot cargo containers, mobile command centers, and microgrids could be deployed across networks and control facilities so racks of computer or communications equipment and their power systems could be protected within them.

Figure 2: EMP-protected doors and filter systems as part of EMP protected 8x20 foot cargo containers.

Getting Help

EMI threats can be complicated to understand and even tougher to mitigate. However, by following these simple triage steps, organizations can acquire EMP protection that can also protect life-sustaining systems from the effects of smaller EMI weapons and larger solar storms. In order to confidently take steps to protect critical infrastructure, here are three categories of available resources:

- *Written resources:* In addition to the conference proceedings of the InfraGard National EMP SIG, there are a number of information sources. First, there are general studies such as the work of the U.S. Congressional EMP Commission and various public domain military standards and manuals. Second, there are organizations such as the IEEE Electromagnetic Compatibility Society (EMC-S) that looks at various types of EMI that can be caused either intentionally or accidentally. The EMC-S also holds regional meetings and an annual meeting around the country. Trade magazines such as Interference Technology will cover issues that include intentional EMI and covers vendors that are active in the field.

- *Corporate resources:* Some interesting and helpful resources are testing companies and organizations, which understand the standards and how to meet them. It is possible to develop relationships with testing company staff well enough to ask what to look for when evaluating vendors. These include companies that test systems and buildings for EMP protection, such as SARA, Inc. or Jaxon Engineering in Colorado Springs, Colorado, and Little Mountain Test Facility at Hill Air Force Base in Ogden, Utah.

- *Conferences and tabletop exercises:* The InfraGard National EMP SIG is conducting its annual conference at the Dupont Summit on 5 December 2104 and will hold a by-invitation-only tabletop exercise on 4 December.

When purchasing products that claim to be EMP protected, it makes sense to ask the vendor: (a) what they mean by that; (b) which objective measure they are using; and (c) whether the product has been tested by an independent testing organization. It also is important to know when a company claims that their product meets an EMP testing standard to know if it meets the entire standard or just part of it. There are some who are experienced in offering EMP triage consulting that also can be engaged. These simple precautions will be helpful as the urgency, importance, and affordability of EMP protection becomes apparent both on its own merits and as part of a total cybersecurity framework. Working together with other users also will make the entire process more interesting, effective, and affordable.

Charles "Chuck" Manto is chief executive officer of Instant Access Networks LLC, a consulting and research and development firm that produces independently tested solutions for EMP-protected microgrids and equipment shelters for telecommunications networks and data centers. He received six patents in telecommunications, computer mass storage, and EMP protection and has another one pending for a smart microgrid controller. He is a senior member of the IEEE and founded and leads InfraGard National's EMP SIG. He can be reached at cmanto@stop-EMP.com

Satellite Navigation & Timing: Good News, Bad News

By Dana A. Goward

Wall Street Examiner Commentary, 18 July 2016 – Few people had realized how many things depend on the Global Positioning System (GPS) – until GPS failed. The first thing most people noticed were record traffic jams in the centers of every major city. Downtown traffic lights were no longer synchronized, drivers were even more distracted than usual and could not find their way, so the number of motor vehicle collisions soared. First responders' radio and dispatch systems worked poorly, if at all. Public safety responses were delayed even more by navigation and traffic problems. When cellphone networks started failing, people began realizing that something had gone terribly wrong.

They noticed that the Internet was not working properly, and ATMs were no longer dispensing cash. Banks, credit unions, and stock exchanges closed for the day because they were unable to reconcile accounts or time-stamp transactions. Scattered power outages added to the general sense of unease. There were isolated reports of violence when people could not access their money, could not get where they needed to go, and saw the power fluctuate. Government officials predicted widespread civil unrest if service was not restored quickly.

Fortunately, the GPS outage only lasted 11 hours. Unfortunately, though, it cost the nation $40 billion in lost productivity, a massive oil spill in San Francisco Bay, two aircraft incidents, countless traffic collisions, and 35 transportation-related deaths over and above those normally expected.

Current Systems & Vulnerabilities

The Good News – The above story is fiction, or at least has not happened yet. Although many people rely on navigation and time signals from U.S. GPS for thousands of everyday uses, the satellite constellation is superbly maintained and operated by the U.S. Air Force. It has never suffered a major failure in its 30+ year history.

The Bad News – The Russian equivalent satellite system, GLONASS, failed for 11 hours in April 2014. Two weeks later, it failed again for half an hour. Satellites are vulnerable to space weather, cyberattack, human error, and growing fields of space debris. Their signals are exceptionally weak and easy to disrupt either intentionally or accidentally. Almost every national military has the capability to jam GPS over broad areas, and the technology is easily available to non-state actors. GPS signals are disrupted tens of thousands of times a day. Fortunately, it is usually across small areas and for short periods, by people using illegal, but easy to obtain, personal privacy devices.

"Spoofing" is becoming more of a problem. By transmitting a similar, yet slightly stronger signal, bad actors can provide false time signals for transactions or takeover a vehicle's navigation. Yet, GPS signals are highly precise and free, so they have been incorporated into nearly every facet of modern life. As Bradford Parkinson, Ph.D., known as the "father of GPS," has observed, reliance on these signals has become "a single point of failure for much of America and is our largest, unaddressed critical infrastructure issue."

New Satellites & Signals

The Good News – New GPS III satellites will help address some of these issues. And some new receivers are being modified to make them less susceptible to spoofing.

The Bad News – Signals from space will always be faint and, therefore, easy to disrupt. U.S. military forces regularly exercise for "A Day Without Space." The Russian military assumes as a matter of doctrine that all space services will be denied to them in combat, because it is so easy for an enemy to do so.

"As Bradford Parkinson, Ph.D., known as the 'father of GPS,' has observed, reliance on these signals has become 'a single point of failure for much of America and is our largest, unaddressed critical infrastructure issue'."

Cost & Implementation

The Good News – A big part of the solution for domestic preparedness is fairly simple and inexpensive. A complementary terrestrial system, based on a mature technology called eLoran, could transmit GPS information at very high power and low frequency, and would be very difficult to disrupt. Although this "GPS-Earth" system would not be quite as precise as "GPS-Space," it would more than meet the needs of 98 percent of users, and have the added benefit of being usable indoors, underground, and underwater. It would both deter those who might want to intentionally disrupt GPS, and provide a second source of information at times and in locations where GPS-Space was not available. With GPS-Space costing over $1.2B per year, GPS-Earth would be a bargain at about $40-50M per year to build and operate across all 50 states.

The Bad News – Although the federal government announced in 2008 that it would build such a system to protect the nation's critical infrastructure, it has never acted on that pledge. It has even begun dismantling and disposing of infrastructure that could speed implementation. And while America has become progressively more dependent on navigation and time from space, Russia, China, Iran, Saudi Arabia, South Korea, and northwestern Europe are all improving their terrestrial backup systems. India and other nations are following suit.

Government Efforts

The Good News – The U.S. Congress has begun to notice the problem and ask questions. The 2014 Defense Authorization Act tasked the administration with

reporting how it will maintain essential national security services when space systems were not available. And a bill approved by the House and under consideration in the Senate would direct the administration to halt dismantling and disposing of infrastructure that could support a quick and inexpensive eLoran/GPS-Earth build-out. It also authorizes partnerships between agencies and/or with private entities to construct such a system.

The Bad News – Although there appears to be some ongoing discussion within the administration as to the path forward on this critical issue, very little has been done.

The Hopeful News – Many people in the administration are worried about GPS vulnerability and want to help protect the United States. Anyone can encourage and help them, support Congress's interest, and raise this issue above the bureaucrats to the leadership level.

Dana A. Goward is the former maritime navigation authority for the United States and is now president and executive director of the nonprofit Resilient Navigation and Timing Foundation. The foundation is dedicated to educating the public about the importance of navigation and timing signals, supporting stronger laws and better enforcement to combat Global Positioning System (GPS) jamming and spoofing, and supporting establishment of strong, difficult-to-disrupt terrestrial systems to pair with GPS. To learn more, visit www.RNTFnd.org

Community Preparedness for Power-Grid Failure

By Mary D. Lasky

When emergency managers perform their jobs well, citizens may feel the government will be there to help in times of emergency. For emergencies that last a few days, most people are able to take care of themselves. Many people may not have considered what happens when emergency managers are not able to respond because of the severity of the event. Planning for large disasters is difficult and there is a fear that even discussion could cause panic among citizens. However, when able to think about it ahead of time, organizations and members of the public would know what they can do to prepare for a major disaster, and thus reduce panic.

Loss of the Electric Power Grid

The grid is the generation and distribution of electrical power in interconnected local and region systems across the entire country. It is possible for certain events to cripple or disable parts or all of this interwoven structure. As a nation, the United States thus far has been fortunate to not lose the entire grid.

A cyberattack could disable a local area or an entire region. It is conceivable that a group of coordinated cyberattacks could disable several regions simultaneously. Depending on the level of disruption to industrial controls that also could cause equipment damage, the length of time power would be lost would depend on the length of time before damaged equipment could be replaced. Given enough damage to parts requiring a long time to replace, outages could last from days to months.

In September 2014, a solar coronal mass ejection, or solar storm, came very near to disrupting power. A Lloyds of London report published in 2013 describes that a power outage across the northeaster United States could last more than a year. A manmade electromagnetic pulse (EMP) could happen if terrorists were to explode a nuclear weapon over the continental United States. This would disable the power grid over a wide area by destroying both microelectronic controls and large transformers. Major transmission transformers are not stockpiled and most are manufactured outside the country. Thus, replacing a damaged transformer could take more than a year.

Ideally, the grid would be protected or hardened against these destructive measures, and businesses, universities, and communities would be capable of generating their own emergency power. However, the United States is not yet at this ideal state. Consequently, if the grid is damaged, everyday life would change drastically. If several major locations are involved at the same time, then mutual aid agreements among emergency managers might be difficult to honor and the local situations could become devastating.

Potential Cascading Events

No matter the cause of a grid collapse or failure of parts of the grid, a series of events could follow – a cascade of tragic proportions. Immediately following a power outage,

major emergency generators start automatically and could continue running until fuel is exhausted. However, with a large-scale grid failure, multiple infrastructures, on which refueling depends, would eventually fail, including the financial sector, transportation, oil refineries, as well as law and order. Fuel would quickly become scarce. Even natural gas supplies could become depleted when compressors are driven by electrical power. Within one week, or likely sooner, most backup generators will have exhausted their fuel supplies

Without electricity, both fresh and wastewater treatment plants would fail. People with their own wells could be affected because the wells usually require an electric pump, which could be powered during a power outage by a generator; but eventually the generator will stop without its own fuel source.

Without trucks operating, food distribution would halt. Existing food on shelves would last for a few days at most. Ideally, big grocers would initiate rationing so allocation would be fair and people would not hoard. However, because of just-in-time inventory practices, food is no longer stockpiled in warehouses. The combination of desperate people and just-in-time distribution would quickly exhaust food supplies.

Hospitals and nursing homes would find that, without electricity, water, sanitation, transportation, and other resources, they could not treat patients. Hospitals would shut down. Medical supplies would be in short supply and people would die. People may not have transportation to get to work, so businesses would stop and, with sustained power outages, there may be little work to do.

In addition to the likely consequences discussed above, unpredictable events also may occur. To better prepare for the unexpected, individuals, organizations, and agencies should determine what is controllable and take action now to mitigate the consequences.

Promoting Individual Actions

Emergency managers often promote personal and family preparedness as a three-day supply of water, food, and medications. In reality, three-week or even three-month supplies may be needed. Although individuals and families should be prepared at home, at work, and even in their cars, only a small portion of the population is likely to be adequately prepared when an incident occurs. It is unclear how many could survive for a long period if they were away from their home. As such, emergency managers should inform the public about potential scenarios, so they can be better prepared:

- *Without power, phone systems and the Internet eventually would stop functioning.* Ways to communicate with family members should be discussed ahead of time. It is important to have a family plan for where to meet and how to communicate without electronic means. With no television or radio, the feeling of isolation and the lack of information would be prevalent. Going to the local fire station might be a place to learn what is happening.

- *Without power, there could be a shortage of water supplies.* Having a generator at home would help with the immediate aftermath of a power failure. Hot-water storage tanks could help in the short run. Rain barrels on gutter downspouts also could provide water in areas with ample rain. However, incredibly, some states have outlawed the use of rain barrels, claiming the rain belongs to the government.

"Major transmission transformers are not stockpiled and most are manufactured outside the country. Thus, replacing a damaged transformer could take more than a year."

In addition, emergency managers could share information with the public about alternative sources of power to assist during long-term power outages. One suggestion is installing solar panels on homes or on poles in backyards. However, since most people who install solar panels do so to cut their power bills, the power generated from the solar panels often goes to the grid. When the grid is not functioning, the solar panels do not provide power to the homes.

This safety mechanism prevents electrical power company crews from being electrocuted by the power coming from the panels while they work to make the grid operational again. To power the home during an outage, homeowners would need to have a switch so they can isolate their solar panels and have the power go to a backup battery. Such switches and batteries, though commonly available, are not commonly used; however, if demand rises, so would the prevalence and affordability of these devices.

Communities Banding Together

Although businesses may be able to function temporarily following a power-grid failure, workers eventually would need to return home to their families. Consequently, businesses including grocery stores and food markets may cease to function.

In urban areas where growing one's own food is not practical, there are some community options that emergency managers could suggest. Victory gardens, where communities garden a plot together, might be a partial solution. Some building owners have the ability to establish gardens on their roofs, which would provide security from renegades. Having an assured source of even a small amount of food could increase survivability. One concern, though, is that well-prepared citizens who do have food would become targets for attack to obtain the food they have. The way to protect against such situations is for neighbors to band together.

Neighborhood groups could consist of a few blocks or an entire county. Volunteer organizations such as Volunteers Active in Disasters (VOAD), Boy or Girl Scout groups, faith-based organizations, and book clubs, also could be considered "neighborhoods." Working together and pooling resources may keep everyone alive longer; there is "safety in numbers."

Before a disaster occurs, these neighborhoods should: (a) share ideas and determine what to do in case of a disaster; (b) recognize each other's strength and needs; and (c) discuss major issues, such as the failure of electrical power for an extended period. For example, the public-private partnership organization, Community Emergency Response Network Inc. in Howard County, Maryland, has regular meetings to discuss various emergencies and related steps toward preparedness. Citizen Corps and Community Emergency Response Teams (CERT) operate in a variety of ways within many communities. Relationships built ahead of time will strengthen the entire fabric of society. After an emergency is not the time to share business cards.

To strengthen communities, it is important to build relationships, share information, and know where to turn in times of a disaster. By helping neighborhoods expand their relationship circles, emergency managers can better serve those with critical needs and create communities that are more resilient.

Mary Lasky, a Certified Business Continuity Professional (CBCP), serves as the program manager for business continuity planning for the Johns Hopkins University Applied Physics Laboratory (JHU/APL), where she coordinated the APL Incident Command System Team. She also as a member of: InfraGard, where she is on the executive committee for the InfraGard EMP-SIG; and the Federal Emergency Management Agency's Nuclear-Radiation Communications Working Group. In Howard County, Maryland, she serves as: president of the Community Emergency Response Network Inc. (CERN); president of the board of directors of Grassroots Crisis Intervention Center; and Finance Committee member for Leadership Howard County and is co-chair of the Steering Committee for the Leadership Premier Program. For many years, she has been on the adjunct faculty of the Johns Hopkins University Whiting School of Engineering. She is the immediate past president of the Central Maryland Chapter of the Association of Contingency Planners (ACP) and has held a variety of supervisory positions in information technology and in business services. Her consulting work has included helping nonprofit organizations create and implement their business continuity plans.

Washington, D.C. – Fail Gracefully, Recover Quickly

By Rodrigo (Roddy) Moscoso

Since the issuance of Presidential Policy Directive 8 in 2011, which established the objective of strengthening the security and resilience of the United States across five core mission areas, the nation's city leaders have been developing and implementing plans to improve their ability to protect and respond to a variety of manmade and natural disasters. Unfortunately, since 2011, homeland security and emergency management personnel have had many examples of critical infrastructure failures, including: the earthquake and tsunami on 11 March 2011 that resulted in Japan's Fukushima Daiichi nuclear power plant meltdown; the North American derecho in the summer of 2012; and Hurricane Sandy, which made landfall in the northeastern United States in October 2012. The increased focus on preparedness and resilience planning coupled with an emphasis on continuous learning from critical infrastructure failures elsewhere is enabling emergency managers to improve their ability to plan for, and respond to, major incidents.

Hazard Identification & Lessons Learned From Other Cities

"First, we want to ensure that we fail gracefully," said Christopher Geldart, director of the District of Columbia's Homeland Security and Emergency Management Agency (HSEMA), in a telephone interview on 19 September 2014. "You can never prevent a failure from happening, but the key to prevention and protection is to take steps to ensure that you fail gracefully and also do the work necessary to shorten the recovery time as much as possible," he added. Recently, D.C. HSEMA took the Federal National Preparedness Framework and created a family of plans that focuses on the five core mission areas, the first of which is Prevention and Protection.

As part of its planning effort, HSEMA identified 18 hazards that are unique to Washington, D.C., and reviewed all previous plans and efforts to improve resilience in these areas. This included looking at ways to harden physical infrastructure and to improve supply chains that aid and shorten the recovery process. Based on the implementation of these plans, HSEMA officials expect only partial power outages with faster recovery times rather than a citywide power failure during a major storm.

Maintaining electrical power continues to be a core focus for the city, as it does for most emergency managers, service agencies, and lifesaving organizations. Hurricane Sandy demonstrated that even well planned and implemented resilience efforts could fail dramatically with significant effects on the public. In New York City, two major hospitals – Langone Medical Center and Bellevue Hospital Center – had to evacuate after their backup generator systems failed. Although the generators were located on upper floors, the pumps and diesel tanks supplying fuel to the generators were located in "flood-protected areas" of both hospitals' basements. Unfortunately, these protections failed and the generators had no fuel to operate.

IDCE

International Disaster Conference & Expo

FEBRUARY 10-12, 2015 NEW ORLEANS, LOUISIANA

FEATURED SPEAKER

Former CIA Analyst

Nada Bakos

UNITING PUBLIC & PRIVATE SECTOR PROFESSIONALS FROM AROUND THE WORLD

CLICK THIS AD FOR MORE INFORMATION

IDCEXPO.NET

At Fukushima Daiichi, 12 of 13 backup generators failed following the tsunami. Although the earthquake itself did not significantly damage the plant, the two large tsunami waves submerged the emergency generators, seawater pumps, and batteries located in the basement of the plant, rendering them inoperative. In short, the lack of power to run the water-cooling system and monitor the reactor itself was directly responsible for the nuclear reactor meltdown.

Location-Specific Considerations

The topography of Washington, D.C., makes it a challenge to provide water to higher elevations while, at the same time, removing the water from low-lying areas. For Geldart, this was the biggest surprise encountered when developing the city's new preparedness plans. "Water is a huge issue, and it is a much more complex system than I originally imagined. As soon as you get backpressure in the system, people must boil water in their homes, and schools and businesses close, including government buildings – and you don't want to tell the White House that they need to boil water," he said.

Power, then becomes the critical element to water delivery as well as to water treatment. "We have two [power] feeders into our Blue Plains water treatment plant but, if we do lose all power there, we have the choice of either dumping raw sewage into the Potomac [River] or backflow the entire city," Geldart added. This scenario actually occurred in May 2006, when 17 million gallons of raw sewage spilled into the Potomac River. Geldart noted that Washington, D.C., now has portable generators staged for responding to such situations.

During the development of the new preparedness plans, HSEMA created separate task forces to focus on key areas, including the ability to quickly deploy emergency power generation across the city. HSEMA is now working on a 10-year plan of investing in water infrastructure enhancements that will better harden the system and help it to fail more "gracefully."

Neighboring Infrastructures & Private Sector Cooperation

On the other side of the Potomac River in Virginia, the issue of power resilience also is at the forefront of preparedness planning. Dominion Power, Virginia's largest power utility, announced this year that it had embarked on a legislatively approved plan to bury approximately 4,000 miles of electrical distribution lines underground in areas where above-ground lines are most susceptible to storms. During the 2012 "derecho" storm, more than one million people lost power in Virginia. Although burying power lines will not guarantee power to residents during a major storm, Dominion anticipates that restoration time will be significantly shorter when outages do occur.

However, funding remains an issue for the plan. In 2005, a Virginia State Corporation Commission estimated the cost of burying all 58,000 miles of Dominion's power lines at $83.3 billion. The current plan calls for moving 350 miles of power lines each year for the next 10-12 years at a cost of $175 million annually. Funding for the plan will come from customer rate adjustments or riders that still await approval by the State Corporation Commission.

Another important element in disaster preparedness and service restoration, particularly electrical services, involves the active cooperation with the private sector. "When Craig Fugate was director of Florida's Division of Emergency Management, he called it the 'Waffle House index'," noted Waffle House spokesman, Pat Warner, vice president of culture, in a telephone interview on 24 September 2014. "Since Waffle House is a 24 by 7 by 365 operation, the status of our open locations was a good measure of power availability after a storm, which we have been sharing with emergency management agencies across the southeast for many years," he added. The Waffle House Corporation has worked to restore power to their locations after major storms as quickly as possible, and has implemented a rapid response effort, including the delivery of generators and fuel to the hardest hit locations. "For many people, [Waffle House] is the first hot meal they have in the aftermath of a hurricane," said Warner.

The information between Waffle House and other businesses and Florida emergency management agencies increased over time, including regular status updates from them and other businesses. When Fugate was appointed as Administrator of the Federal Emergency Management Agency (FEMA) in 2009, information exchange with the private sector increased, resulting in the establishment of the National Business Emergency Operations Center (NBEOC), which "serves as FEMA's clearinghouse for two-way information sharing between public and private sector stakeholders in preparing for, responding to, and recovering from disasters."

For the Waffle House, which has its own emergency operations center in Atlanta, Georgia, the focus now is to use social media to "push" information to customers about which locations are open in order to manage the flow of people. The company also has developed a new "Waffle House on Wheels," which can go to the hardest hit or underserved locations following a major storm.

Emergency managers always must be ready for any challenge presented to them, particularly those that former Defense Secretary Donald Rumsfeld called, "the unknown, unknowns." However, mitigating strategies, including the development of thoughtful and comprehensive preparedness and resilience plans, can help to reduce the severity and impact of even an "unknown" event. Coupled with a strategy of collaboration with the private sector, a more holistic view can be achieved by emergency managers, which is the first, and most important, step in addressing the problem at hand, and which also serves as the basis for future preparedness planning.

Rodrigo (Roddy) Moscoso currently serves as executive director of the Capital Wireless Information Net (CapWIN) Program at the University of Maryland, which provides software and mission-critical data access services to first responders in and across dozens of jurisdictions, disciplines, and levels of government. Formerly with IBM Business Consulting Services, he has more than 20 years of experience supporting large-scale implementation projects for information technology, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.

"Old-School" Response to Medical Emergencies

By Joseph Cahill

This current emergency medical services (EMS) dispatch and response process has evolved significantly over the past few decades. A dispatcher records the details of a 911 call in a web-based application. That information flows through a computer terminal into an ambulance. The unit responds using directions from a global positioning system unit on the vehicle's dash. Emergency medical technicians use a wireless tablet to complete an ambulance report. Finally, the report is uploaded to a secure cloud over a virtual private network, where hospital staff as well as EMS headquarters can access the data in real time.

Loss of Connectivity Threats

As EMS personnel become more dependent on technology for daily tasks, the system still must be able to operate when electronic data components fail. System complexities – coupled with the potential for engineered failures as part of a cyberattack or as an element in a broader attack strategy – increase the likelihood that a failure eventually will occur. In addition, a growing dependence on cashless transactions means that businesses essentially close when connectivity to the banking system is disrupted and companies are unable to process credit or debit payments.

> ***"When a system failure occurs, command needs to be ready to activate the plans and lead personnel through operations, which likely will be unfamiliar and tedious to a generation acclimated to real-time data and technological tools."***

One way to reduce the impact of power outages and technology failures is to develop a "technology crash cart" process similar to manual machines still used in many restaurant operations. When banks first introduced credit cards, businesses created impressions of the card using carbon paper – which is one of the reasons numbers and names on the card are embossed rather than printed – and presented them to the credit card company in exchange for payment. By assembling a technology crash cart with carbon paper forms and the machine used to take the impressions, businesses can continue to serve customers who have no cash. However, because there would be no system to validate the card, the businesses would have to accept a degraded system, but at least would be able to continue operations.

Traditional Nonautomated Methods

The first step for building an EMS technology crash cart would be to perform a workspace audit (see "Armageddon Plan" article from 19 October 2005), which would include:

- Noting every piece of technology used during the course of an agency's business; and
- Assembling an institutional memory team, including staff experienced enough to answer the question, "How did we used to do that?"

In New York City's EMS in the 1980s, dispatch recorded details of 911 calls on index cards. That information was shared over the radio and the ambulance crew wrote it down. The unit responded using a printed map. An emergency medical technician completed an ambulance report with pen and paper. A copy of that report was provided to the hospital staff and another sent to headquarters through interoffice mail. EMS could use this "old-school" way of doing business again when current technologies fail.

Agencies should tailor a technology crash cart for each critical mission area:

- *Ambulances* – The ambulance should have a box tucked away with a map, a pad of blank paper, pens, and paper ambulance reports.
- *Dispatch* – Dispatchers should have forms for recording the call information and tracking unit progress throughout the call cycle.

Global tools such as a board for tracking unit status for the entire system also should be available. All work areas require a written and trained plan with procedural instructions because, of course, a plan no one has been trained on does not exist.

Finally, when a system failure occurs, command needs to be ready to activate the plans and lead personnel through operations, which likely will be unfamiliar and tedious to a generation acclimated to real-time data and technological tools. As modern EMS technology continues to advance, there is still a need to prepare for reintroduction of traditional EMS practices.

Joseph Cahill is the director of medicolegal investigations for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as citywide advanced life support (ALS) coordinator for the FDNY – Bureau of EMS. Before that, he was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. He also served on the faculty of the Westchester County Community College's paramedic program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.