



DAEDALUS
FOCUS

GRID ACT IMPACT

ISSUE DATE: 1 NOVEMBER 2010

GRID ACT IMPACT: RESULTS OF NEW CONSENSUS WARNING OF A YEAR-LONG BLACKOUT

ABOUT THE AUTHOR

Charles L. Manto

As CEO of Instant Access Networks, LLC (www.stop-EMP.com) Mr. Manto has developed a civilian critical infrastructure EMP rating system, developed EMP protected rooms to protect critical infrastructure such as communications and power systems from EMP, and won four state/university R&D grants for the development of EMP-safe microgrids and renewable energy. He led operations for a broadband CLEC, a computer industry start-up, a county economic development corporation and was the lead consultant for broadband deployment strategies for 12 MD counties. He ran a venture capital due-diligence service for Gartner Group and developed international projects for industrial defence conversion in the former Soviet Union under the Nunn-Lugar Act. He won five patents and has others pending. He graduated from the University of IL with an MA in 1979.

Copyright and Disclaimer

This report is © Entity X, 2010. Where it has not been possible to locate the original copyright owner of photographs and other non Entity X content we tender our apologies to any owner whose rights may have been unwittingly infringed. The links to external websites included in this report are for ease of reference only and Entity X takes no responsibility for the content presented.

Geomagnetic storm charts by permission of John Kappenman

GRID ACT IMPACT: RESULTS OF NEW CONSENSUS WARNING OF A YEAR-LONG BLACKOUT

Report Overview

Space-weather experts have changed their prediction of the effects of the 100-year solar storm from likely being a weeklong blackout across the East Coast through Chicago to one that could easily be yearlong, with restoration taking four–ten years. This announcement prompted a tabletop exercise in March 2010, sponsored by NOAA in Colorado, followed by an **emergency management bulletin** nationwide. The change in forecast was prompted by the analysis reported in recent studies such as the National Academy of Sciences 2008 **Severe Space Weather Events – Understanding Societal and Economic Impacts** and the final US EMP Commission reports in 2008 (www.empcommission.org). These spawned support for a subsequent NERC **report on high-impact low-frequency events** and a set of FERC reports published in January 2010: **Electromagnetic Pulse – Effects on the US Power Grid**.

As a result, provisions to address these issues were included in the **Grid Act (HB5026)** passed by unanimous consent in the US House of Representatives on 9 June 2010. If it passes the Senate and becomes law, it would empower FERC to take emergency actions to protect regional grids from cyber threats such as these. Passage in the House already demonstrates a growth of consensus from communities of experts to policy makers that should cause mission-critical infrastructure owners and operators to consider electromagnetic pulse (EMP) threats far more seriously than before. Both natural and manmade EMP threats have already been recommended to be included in all-hazards business continuity planning for years in documents such as the fire code NFPA 1600. The significance of this bill goes beyond that there is agreement, to recognising that these threats cannot remain ignored.

There is also agreement that these events are qualitatively different in that the duration and geographic spread of the effects are far greater – spanning months and geographic regions as large as continents. In the case of a severe solar storm, it would most likely be a global event. Manmade EMP can disrupt or damage interoperable communications systems required by first responders and controls needed by infrastructure, and those technical systems that do survive would eventually stop working once their power systems failed from either manmade or natural EMP. Simultaneous EMP hits on interdependent technology and infrastructure will create massive simultaneous cascading failures.

This report will provide an overview of the bill, the threat, its economic impact and the action that corporate or government security experts need to take.

SUMMARY

- Worst-case natural or manmade EMP events can damage 300 or so of the largest transformers that take at least a year to make
- Economic studies project \$multi-trillion economic impacts
- Duration and geographic reach of impact requires broader recovery planning participation as recommended by the fire code for business continuity, NFPA 1600
- First civilian planning exercises began August 2009, more planned for 2010/11
- Worst-case scenario without preparation is a sovereignty-ending event
- Protection of the grid is relatively economical but will take up to five years
- Development of protected local power generation is urgent and profitable

The New Opinion about Impact and Likelihood

The changes in the consensus opinion among experts are that:

1. Solar storms can have ten times greater impact than expected
2. Manmade EMP is more likely than previously thought
3. Disasters could last months and threaten US sovereignty

It has been long understood that the likelihood of a severe solar storm is 100% over time and that there have been such occurrences in the recent past prior to the establishment of modern electric grids. What is new is that the projected impact is much closer to that of a manmade high-altitude nuclear EMP (HEMP) attack.

The resulting ground-induced currents would be expected to damage hundreds of high-voltage transformers that take over a year to build, creating blackouts over large regions that could last a year or longer. Power would be rationed during the four-ten years it would take to bring service back to pre-incident levels. The manmade version of the threat is a broadband electromagnetic assault differentiated by the addition of quicker pulses; the quickest, named E-1, are in the nanosecond range.

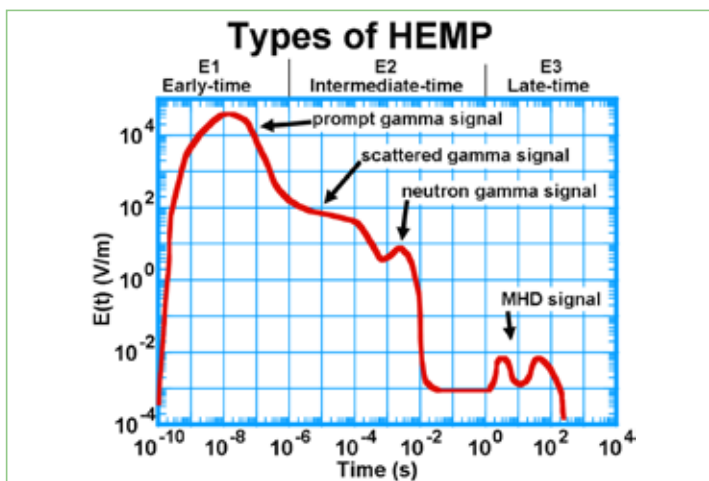


Fig. 1: This chart, 'Various Parts of a Generic HEMP Signal' can be found on p. 2-1 of the 2010 FERC report on EMP, Meta-R-324, *High-Frequency Protection Concepts for the Electric Power Grid* by William Radasky and Edward Savage by Metatech Corporation

Coincidentally, smaller intentional electromagnetic interference (IEMI) weapons can produce the fast pulses but have a shorter range and lack the ability to create a meaningful ground-induced current created either by the slower pulse of a high-altitude nuclear burst (named E-3) or by a geomagnetic storm. However, they can still disrupt or damage controls that lead to other serious problems. The differences between these attack modes and their consequences are explained in detail in the FERC reports mentioned above.

Numerous states' militaries have highlighted the importance of incorporating IEMI weapons in asymmetric or combined-arms operations. China and Russian military organizations have published papers describing how IEMI weapons could be used in attacks against Western militaries to reduce their technological advantages. More importantly, there are numerous examples of criminals and terrorists using, or attempting to use, IEMI weapons as part of terrorist attacks or crimes. As such, IEMI weapons, as part of an overall cyber-operation by a hostile state or organization, are a likely scenario.

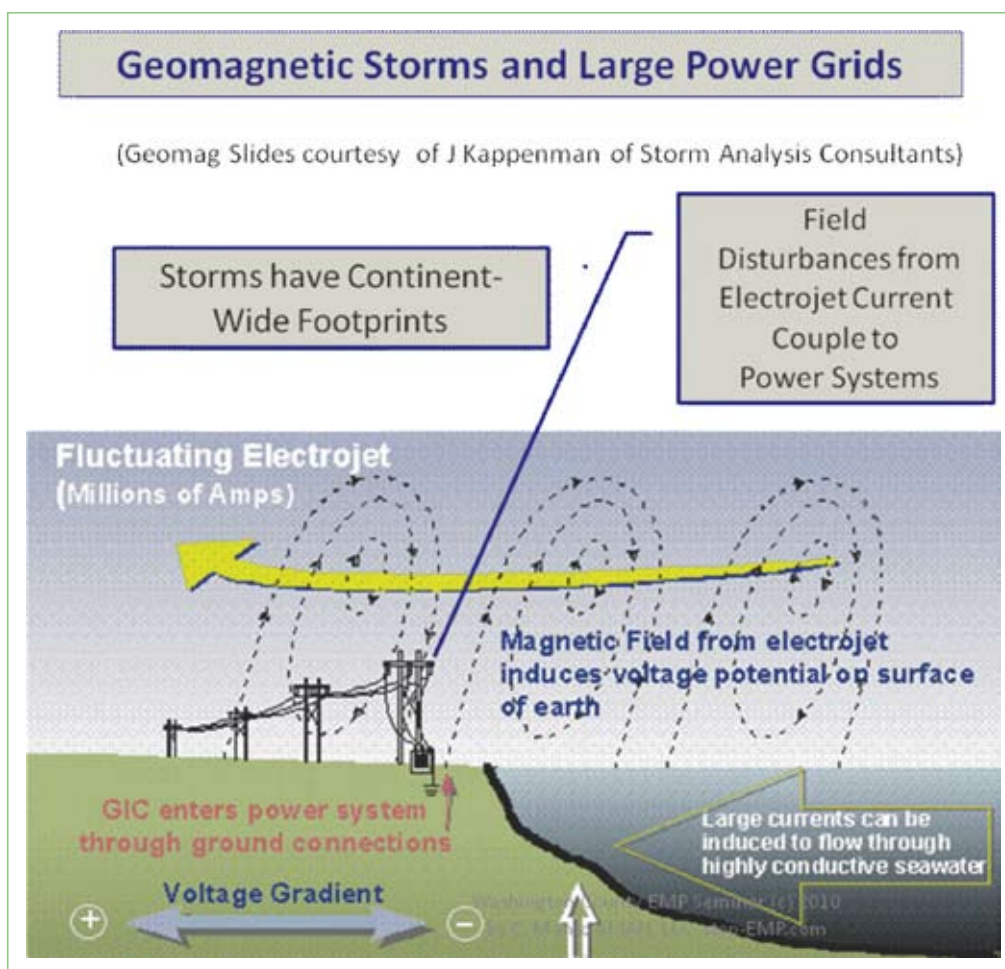


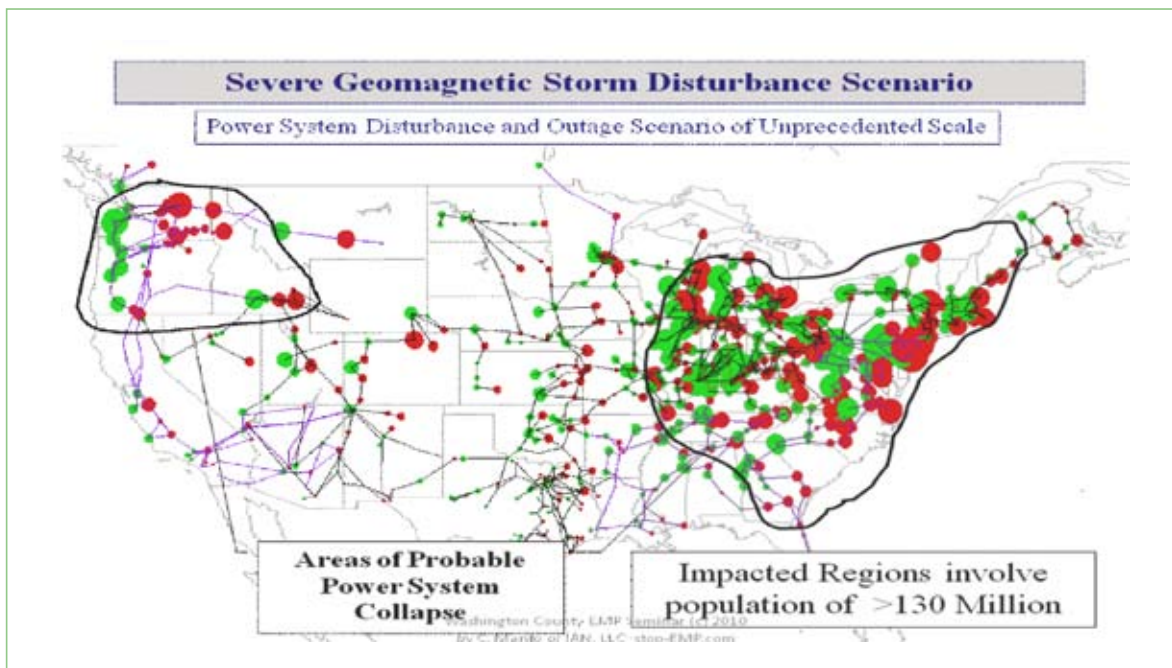
Fig: 2

While critical infrastructure is unprotected, economic assessment has shown that manmade EMP is one of the least expensive ways to cause the most economic damage to the country and this increases the probability that some adversaries would want to make an attempt. A small nuclear payload that can be delivered anywhere between 80 miles or higher from an off-shore freighter could create a regional disaster with **\$T economic impacts** with possibly no forensic evidence. This and similar delivery techniques could make attribution impossible or irrelevant, rendering deterrence less potent (see the US Congressional EMP reports mentioned above). The manmade EMP capabilities of a perpetrator are more dependent on their **cash and project management skills** than their own subject-matter expertise or technology, which can be bought or borrowed (black market scud class missiles can be obtained for between US\$¼ million and US\$1 million and the new cargo container systems [class K, which carries four missiles] from a Russian provider were recently reported as being offered new for US\$10 million).

The Political Sea Change of the Grid Act Impacting Security Policy

Security professionals and policy makers should appreciate the sea change in attitudes towards EMP because of the issues underlying the Grid Act. Previously, there were some with a reasonably good technical understanding of EMP who would downplay its seriousness because although they recognised that high-altitude nuclear EMP can cause severe infrastructure and economic damage to the extent that tens of millions could perish, they also believed that creating a missile defence system would not only be expensive but also provoke an even likelier response that could cause equal or greater damage. So, they would prefer to not bring up the EMP issue for fear that someone would use it as a Trojan horse to sneak in the need for a missile defence system.

The missile defence issue is a complicated one in itself but can be argued very differently and in a way that could minimize inherent risks. But, regardless of opinions towards missile defence, all would acknowledge that creating more robust and hardened systems makes sense. However, now that it is understood that an extreme solar storm could be far more devastating and much more along the lines of an intentional EMP event, the political issues have changed. No one can be accused of wanting a missile system to shoot down solar storms. So, it is much safer politically to talk about the combined threat of an extreme solar storm that is 100% likely to happen and the man-made EMP threat that grows in likelihood in proportion to our vulnerability. For these reasons, the Grid Act that includes geomagnetic storms, nuclear EMP and smaller intentional electromagnetic interference (IEMI) weapons has received overwhelming bipartisan support in the House. In other words, EMP is now a politically correct topic. This has the added benefit of providing security professionals and policy makers the opportunity to visit a class of security threat and disaster that is regional or continental in scope, lasting months and threatening continuity of government.



Grid Act: Directs FERC to require any owner, user, or operator of the bulk-power system in the United States to implement measures necessary to protect the system against specified vulnerabilities.

Mitigation Benefits

Despite the overwhelming nature of this problem and relatively wholesale vulnerability of civilian infrastructure as brought out in the EMP Commission reports through 2008 and the recent ones just released by FERC, there are good news elements:

- Engineering methods to protect against manmade nuclear EMP can also protect against the combination of geomagnetic storms and IEMI
- Protecting as much as 10% of the critical infrastructure can eliminate as much as 30–40% of the economic damage
- Creating solutions through **protected local power** production can create peak load management savings and other economic benefits
- Assessments can be integrated into crisis management plans that meet fiduciary responsibilities and lower insurance costs

CRS Summary of The Grid Act (HB 5026): Directs the Secretary to establish a program to develop technical expertise in the protection of systems for the generation, transmission, and distribution of electric energy against either geomagnetic storms or malicious acts using electronic communications or electromagnetic pulse.

The Late Start in Emergency Planning Demonstrates the Need for Triage

The first civilian federal emergency management tabletop exercise for a long duration blackout was reported by NOAA in February 2010. The first local government EMP tabletop exercise was completed in Alma, NY, in August 2009 and a second in Carlisle, PA, on 26 October 2010. Others are planned for eastern NY and western MD in the coming months. Confronting these threats will be overwhelming and prompt most to deny or minimize them. Triage will be necessary from planning through mitigation and recovery stages to encourage action. Fortunately, there are some measures that are quick and inexpensive that can create some benefits and reduce risk. There are other measures that will cost time and financial resources but can be prioritized and incrementally implemented.

Infrastructure owners and managers can use a civilian EMP rating structure that will quickly sort out the most important and vulnerable assets, and apply the amount of protection to provide the best value for the least expense. In this way, an organization can immediately enhance its crisis management plan and take measures to protect assets and capabilities while recruiting the resources from suppliers and the community at large to further improve recovery times. (The author of this report has organized multiple companies to provide the first such assessment and use of a civilian infrastructure rating structure for a 500,000 Sq Ft food production facility and its utilities suppliers.)

(An example **civilian infrastructure assessment and an industry reference letter**; see the upcoming full report on threats, mitigation techniques and an assessment approach that maximizes protection at the least cost as soon as possible.)

Sample Scenario Considerations

Close-Range Intentional Electro-Magnetic Interference (IEMI) Attacks

These weapons come in different sizes and at different costs with a variety of capabilities. A **government report** out of Dahlgren provided an overview of accidental and intentional EM events from sources as small as a cell phone to as large as a radar system. Governments around the world are funding new EM weapons while private sector firms are continuing to announce new weapons. Plans that include EMP protection should be continually updated to take these changes into consideration. Some quick action that can be taken is to review

physical perimeter security and access measures to make sure security processes will prevent these shorter range weapons from coming too close to sensitive controls and equipment that would be unprotected. Valuable technical infrastructure that is chosen to be protected from EMP will also be protected from IEMI threats.

Distinguishing between EMP Attacks and Geomagnetic Storms

EMP attacks create fast-rise time pulses through the atmosphere in the nanosecond range that can affect electronics and controls whether or not they are connected to long conductors such as power or communication lines. They are depicted in Fig. 1 above as E-1 pulses. Depending on the size of the EMP event, it may also have a sizeable E-3 pulse that creates ground-induced currents similar to an extreme solar storm.

Extreme storms will not create the fast-rise time pulse but can disrupt and damage transformers along with anything connected to these grounded long-lines. While an intentional EMP attack should make it obvious that other attacks of a similar or different sort might follow, an extreme solar storm event might make the country so vulnerable that it could invite subsequent attacks (or “offers of help”) by those wishing to take advantage of the resulting weakness. In addition to follow-on attacks, the cascading effects of a long-term blackout will have serious consequences for communications, food production and distribution, water supplies and sanitation, and ecological disasters. For example, spent-fuel containment facilities are no longer able to cool water in containment facilities and toxic nuclear waste would be air-borne from any of the hundred or so nuclear plants that would be affected. Each of these scenarios points out the need for crisis management and business continuity that extends beyond your organization to your supply chain and community.

Next Steps

- 1. Assess EMP requirements of your own core entity and supply chain**
- 2. Begin protected local power generation capability (impact to local power suppliers and users)**
- 3. Conduct EMP triage**

IMPLICATIONS

Security professionals: Review all-hazards business continuity plans and take steps to ensure that these vulnerabilities are addressed. Undertake EMP assessments to see what can be protected quickly and inexpensively and how to make wise investments with scarce resources. See if key suppliers and the local community are also protected since their failures to protect themselves can create protracted loss of resources and staff in your organization that could be measured in months. Facilitate discussions with senior executives to discover resources required internally and from business partners. Be attentive to community action that can attract outside resources to enhance your own abilities to prepare. Don't wait for the federal government or large utilities to take action, but begin local mitigation efforts such as the creation of protected local power production and communication facilities. Develop 'work-around' measures in light of infrastructure that you can't control or protect. Discover local food reserves and provide special protection for them so that your staff and their families can be fed.

Policy makers: Foster awareness and mitigation action from the local level up. Help foster local resilience and independence and minimize dependence on outside help while trying to foster cooperation and mutual aid capabilities. While infrastructure is still vulnerable, consider ways to develop yearlong food supplies and spare parts inventories for critical infrastructure. Begin by providing two-week-long food and water capabilities in your own facilities for 'shelter-in-place' scenarios such as a dirty bomb and then work through other hazards that would compel greater local resilience. Many infrastructure leaders that are not included in emergency planning for shorter duration disasters, such as food producers, should be recruited to participate in emergency planning. Economic development entities should consider ways to foster investment in local critical infrastructure that can help create jobs and new services while providing community sustainability. Use EMP protection as an opportunity to jump-start renewable energy markets, create energy and food security and develop stronger local economies and relationships.

Intelligence professionals: Foster relationships through groups such as Infragard, comprised of private sector infrastructure businesses under nondisclosure agreements with each other and the FBI. They can support critical infrastructure protection efforts and more thorough connection of local communities that can provide assistance to each other in times of prolonged disaster. This will also provide avenues of intelligence input from those looking to exploit infrastructure weaknesses in times of disruption. Keep aware of those waiting for 'zero hour' type moments that may interpret an EMP event as the trigger they need to do more damage on their own. Also, be aware of local gangs that can use their large number of armed followers to take control of critical infrastructure and supplies when law enforcement and National Guard elements are stretched.

THE DAEDALUS REPORT SERIES

The Entity X Daedalus series of reports informs clients of emerging trends and developments in the areas of cyber threats, net-centric security and electronic attack, authored by respected experts on the subject. The monthly *Daedalus Report* provides comprehensive analysis of emerging issues and incorporates an annex generated by our partners Lexis Nexis Analytics which provides a summary of the world's press articles from over 68,000 sources. *Daedalus Focus* reports are issued as developments occur and provide in-depth technical detail, case studies, or code samples; subscribers can also request subjects for Entity X to focus on. Our *Daedalus Special* reports, for certain government clients only, highlight sensitive matters relating to exploitation opportunities.

ABOUT ENTITY X

Electronic warfare was formerly an issue for the military on the battlefield, but now it affects every aspect of our lives, our work and our government. At Entity X Inc we have recognized the growing significance of cyber threats and net-centric warfare. We're a team of highly experienced IT professionals working at the cutting edge of technology. Unlike conventional IT security firms we seek to develop in our clients a greater and deeper understanding of the range of disparate yet rapidly evolving threats that governments, businesses and individuals face. Entity X Inc produces the Daedalus report series to inform and brief our clients and we also provide consultancy and training in this specialized but increasingly significant field.

Contact

info@entity-x.com

Contributors

Charles L. Manto,
CEO, Instant Access Networks, LLC