ENERGY LAW JOURNAL

Volume 34, No. 1 2013

VULNERABILITY OF NATIONAL POWER GRIDS TO ELECTROMAGNETIC THREATS: DOMESTIC AND INTERNATIONAL PERSPECTIVES

*Avi Schnurr**

Synopsis: Rapid evolution of the national power grid and the bulk power system in size, scope, technology, and structural complexity has been accompanied by a substantial increase in sensitivity to electromagnetic disturbances, both natural and malicious. This increasing sensitivity will be further exacerbated by extensive grid renovation in the next ten to twenty years. When combined with new evidence of infrequent but Severe Space Weather events and with rising concerns from international political instabilities and proliferation trends, this expanding sensitivity has introduced a new dimension of risk to power grid reliability and security. This article, following a technical and historical summary, reviews some of the fundamental electromagnetic threat (e-threat) issues and complexities being considered by policy makers and regulators, and summarizes grid hardening options. This article explores unique challenges associated with an issue which affects many government functions, highlighting perspectives expressed by different agencies in the United States and allied governments. The article concludes with a short menu of regulatory considerations and industry-initiative measures that could help address e-threat concerns.

* M.Sc., physics, the University of California, Los Angeles. Avi Schnurr is Coordinator of the International Electric Infrastructure Security Summit Series, and CEO and President of the Electric Infrastructure Security (EIS) Council. He has reviewed electromagnetic threats and power grid protection options for the White House Office of Science and Technology Policy, Congress, the Federal Energy Regulatory Commission, the Department of Energy, the Department of Defense, National Security Council staff, and other U.S. government agencies, and has briefed cabinet members, chief scientists, and other senior officials in allied governments and international governmental bodies.

I. INTRODUCTION

A. Overview

1. The Critical Role of Power Grids in Modern Societies

Of all the basic utilities and infrastructures essential for the functioning of modern society, the power grid system has become, by far, the most critical.

Throughout history, societies depended on co-located, independent producers for their most fundamental resources, and in the early days of electric power the situation was no different. Today, after nearly a century of living with an integrated national power grid delivering reliable, easily available electric power, our homes, factories, social institutions, and the basic tools of commerce

cannot survive without it. In the modern world, national growth is paced by the rate of cost effective development of the power grid.

This revolutionary change has led to unprecedented growth in the nation's integrated electric grid. Over the last few decades the electricity sector has experienced massive growth while taking advantage of new technology to limit costs, as power companies systematically replaced armies of electrical engineers with Supervisory Control and Data Acquisition (SCADA)[1] computer control systems; planned and implemented smart equipment innovation at generating stations, power line substations, and homes; and moved power over continental distances using ever higher voltage Extra High Voltage (EHV) transformers and longer transmission lines.[2] Today, it is fair to view the nation as spanned by three, enormous, highly organic power systems with power generation and use typically separated by huge distances, made possible by a grid of long, high voltage transmission lines overlaid by layers of ubiquitous computer control networks.

2. Protecting the Power Grids: The Role of Regulatory Institutions

In developed countries, the importance of the nationwide, organic power grid, and the consequent potential for highly leveraged negative impact associated with losses of essential utilities and services, almost invariably results in regulatory structures which attempt to manage such risks. Bulk power systems, broadly recognized as the foundation for most or all other essential utilities and services, are subject to such regulatory control.

In the United States this control is implemented at both the federal and state levels. The Federal Energy Regulatory Commission (FERC) has authority to impose mandatory reliability standards, working through the North American Electric Reliability Corporation (NERC), the Congressionally-mandated Electric Reliability Organization (ERO), which develops and enforces compliance standards and applies penalties.[3] The individual states then maintain their own regulatory utility commissions – governing bodies that regulate the rates and services of local power companies.[4]

3. Unique Concerns with Emerging Electromagnetic Threats

While regulators and other energy sector stakeholders grapple with a wide range of hazards, they are beginning to find that emerging electromagnetic

1. REPORT OF THE COMMISSION TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, CRITICAL NAT'L INFRASTRUCTURES 1-2 (Apr. 2008) [hereinafter EMP COMM'N 2008 REPORT], *available at* http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.

2. PATRICIA HOFFMAN & WILLIAM BRYAN, OFFICE OF ELEC. DELIVERY AND ENERGY RELIABILITY, LARGE POWER TRANSFORMERS AND THE U.S. ELECTRIC GRID 18 (June 2012), *available at* http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.

3. *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 F.E.R.C. ¶ 61,062 (July 20, 2006); *see also FERC & NERC*, BWISE, http://www.bwise.com/grc-challenges/regulatory-compliance/ferc-and-nerc (last visited Feb. 24, 2013).

4. *See generally* NAT'L ASSOC. OF REGULATORY UTIL. COMM'RS, http://www.naruc.org/ (last visited Feb. 24, 2013).

threats are almost unique among the many concerns they address. As we will see below, electromagnetic threats (e-threats) are classified as low frequency events with the potential for serious or catastrophic damage affecting huge regions.[5] These characteristics tend to make e-threats a natural and important subject for both government and corporate action.

Paradoxically however, these same features also put this threat outside normal management processes. Both government agencies and large corporations typically use many experiences with a crisis to define its impact, develop mitigation measures, and build support for their implementation. With e-threats, this gradual learning and protection process does not work. As we will see below, projected impacts range from an extended subcontinental blackout to a crisis in societal continuity. An unprepared nation experiencing its "first" severe electromagnetic event may have no opportunity for gradual recovery.

4. Adapting Management Tools to Address Emerging Threats

If typical government and corporate hazard management processes are poorly suited to this serious, emerging hazard, finding ways to adapt and successfully use these tools become urgent priorities. And since both automated hardware protection and operational procedures are now or will soon be available, this has become both relevant and timely. As effective protection measures become available, the scope, speed, and mandating authority for test and implementation of such measures become important questions.

Given the urgency, this subject invites well-informed dialogue on the balanced roles of regulatory control and commercial sector independent initiative, and on developing corporate and government processes that can begin resolving this grave, emerging concern.

B. Organic Risks to the National Power Grid

Generally speaking, evolving architectures and technologies have done well in meeting the challenge of society's growing demand for reliable and cost effective power. However in recent years, regional blackouts from a variety of natural disasters have sensitized government agencies, regulators, power companies, customers, and other stakeholders to increasing concerns over the resilience and security of the integrated power grid, especially for failure modes directly associated with the grid's organic, integrated architecture.

In a distributed non-integrated system, all failures are local. In an integrated, organic system, as for any organism, an acute failure in one critical element can lead to catastrophic failure of the entire system. While integrated architectures can be optimized in ways that distributed, non-integrated networks cannot, they also have the potential for far more dangerous, system-wide failure modes.

To use a particularly apt metaphor, all our societal "eggs," our critical infrastructures, are now embedded in one massive, interdependent organic power

5. HIGH-IMPACT LOW-FREQUENCY STEERING COMM., HIGH-IMPACT, LOW-FREQUENCY EVENT RISK TO THE NORTH AMERICAN BULK POWER SYSTEM 3 (June 2010) [hereinafter HILF REPORT], *available at* http://www.nerc.com/files/HILF.pdf.

grid "basket." Our ability to function as a modern society, to protect our nation and even to eat, drink, and maintain the most essential features of a productive, healthy society now depend completely on the resilience, security, and integrity of that basket. Any risk factor that might cause a medium-to-long term failure of this integrated network, putting at risk large geographic regions for significant durations, could have unprecedented and shattering consequences.

As we will see, electromagnetic threats are an example of just such a risk factor, with the potential for a single event to exploit common design weaknesses over large regions. Even cyber threats, while dangerous and urgent, typically cannot use the same malicious software engines to effectively attack highly variant SCADA control systems scattered throughout the power grid.[6]

C. Summary

Electromagnetic threats to the national power grid are becoming a new, fundamental concern, and are receiving increasing attention by regulators, legislators, concerned power companies, and other energy sector stakeholders. This article will lay out the basis and historical context of these risks, review the protection options now receiving increasing scrutiny, and discuss the implications for regulatory or industry-initiative options.

II. DEFINING ELECTROMAGNETIC THREATS (E-THREATS)

Electromagnetic threats fall into two broad categories, which will be discussed in some detail below. In this section, it will be helpful to introduce basic terminology needed to explore these concerns.

Natural threats are caused by Severe Space Weather, including solar flares and coronal mass ejections (CMEs).[7] These solar events cause Geomagnetic Disturbances (GMDs), which in turn create quasi-DC Geomagnetically Induced Current (GIC), as distortions in the earth's magnetic field drive large, damaging GIC currents through the ground and into the large EHV transformers that transmit electric power through the power grid.[8]

While natural and malicious e-threats share similarities, both also have unique features. Malicious threats include a wide-area Electromagnetic Pulse (EMP) strike, caused by a high altitude nuclear detonation (also known as High Altitude EMP – HEMP), and local attacks from Intentional Electromagnetic Interference (IEMI) or "non-nuclear EMP" devices.[9] HEMP, like Severe Space Weather, exposes transformers and other power grid components to high GIC levels, but all EMP events also generate a fast electromagnetic pulse (E1) that can disrupt electronics.[10] For HEMP, that pulse can cover areas of subcontinental scale.[11]

---

6. EMP COMM'N 2008 REPORT, *supra* note 1, at 24.
7. HILF REPORT, *supra* note 5, at 61.
8. *Id.*
9. *Id.* at 77, 89.
10. *Id.* at 80-89.
11. *Id.* at 82 (citing EMP COMM'N 2008 REPORT, *supra* note 1).

A. Societal and Environmental Impact

Given the potential effects of high level GIC on many key EHV transformers, an unprotected national power grid could risk an unprecedented long term, wide area blackout from a Severe Space Weather or EMP event. With estimates for replacement times for even a single EHV transformer running at more than a year, the Oak Ridge National Laboratory conducted a major study of risks from space weather and EMP for the FERC, the Department of Energy (DOE), and the Department of Homeland Security (DHS), and estimated that, in the aftermath of such a major storm, as many as 130 million U.S. households could be left without power, with some of these outages extending for a period of four to ten years.[12]

The "fast" or E1 HEMP pulse can have a similar impact, with damage to substation electronics and distribution line failures anticipated over very large areas.[13] Without advanced planning, provisions for adequate spares, and other basic E1 protection measures, limited manpower and logistics constraints could turn otherwise-manageable partial equipment failures into long term, non-recoverable disasters.

Depending on the scale of the damage, the impact could be unprecedented. If the outages are long term and affect large areas, other critical power-intensive infrastructures would fail. Without a functional power grid, collapse of the water, communication, transportation, food, sewage, medical care, and security infrastructures, and consequent coolant failure at nuclear power generating stations and chemical plants, could mean an end to societal continuity and irreversible environmental damage in regions of subcontinental scale.

B. Natural Threats: Severe Space Weather

Solar activity can cause changing conditions in the near-earth space environment which can dramatically affect modern technology. These environmental effects, generally referred to as "space weather," are regularly monitored by federal and international agencies. Space weather events affect national power grids and can degrade satellite operation, force changes in air transportation corridors, and cause disturbances affecting a wide range of modern electronic systems.[14]

One of the most important space weather effects is a Coronal Mass Ejection (CME). Often accompanying solar flares, CME's occur when the sun ejects a massive cloud of energetic plasma, a condition solar astronomers typically see many times each year, as jets of erupting mass separate from the sun, headed in

---

12. OAK RIDGE NAT'L LAB, FERC EMP-GIC METATECH REPORTS 319-324, EXECUTIVE SUMMARY i (2010) [hereinafter OAK RIDGE EXEC. SUMMARY], *available at* http://www.ornl.gov/sci/ees/etsd/pes/pubs/ferc_Executive_Summary.pdf (citing NAT'L ACAD. OF SCIENCES, SEVERE SPACE WEATHER EVENTS—UNDERSTANDING SOCIETAL AND ECONOMIC IMPACTS: A WORKSHOP REPORT (2008)).

13. HILF REPORT, *supra* note 5, at 80, 82, 89.

14. JOHN KAPPENMAN, METATECH CORP., META-R-319 GEOMAGNETIC STORMS AND THEIR IMPACTS ON THE U.S. POWER GRID 4-1 (Jan. 2010) [hereinafter KAPPENMAN META-R-319], *available at* http://www.ornl.gov/sci/ees/etsd/pes/pubs/ferc_Meta-R-319.pdf. This report is part of the Oak Ridge National Laboratory Study. OAK RIDGE NAT'L LAB, FERC EMP-GIC METATECH REPORTS 319-324 (2010) [hereinafter OAK RIDGE NAT'L LAB. STUDY], *available at* http://www.ornl.gov/sci/ees/etsd/pes/ferc_emp_gic.shtml.

random directions.[15] When the sun produces an unusually large CME, if it also happens to be headed for the earth, the earth's magnetic field can be significantly distorted, generating large geomagnetically-induced currents which can flow through and damage the large EHV transformers that distribute power through national power grids.[16]

1. Historical Context

In 1859, British solar astronomer Richard Carrington witnessed the beginning of a particularly severe solar flare.[17] Newspapers from the time talked about brilliant auroral "Northern Lights," bright enough to read newspapers at midnight, reaching past Florida toward the equator.[18] Current surges in the only long distance electrical system that existed at the time – the national and international telegraph network – shut down the system, causing fires in some telegraph stations.[19]

While there have been a number of low and moderate level space weather events over the last century, most of the growth of the modern power grid began shortly after a second Severe Space Weather event in 1921, of nearly the same magnitude as the flare observed by Richard Carrington (typically known as the "Carrington Event").[20] Like its predecessor, this storm disrupted telegraph service.[21] It also burned out cables, disabled New York Central Railroad's signal system, and started a fire that burned down the Central New England Railroad station.[22] Although taking place sixty-two years after the Carrington event, this storm took place long before the development of today's sensitive digital electronics, and the far more vulnerable, continent-spanning organic power grid that characterizes our modern national power grid.

a. Summary of Government Studies

Following initial concerns raised by the Congressional EMP Commission, e-threat studies from a number of government agencies have taken place over the last several years.[23] Studies and reports included the Congressional EMP

15. *Space Weather: Sunspots, Solar Flares & Coronal Mass Ejections*, SPACE.COM, http://www.space.com/11506-space-weather-sunspots-solar-flares-coronal-mass-ejections.html.

16. *Id.*; *see also* HILF REPORT, *supra* note 5, at 61.

17. Trudy E. Bell & Dr. Tony Phillips, *A Super Solar Flare*, NASA SCIENCE (May 6, 2008), http://science.nasa.gov/science-news/science-at-nasa/2008/06may_carringtonflare/.

18. *Id.*

19. *Id.*

20. ELEC. INFRASTRUCTURE SEC. COUNCIL, SEVERE SPACE WEATHER – GEOMAGNETIC STORMS, *available at* http://www.eiscouncil.com/images/upload/media/Geomagnetic%20Storms%20-%20Information%20Sheet.pdf (last visited Feb. 16, 2013).

21. *Id.*

22. *Id.*

23. For a convenient resource containing a majority of these reports, and other similar risk assessment documents, see *Resources*, EIS COUNCIL, http://www.eiscouncil.org/English/Resources/ResourcesCategory.asp?catId=221 (last visited Feb. 24, 2013).

Commission (both the 2004 Executive Summary and the 2008 Final Report);[24] a Congressional Strategic Posture Commission Report;[25] the National Academy of Sciences and National Aeronautics and Space Administration (NASA) Severe Space Weather Report;[26] the DOE / NERC High Impact, Low Frequency Risk Report;[27] and the Oak Ridge National Laboratory Study and Report for DOE, the FERC, and DHS.[28] There have also been several international studies addressing this subject, including the U.K. Defence Select Committee e-threat Report, published in February 2012.[29]

According to all the government studies, today's power grids are many orders of magnitude more sensitive to a predicted hundred-year class[30] Severe Space Weather event or a malicious EMP strike than the limited, local systems in use in the early twentieth century.[31]

For both space weather and the HEMP "E3" pulse, high GIC flows in the unprotected power grid could cause permanent damage to many of the EHV transformers that form the "ligaments" of that system.[32] According to the studies, projected damage levels could lead to long term, wide area grid shutdowns – either immediately or some days or weeks after the event, due to cumulative transformer failures.[33]

For HEMP, in addition to the above-mentioned recent studies, the weapon's unique history, a core element of superpower nuclear strategy since the 1960s, produced a vast body of effort. Research included a DOD-funded scientific study of HEMP, nuclear weapons testing, nuclear effects modeling, and military system impact assessment, including extensive laboratory testing of hardware

---

24. EMP COMM'N 2008 REPORT, *supra* note 1; COMM'N TO ASSESS THE THREAT TO THE UNITED STATES FROM ELECTROMAGNETIC PULSE (EMP) ATTACK, EXEC. REPORT (2004) [hereinafter EMP COMM'N 2004 EXEC. REPORT], *available at* http://www.empcommission.org/docs/empc_exec_rpt.pdf.

25. CONG. COMM'N ON THE STRATEGIC POSTURE OF THE UNITED STATES, AMERICA'S STRATEGIC POSTURE (2009), *available at* http://www.usip.org/files/America's_Strategic_Posture_Auth_Ed.pdf.

26. COMM. ON THE SOCIETAL AND ECON. IMPACTS OF SEVERE SPACE WEATHER EVENTS, SEVERE SPACE WEATHER EVENTS – UNDERSTANDING SOCIETAL AND ECONOMIC IMPACTS: A WORKSHOP REPORT (2008) [hereinafter NASA/NAS study], *available at* http://www.nap.edu/catalog.php?record_id=12507.

27. HILF REPORT, *supra* note 5.

28. OAK RIDGE NAT'L LAB. STUDY, *supra* note 14.

29. DEFENCE COMM., DEVELOPING THREATS: ELECTRO-MAGNETIC PULSES (EMP), 2010-12, H.C. 1552 (U.K.) [hereinafter U.K. H.C. DEFENCE COMM. REPORT], *available at* http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/1552/1552.pdf.

30. The Oak Ridge FERC/DOE/DHS study concluded that there is a historical pattern of Severe Space Weather events, typically around once per century. OAK RIDGE EXEC. SUMMARY, *supra* note 12, at i.

31. *See, e.g.*, HILF REPORT, *supra* note 5, at 68, 74-76; NASA/NAS Study, *supra* note 26, at 11-12, 77-78.

32. *See, e.g.*, HILF REPORT, *supra* note 5, at 68-76, 86-89; KAPPENMAN META-R-319, *supra* note 14, at 4-11.

33. If GIC reduces the service life of a transformer to "zero," the transformer will fail immediately. However, an intermediate effect would be to reduce the service life to just a few days, weeks, or months, leading to gradual failure of those transformers over that extended time period and a long term blackout. This is a simple consequence of the phenomenon of "reduced service lifetime" as a function of GIC. *See, e.g.*, NORTH AM. ELEC. RELIABILITY CORP., 2012 SPECIAL RELIABILITY ASSESSMENT INTERIM REPORT: EFFECTS OF GEOMAGNETIC DISTURBANCES ON THE BULK POWER SYSTEM iii (Feb. 2012), https://www.frcc.com/Public%20Awareness/Lists/Announcements/Attachments/105/GMD%20Interim%20Report.pdf.

vulnerability.[34] For example, there were both upper atmosphere and underground nuclear tests, focused on anchoring the Pentagon's massive MICE code,[35] which became – and remains – the primary tool for understanding the full range of magnetohydrodynamic nuclear effects, including HEMP.[36] In fact, most strategic military weapons systems developed during the last half of the twentieth century included a requirement for HEMP-protected design, generally designated by the code-name "TEMPEST."[37]

While this vast body of HEMP military modeling, testing, design, and hardening technology created a substantial library for electronic system protection and became a common, accepted element of strategic military system design, carryover to increasingly vulnerable civil infrastructures was rare until the beginning of the 21st century. In fact, risks and options for civil infrastructures were not systematically reviewed until the Congressional EMP Commission began breaking this rather arbitrary military vs. civil distinction, with publication of the Commission's Executive Summary in 2004.[38]

For HEMP E1,[39] the conclusions of all the government studies are similar to the study conclusions for Severe Space Weather and HEMP E3. Ubiquitous electronic hardware represents another dimension of the Power Grid's vulnerability to HEMP, with the trend strongly favoring increasing vulnerability, as power grid components are systematically upgraded with new, more vulnerable technology.[40]

Surprisingly however, since E1 power grid vulnerability is a consequence of projected failure of only a portion of substation SCADA systems and electronic and control components, E1 protection may, in large part, be a matter of procuring and appropriately deploying adequate spares for a range of basic, low cost components, hardening selected substation control buildings, and developing focused recovery plans for implementation.[41]

---

34. *See generally e.g.*, TERRENCE R. FEHNER & F.G. GOSLING, OFFICE OF HISTORY AND HERITAGE RES., U.S. DEP'T OF ENERGY, ATMOSPHERIC NUCLEAR WEAPONS TESTING 1951-1963, *in* BATTLEFIELD OF THE COLD WAR: THE NEVADA TEST SITE, Vol. 1 (Sept. 2006), *available at* http://energy.gov/sites/prod/files/DOENTSAtmospheric.pdf, *and Nuclear Weapon Testing*, FED. OF AM. SCIENTISTS, http://www.fas.org/nuke/intro/nuke/test.htm (last visited Feb. 24, 2013).

35. DR. STEVEN CHAVIN, E-THREAT PROTECTION FOR INFRASTRUCTURE CONTINUITY—THE PHYSICS OF THE THREATS (a limited access briefing; on file with author).

36. *Id.* MICE stands for Magnetohydrodynamic Implicit Continuous-Fluid Eulerian. "MICE is a Magnetohydrodynamic EMP code used to calculate many parameters associated with a nuclear detonation in space." Private communication with Dr. Steven Chavin, one of the authors of the model.

37. *See generally* NAT'L SEC. AGENCY, TEMPEST: A SIGNAL PROBLEM, *available at* http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf (approved for release by NSA on Sept. 27, 2007).

38. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24.

39. *See, e.g.*, HILF REPORT, *supra* note 5, at 81-86.

40. "The common element that can produce such an impact from EMP is primarily electronics, so pervasive in all aspects of our society and military, coupled through critical infrastructures. Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow." EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at Abstract.

41. *Id.* at 89.

2. GIC Impact: Common to Both Space Weather and EMP

a. Transformer Risk

Geomagnetically Induced Current (GIC), caused by either Severe Space Weather or an EMP E3 pulse (see Section II.C. below), flows through the ground into EHV transformers.[42] Where GIC levels from either natural or malicious causes exceed transformer "withstand" capability, EHV transformers may become unusable, either due to GIC-induced melting of segments of the core windings, degrading and burning insulation, or other heating and hot-spot related effects.[43] Depending on the event heuristics, damage caused by a severe electromagnetic disturbance could cause failures in real time, or in succeeding days or weeks. If enough transformers are affected, or if transformers coupled to power generators are affected, the grid would go down permanently until the transformers can be replaced, estimated in the Oak Ridge National Laboratory Report to be several years.[44]

While there has been less evaluation of the bulk power system's large generators, malfunctions during moderate solar flare events indicate a Severe Space Weather event or a large EMP E3 pulse may generate negative current problems, causing damaging generator torqueing.[45] Reworking damaged generators is a very long process.

C. Malicious Threats

At ranges varying from local to subcontinental, malicious electromagnetic threats are a serious risk to a wide variety of infrastructures and utilities. The national power grid, however, is a primary concern: preventing long term regional power outages will be essential to avoid cascading failure of all other utilities and societal infrastructures. Implementing protective measures for power grid components is thus the first priority in assuring reasonable security against both HEMP and IEMI threats.[46] This section will provide a context for understanding both the problem and mitigation strategies.

HEMP actually refers to several different pulses, all produced by any upper atmosphere nuclear detonation. Each pulse has different characteristics: there is a prompt, very fast and high intensity nanosecond class pulse (E1), an intermediate time microsecond class pulse (E2), and a slow pulse (E3), which can last hundreds of seconds.[47]

For our purposes in this section, it will be most useful to focus on the E1 pulse. E2 behaves much like lightning, typically at lower magnitude: while, unlike lightning, it would "strike" at once in many locations in a large region, conventional, commonly used lightning arrestors may provide adequate protection. Damage caused by E3 behaves much like Severe Space Weather, as

42. KAPPENMAN META-R-319, *supra* note 14, at 4-10, 4-11.

43. *Id.* at 4-4 to 4-10.

44. *See, e.g.*, *id.* at 4-18 to 4-22 (discussing emergency replacement of EHV transformers).

45. *Id.* at 4-1 to 4-3 (highlighting grid collapses such as Hydro Quebec and Eskom in South Africa).

46. OAK RIDGE EXEC. SUMMARY, *supra* note 12, at iii-iv (IEMI devices are also referred to in EMP discussions as non-nuclear EMP threats).

47. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at 5-6.

discussed above (see section II.B.i). Measures taken to protect against GIC, whether from natural or malicious causes, will protect against this pulse.

In the discussion below, it is important to note that IEMI devices generate pulses comparable to or greater than E1, though at far shorter range. The phenomenology, impact, and protective measures suitable to HEMP E1 are typically applicable to electromagnetic pulses from short range IEMI devices.

1. High Altitude Electromagnetic Pulse (HEMP)

Detonation of a nuclear warhead at altitudes above approximately 30 km creates an electromagnetic pulse, a powerful field of electromagnetic energy that can extend for hundreds of kilometers: out to the horizon seen from the detonation altitude.[48] This pulse occurs automatically, with detonation of any nuclear device above the atmosphere. No unique, EMP-enhancing design is required, though such designs were apparently developed by superpowers during the Cold War,[49] and may now be more widely available.

The unique and dangerous characteristics of HEMP include its remarkable range, and its impact on the electronic components that have become ubiquitous in modern society. With a range of up to many hundreds or a few thousand kilometers, even an entry-level nuclear warhead on a single medium range missile, launched from a seemingly innocuous freighter, could deliver a devastating strike on any of the world's developed nations. If the power grid in a targeted nation is unprotected, such a strike has the potential to cause cascading and long-term failures of all critical infrastructures, threatening societal continuity.

It is this capability which makes EMP a uniquely dangerous asymmetric weapon, giving unprecedented power to any rogue state or trans-national terrorist group that could acquire even an entry-stage nuclear warhead. For example, use of such a warhead against a typical, major city in a more "conventional" mode, with detonation at or near ground level, would severely damage the city, killing tens of thousands, and potentially up to a few hundred thousand through later fallout consequences.[50] By contrast, a Severe Space Weather event or an HEMP attack could severely damage the entire nation, shutting down vital infrastructures for years over huge areas. For the United States, it was estimated that more than 100 million households could be left without power, some for a period likely to last years.[51]

Taken together, the devastating range and impact of a single EMP "bullet," the steady growth of proliferation, and the weakening relevance of traditional deterrence strategies have all combined to place HEMP weapons near the top of the threat list for security forces in most developed nations.

48. HILF REPORT, *supra* note 5, at 77-80.

49. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at 1-2.

50. William C. Bell & Cham E. Dallas, *Vulnerability of Populations and the Urban Health Care Sys. to Nuclear Weapon Attack – Examples From Four American Cities*, INT'L J. OF HEALTH GEOGRAPHICS tbl. 3 (Feb. 28, 2007), *available at* http://www.ij-healthgeographics.com/content/pdf/1476-072X-6-5.pdf.

51. OAK RIDGE EXEC. SUMMARY, *supra* note 12, at i.

a. Historical Context

HEMP was first observed in 1962, when the United States began conducting a series of upper atmosphere nuclear tests.[52] While theorists had predicted this effect, it came as a surprise to authorities when, during the nuclear test code-named Starfish Prime, there were electrical failures in Hawaii, 800 miles from the nuclear missile launch site in the Pacific Ocean.[53]

Later that year the U.S.S.R. carried out similar tests, detonating nuclear warheads at high altitudes over Kazakhstan.[54] For those tests in which data was provided, years later, to U.S. authorities, open source briefings indicate that the high altitude detonations were remarkably destructive, causing breakdowns and failures in buried and above ground power and phone lines, burning out radars and radio equipment, and destroying Kazakhstan's power substations.[55]

As a result of these early tests, an HEMP strike quickly became standard doctrine in developing nuclear war strategies. Any superpower nuclear missile exchange would begin with a small wave of missiles detonating at high altitude to deliver an EMP strike, intended to destroy command, communication, and control systems, and prevent a counterstrike. In fact, this feature of nuclear strategic doctrine introduced what became the most dangerous instability of the Mutually Assured Destruction (MAD) strategy that characterized the Cold War years.[56] Both sides were forced to recognize even a single suspected enemy missile launch as a probable devastating, disabling threat, mandating launch of a full nuclear arsenal counterstrike in minutes, on warning of even a single enemy missile. On one famous post-cold war occasion, this HEMP-based instability brought the world close to an inadvertent launch of the U.S. and Russian nuclear missile fleets – an accidental nuclear war.[57]

Following the end of the Cold War, with expanding nuclear proliferation, concerns grew that the rapid growth of the U.S. power grid, in both scale and technology, might be creating a new, inadvertent civilian infrastructure vulnerability to HEMP. In 2000, the U.S. Congress, responding to these concerns, formed The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, commonly known as the "Congressional EMP Commission."[58] The Commission, taking testimony from all agencies of the U.S. government supplemented by laboratory tests and analysis by defense contractors and other consultants and testing organizations, issued a number of reports, in both restricted and unrestricted access volumes,

52. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at 4.

53. *Id.*

54. ELEC. INFRASTRUCTURE SEC. COUNCIL, USSR NUCLEAR EMP UPPER ATMOSPHERE KAZAKHSTAN TEST 184 (2012), *available at* http://www.eiscouncil.com/images/upload/media/Soviet%20Test%20184.pdf.

55. *Id.* at 4.

56. EMP COMM'N 2008 REPORT, *supra* note 1, at 45.

57. David Hoffman, *Cold-War Doctrines Refuse to Die*, WASH. POST (Mar. 15, 1998), http://www.washingtonpost.com/wp-srv/inatl/longterm/coldwar/shatter031598a.htm.

58. Floyd D. Spence Nat'l Def. Authorization Act for Fiscal Year 2001, Pub. L. No. 106-398, tit. XIV, 114 Stat. 1654 (2000).

including an unclassified Executive Summary Report (2004)[59] and a Final Report (2008).[60]

The Commission's reports, the first of the many recent government agency reports summarized above, found that, while HEMP and Severe Space Weather must be considered potential existential threats to the continuity of the nation, cost effective measures are feasible to harden the power grid and, over time, other critical infrastructures. [61]

International cooperation also began during this period, highlighted by the annual meetings of the Electric Infrastructure Security Summit, with cabinet officials and other senior government representatives and scientists from dozens of nations meeting together to review and discuss both e-threats and protection options and strategies.[62]

b. EMP Impact

The HEMP impact on the power grid is typically characterized according to the effects of each pulse type, including the short pulse (E1), and the long pulse (E3) effects (E2 is generally not considered a factor – see Section II.C. above).[63]

i. Long Pulse

The effects of the long EMP pulse, also known as "E3," are functionally very similar to the impact of a Severe Space Weather-caused GIC event discussed above,[64] though the affected region would, of course, depend on the strike location(s). The primary E3 risk is, therefore, to EHV transformers.

ii. Short Pulse

The short EMP pulse, known as "E1,"[65] creates a very brief, very high intensity field that causes electric breakdown in some, not all, exposed components. Unprotected substations within the footprint of this pulse would generally fail from several overlapping effects. Most low voltage distribution lines would go down, since flashover (arcing) of even one of the many insulators on any single line will make that line non-operational. Substation control and data systems as well as individual residential smart meters would also typically break down, due to E1-caused burnout and upsets of portions of critical systems, including power relays, SCADA controller computers, switches, and other electronic and circuit components. Given the huge footprint of the field, most or

59. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24.

60. EMP COMM'N 2008 REPORT, *supra* note 1.

61. *See, e.g., id.* at 46.

62. *See, e.g.*, ELEC. INFRASTRUCTURE SEC. SUMMIT, EISS III LONDON REPORT: CONCLUSIONS AND RECOMMENDATIONS (May 2012) [hereinafter EISS III LONDON REPORT], *available at* http://www.eissummit.com/images/upload/conf/media/EISS%20III%20London%20Report.pdf.

63. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at 5-6.

64. *See generally* KAPPENMAN META-R-319, *supra* note 14.

65. *See generally* EDWARD SAVAGE, JAMES GILBERT & WILLIAM RADASKY, METATECH, META-R-320, THE EARLY-TIME (E1) HIGH-ALTITUDE ELECTROMAGNETIC PULSE (HEMP) AND ITS IMPACT ON THE U.S. POWER GRID (Jan. 2010), *available at* http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-320.pdf (prepared as part of the Oak Ridge Study).

all substations would break down in a large portion of the continent, even without E3-induced damage of the critical EHV transformers.

Unlike the situation for a more isolated problem, it would not be possible to bring large, expert teams and spare equipment from nearby, unaffected facilities. With substation breakdowns taking place on subcontinental scales, available trained manpower and spare equipment would be small in comparison with the need. Locating problems would also be extremely difficult, with the SCADA control and data acquisition systems down.

Complicating the problem further, logistics would be a critical problem. Gas stations would no longer operate, telephone and cell phones would fail, and the entire commercial sector in the region – both wholesale and retail – would be closed. Of course, even retention of the inadequate numbers of trained personnel available before the event occurred would quickly become impossible, as they struggle to find food, water, functional shelter, and security for themselves and their families. When these problems are coupled with EHV transformer failures due to the EMP E3 pulse, the overlapping problems become impossible to deal with.

2. Intentional Electromagnetic Interference (IEMI)

With the national power grid today considered to be the primary civil utility, and the critical linchpin required to avoid cascading failure of the other societal infrastructures, assuring the continuity of secure power has become a primary focus of energy policy.

This reality has been a central theme recurring in all the government studies that have looked at e-threat vulnerability, beginning with the two reports of the Congressional EMP Commission.

In fact, this is true today not only for basic societal infrastructures, but also for military and security capability. Speaking in London at Electric Infrastructure Security Summit III in May 2012, U.S. Assistant Secretary of Defense Dr. Paul Stockton made this extremely clear.[66]

> Even if we were in a hardened DOD facility from an inside the base perspective, it's that flow of electric power, that resilient flow of electric power that we need to be able to ensure so that in turn we can live up to our commitments to the American people to execute the responsibilities assigned to us.[67]

Summarizing the Pentagon's dependence on reliable power, he continued, "The Department of Defense is utterly dependent [on the power grid] to execute its responsibilities."[68]

While it is clear that a wide area HEMP attack involves far higher risk for society, growing concerns have been voiced recently for the potential risk from non-nuclear EMP devices (NNEMP), also known as IEMI. These concerns have been summarized in a number of focused conferences and papers addressing this topic. For example, in his paper, *The Threat of Intentional Electromagnetic Interference (IEMI) to Wired and Wireless Systems*, Dr. William A. Radasky

66. EISS III LONDON REPORT, *supra* note 62, at 19.

67. *Id.*

68. *Id.*

points to a number of key factors that have made these threats a growing concern:

- Criminal threats are increasing world-wide, especially with regard to information security[;]
- Covert operations outside of physical barriers are attractive to criminals[; and]
- Technological advances have produced higher- energy RF sources and more efficient antennas, allowing the use of these weapons at further ranges.[69]

"Society's dependence on information and on automated mission-critical and safety-critical electronic systems is increasing."[70] And while IEMI weapons lack the vast range of HEMP, over short ranges they could actually be more dangerous. Such devices, built from easily obtained, commercially available hardware, reportedly have been demonstrated to produce pulses "almost an order of magnitude greater than the largest [nuclear EMP (NEMP) pulses]."[71]

The source of the concern is that "[t]he non-nuclear EMP threat (NNEMP) arises from the ability to build extremely powerful radio transmitters that can duplicate the waveforms and intensities of the EMP portion of a nuclear explosion."[72]

Such systems may be ideal for terrorists. While a competent electrical engineer could build such a device, they are also available commercially, and their sale – typically for use as test equipment – is not restricted. In one recent example, such a device, referred to by the manufacturer as the "EMP Suitcase,"[73] was successfully shipped internationally by a commercial carrier, and carried into a central parliamentary building.[74]

Given an appropriate deployment, the potential for use of such devices to disable a power substation control center or other critical equipment, and then be reused to do additional damage, adds a new element of urgency to addressing malicious e-threat risks.

3. Geopolitical Risk Assessment

A cursory review of newspaper headlines over the last fifteen years helps explain why NATO Secretary General Anders Fogh Rasmussen's message to NATO's annual Conference on Weapons of Mass Destruction (WMD) and Arms Control included an implicit admission that the risk of proliferation is growing,

---

69. William A. Radasky, *The Threat of Intentional Electromagnetic Interference (IEMI) to Wired and Wireless Systems*, *in* EMC-ZURICH 2006, at 160 (2006) (subscription service), *available at* http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1629584&contentType=Conference+Publications&refinements%3D4294705264%26sortType%3Dasc_p_Sequence%26filter%3DAND%28p_IS_Number%3A34187%29.

70. *Id.*

71. Curtis Birnbach, Advanced Fusion Sys., Understanding the Problem: Nuclear and Non-Nuclear EMP, slide 4 (2011), *available at* http://www.eissummit.com/images/upload/conf/media/Curtis%20Birnbach%20Presentation.ppt. This powerpoint was part of Mr. Birnbach's presentation at the EISS Summit II in Washington, D.C. on April 11, 2011. To view other presentations from the Summit, see THE ELEC. INFRASTRUCTURE SEC. SUMMIT: THE 2ND ANNUAL WORLD SUMMIT ON INFRASTRUCTURE SEC., http://www.eissummit.com/archive_Washington11.asp (last visited Feb. 16, 2013).

72. Birnbach, *supra* note 71, at slide 5.

73. EISS III LONDON REPORT, *supra* note 62, at 22 (example of an EMP Suitcase).

74. Details of this occurrence are based on private communications by the author, who may be contacted for further reference.

referring "to the growing number of countries and non-state actors that are seeking WMD or the means to deliver them."[75]

With deterrence in the multi-polar, increasingly ideologically-driven post-cold war world already playing a dwindling role, HEMP may further undermine some of the last remaining value in the strategy sometimes credited with keeping the peace for decades. An EMP attack would have a devastating impact on all the normal channels of government coordination and communication, including intelligence and data gathering assets, and nuclear forensics. Indeed, with a severe societal breakdown, the basic continuity of government agencies would be at risk. Under such circumstances, it is judged unlikely that the source of an EMP attack – given even a minimal attempt to disguise it – would ever be known.

In fact, however, the issue with deterrence may be even more severe. If trans-national terrorist forces were to acquire even a small nuclear warhead to use with the short and medium range missiles that such groups already control, finding the return address needed for the deterrent equation would, of course, be irrelevant.

With NATO and other national and international agencies projecting a pattern of steady growth in proliferation of an asymmetric weapon of such breathtaking power,[76] multiple U.S. government commissions have called for progress in critical infrastructure protection as a matter of urgency.

The Congressional EMP Commission summarized these geopolitical concerns in the introduction to the Commission's 2004 Executive Summary:

> Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication. EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences.
>
> . . . .
>
> The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected. Correction is feasible and well within the Nation's means and resources to accomplish.[77]

III. THE GOVERNMENT PERSPECTIVE: THE VIEWS OF U.S. AND INTERNATIONAL REGULATORY, ENERGY, AND SECURITY AGENCIES

A. The Interagency Syndrome: Dealing With Risks That Cut Across Agency Boundaries

Given the remarkable scope of the problem, both public and private domains will need to be involved. Thus, one of the most striking features of this issue is the remarkable contradiction between the potential scope of an e-threat crisis, and the relatively slow pace of either government or corporate action to address it.

---

75. *NATO and Partners Examine Non-Proliferation, Arms Control and Disarmament*, N. ATLANTIC TREATY ORG. (June 16-17, 2011), http://www.nato.int/cps/en/natolive/news_75428.htm.

76. U.K. H.C. DEFENCE COMM. REPORT, *supra* note 29, at Ev 5.

77. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at Abstract.

As indicated above, government agencies and departments participating in recent e-threat studies include all relevant departments and agencies of the U.S. government and the U.S. Congress, as well as international studies from the United Kingdom and other allied nations. The studies have all reached the same general conclusion, consistent with the substantial body of previous, related military studies[78]: Severe Space Weather and HEMP have the potential to cause unprecedented, long term blackouts on subcontinental scales.[79]

We are left, therefore, with a compelling mystery. While important steps have begun, why has neither government nor corporate action been more timely? What are the roadblocks that have slowed a broader, faster response?

At the risk of oversimplifying an issue that goes to the heart of a number of classic governmental processes, two primary forces tend to slow proactive efforts to address large scale risks of this nature.

1. Evaluating Risk: Prevention vs. Recovery

Projected societal risks, regardless of scale, are inevitably considered in the wider context of a long list of such concerns. Neither governments nor corporations can address them all. The almost invariable rule is to evaluate and prioritize such lists through the simple expedient of waiting to experience a predicted crisis many times, using the consequences both to tune prevention and recovery planning, and to build stakeholder support. While far from ideal, this imperfect process does, in the long run, work. And it has the advantage of replacing the uncertainties of foresight with the clarity of 20:20 hindsight.

For a government, and especially a democracy, this less-than-ideal approach also comes with other built-in incentives. Elected officials are almost always given more credit for their organizational skills in recovering from a crisis than for the leadership it takes to avoid one. Politically, crisis response is almost always easier to justify and motivate than crisis prevention.

Unfortunately, when a crisis is large enough to impact societal continuity, this approach is fatal. If there is no advance preparation, the first national experience of a severe e-threat may be catastrophe.

2. Managing Risk: The e-threat Government Overlay

In addition to the basic prioritization issues that make hindsight a more dependable ally than foresight, there is another basic problem. To illustrate this, we can use a comparatively recent, ready-made example.

Beginning in the early 1980's, the United States, international governments, and the commercial sector all began to realize that the developed world faced a technical issue that cut across nearly all sectors of government and society: the

78. *See, e.g.*, DEP'T OF DEF., DEF. SCI. BD. TASK FORCE, SUMMARY REPORT NO. 1: SURVIVABILITY OF SYSTEMS AND ASSETS TO ELECTROMAGNETIC PULSE (EMP) AND OTHER NUCLEAR WEAPON EFFECTS (NWE) (Aug. 2011) [hereinafter DEFENSE SCIENCE BOARD REPORT], *available at* http://www.acq.osd.mil/dsb/reports/ADA550250.pdf.

79. *See generally Risk Assessment and Protection Library*, EIS COUNCIL, http://www.eiscouncil.com/English/Resources/ResourcesCategory.asp?catId=221 (compiled library of documents and reports relating to infrastructure protection).

Millennium Bug.[80] While the consequences of a Y2K software failure would be highly system dependent, almost every aspect of the government and commercial sectors faced the same fundamental risk: developers of their software infrastructures had often ignored a known, serious flaw in handling date encoding for the new century. Technically, the problem was rarely challenging. The difficulty was in managing an issue that affected so many different areas.

In the words of one of the governors of the U.S. Federal Reserve System, "[a]lthough the problem itself is not technically difficult, ensuring that information systems are Year 2000 compliant is a management challenge of enormous scale and complexity. [T]his matter will impact every organization everywhere . . . ."[81] With e-threats, we are dealing with an issue often seen to have a similar management complexity. And, unlike the Y2K problem, government and commercial sector efforts to address electromagnetic threats are working to an unknown deadline.

E-threats are projected to have a substantial impact in the domains of almost every aspect of government. While the primary risk from severe solar weather would be to the security of the national power grid, long term failure of that grid would cause cascading failures affecting everything from banking and finance to agriculture, the environment, education, medical care, telecommunications, transportation, and so on. A malicious HEMP attack carries the same, practically unlimited range of consequences, with the added dimension of direct attack on electronic systems within a large target zone.

This breadth of impact means there is no congruence between the threat and our most basic government structures. And, in fact, most branches of government, while increasingly voicing alarm over e-threat risks, have found their organizational responsibilities are a poor match, at best, to deal with the problem.[82]

Thus we find that many U.S. government departments and agencies are beginning to look internally at the limited measures they can take to protect their own systems, while calling publicly for more fundamental action to address the threat itself, more directly.[83]

To a large extent, the commercial energy sector faces a similar challenge. While the e-threat issue is relevant to the approximately 300 U.S. large bulk power companies, and many have expressed concern and interest in making progress at understanding and addressing these threats, existing energy sector member organizations do not have tools to help motivate, empower, or coordinate a voluntary strategy among these companies.[84]

---

80. *See generally* JEROME T. MURRAY & MARILYN J. MURRAY, THE YEAR 2000 COMPUTING CRISIS (McGraw-Hill, 1996) (PBI, 1984) (originally published under the title COMPUTERS IN CRISIS).

81. Edward W. Kelley, Jr., Governor, Fed. Reserve Bd., Remarks before the Professional Banker's Association 1 (Dec. 15, 1997), *available at* http://www.bis.org/review/r980102e.pdf?frames=0.

82. EMP COMM'N 2008 REPORT, *supra* note 1, at vii-viii.

83. For example, the Pentagon's efforts on EMP are limited to addressing their own systems' vulnerability rather than protecting society overall by hardening the power grid. *See generally* DEFENSE SCIENCE BOARD REPORT, *supra* note 78.

84. *See, e.g.*, Janet Raloff, *Elec. Grid Still Very Vulnerable to Electromagnetic Weaponry*, SCI. NEWS (July 23, 2009), http://www.sciencenews.org/view/generic/id/45868/description/Electric_grid_still_very_vulnerable_to_electromagnetic_weaponry (discussing development of smart-grid technology and EMP threats).

In fact, however, the management problem may not be as complex as it at first seems.

While the impact of a space weather incident would be felt by all sectors of society, these effects would almost all be secondary to failures of portions of the national power grid. And although malicious EMP could affect society broadly and directly, the most damaging consequences would be felt by the energy sector and related critical utilities. The effects on other infrastructures, though severe if there is no planning, will be less catastrophic. If the energy sector were protected, damage to these other infrastructures would be painful, but recoverable.

This understanding suggests a time-phased protection architecture should be adequate, beginning with the energy sector and other critical societal infrastructures, while encouraging other sectors of the economy to address issues over time.

B. U.S. Government Perspectives

1. The Department of Homeland Security

In its final report published in 2008, the Congressional EMP Commission recommended that DHS "play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences."[85]

Speaking to the House of Representatives Committee on Homeland Security, at a Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee hearing on September 12, 2012, Brandon Wales, DHS's National Protection and Programs Directorate Infrastructure Analysis and Strategy Division Director, summarized the department's evolving efforts in this area.[86] Speaking of the Commission recommendation, Mr. Wales summarized: "The Department takes that recommendation seriously."[87]

While DHS has no authority over the commercial power sector, its ability to define serious national-scale threats, combined with its other wide ranging responsibilities, give it a unique opportunity to help with preparations to address electromagnetic threats. For example, responding to Congressional requests, DHS is reportedly considering adding EMP as one of the National Planning Scenarios, "a diverse set of high-consequence threat scenarios of both potential terrorist attacks and natural disasters."[88]

Two years ago, DHS participated with DOE and the FERC in the Oak Ridge National Laboratory e-threat Study, a major, thousand page report that

85. EMP COMM'N 2008 REPORT, *supra* note 1, at 181.

86. *The Electromagnetic Pulse (EMP) Threat: Examining the Consequences: Hearing Before the Subcomm. on Cybersecurity, Infrastructure, Prot., and Sec. Technologies, H. Comm. on Homeland Sec.*, 112th Cong. 1 (Sept. 12, 2012) (written testimony of Brandon Wales, Director of National Protection Programs Directorate Infrastructure Analysis and Strategy Division) [hereinafter Wales Subcomm. Testimony], *available at* http://www.dhs.gov/news/2012/09/12/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity.

87. *Id.*

88. *National Preparedness Guidelines*, DEP'T OF HOMELAND SEC., http://www.dhs.gov/national-preparedness-guidelines (last visited Feb. 16, 2013).

represents the most recent major study done in this area.[89] From the comments made by Director Wales at the House Homeland Security Committee, it seems this focus is continuing, as DHS is working to define and expand its role in this area.

In his testimony, Director Brandon Wales pointed out that "EMP in its various forms can cause widespread disruption and serious damage to electronic devices and networks, including those upon which many critical infrastructures rely, such as communication systems, information technology equipment, and supervisory control and data acquisition (SCADA) modules . . . EMP places all critical infrastructure sectors at risk."[90] In these remarks, Director Wales was referring to Severe Space Weather, HEMP, and IEMI as different forms of EMP.

Speaking in regard to the nation's evolving vulnerability, he continued, "today's power grid and information networks are much more vulnerable to EMP than those of a few decades ago."[91]

He also addressed specifically the risk from both Severe Space Weather and HEMP. On space weather, he said, "[an] extreme CME is the Department's biggest Solar Weather concern. It could create low-frequency EMP similar to a megaton-class nuclear HEMP detonation over the United States, which could disrupt or damage the power grid, undersea cables, and other critical infrastructures."[92]

In regard to HEMP, he pointed out that an HEMP threat could be launched from a number of different platforms, increasing the risk that such an attack could come from a rogue state or terrorist group.[93] "HEMP threat vectors can originate from a missile, such as a sea-launched ballistic missile; a satellite asset; or a relatively low-cost balloon-borne vehicle," he said.[94] "A concern is the growing number of nation-states that in the past have sponsored terrorism and are now developing capabilities that could be used in a HEMP attack."[95] Depending on the deployment, he continued, "One high-altitude burst could blanket the entire continental United States and could cause widespread power outages and communications disruptions and possible damage to the electricity grid for weeks or longer."[96]

In a final specific reference to the third class of e-threats (IEMI, also referred to as Non-Nuclear EMP – NNEMP, or Radio Frequency Weapons – RFW), he pointed out that the capabilities inherent in such comparatively simple weapons could be significant.

> Devices that can be used as RFWs have unintentionally caused aircraft crashes and near crashes, pipeline explosions, gas spills, computer damage, vehicle malfunctions, weapons explosions, and public water system malfunctions. The

89. OAK RIDGE NAT'L LAB. STUDY, *supra* note 14.

90. Wales Subcomm. Testimony, *supra* note 86, at 2.

91. *Id.* at 1.

92. *Id.*

93. *Id.*

94. *Id.*

95. *Id.*

96. *Id.*

> Department believes that much of the mitigation and planning we are doing for other types of EMP will help reduce our threat to NNE[M]P." [97]

2. The White House

Over the last several years the White House began taking an active interest in Severe Space Weather, with the Office of Science and Technology Policy (OSTP) taking a leading role.[98] Recognizing the management challenges associated with large scale, cross-departmental issues like Space Weather, the OSTP began hosting periodic meetings of a Geomagnetic Interagency Working Group, to review new developments, and share information.[99]

Summarizing the issue from a White House perspective, Tamara Dickinson, a senior OSTP policy analyst, said, "[s]pace weather is a serious matter that can affect human economies around the world,"[100] speaking to attendees of the 2012 Space Weather Enterprise Forum in Washington, D.C. A primary focus of the White House is to help ensure a continued solar observation capability, calling for a replacement for the aging Advanced Composition Explorer (ACE) satellite, which today provides the best available space weather data.[101] Although the White House effort is limited, its focus grows from an early 2012 presidential directive to the OSTP and the National Security Staff, "to aggressively move forward with space weather mitigation efforts."[102]

3. The Department of Defense

With no single government office responsible for the full scope of e-threat issues, departments and agencies have tried to take limited steps in areas that fall within their authority. The Department of Defense's approach is a typical example.

Speaking in London at Electric Infrastructure Security Summit III in May 2012, Assistant Secretary Dr. Paul Stockton explained that "DOD cannot perform its mission without commercial power industry cooperation."[103] "Even if we were in a hardened DOD facility from an inside the base perspective," he said, "it's that flow of electric power, that resilient flow of electric power that we need to be able to ensure so that in turn we can live up to our commitments to the American people to execute the responsibilities assigned to us."[104]

DOD officials have made it clear that, though they are deeply concerned, they have been limited to addressing only those risks that fall within their direct responsibility. Given anticipated large scale energy sector failures, DOD has

---

97. *Id.* (internal citation omitted).

98. NAT'L SPACE WEATHER PROGRAM, 2012 SPACE WEATHER ENTERPRISE FORUM SUMMARY REPORT 21-22 (2012), *available at* http://www.ofcm.gov/swef/2012/SWEF%20SumReport%20v%20final.pdf.

99. *Id.* at 22.

100. Randy Showstack, *White House and Agencies Focus on Space Weather Concerns*, 93 EOS, TRANSACTIONS, AM. GEOPHYSICAL UNION No. 25, 235, 235 (June 19, 2012), *available at* http://onlinelibrary.wiley.com/doi/10.1029/2012EO250003/pdf.

101. *Id.*

102. *Id.*

103. EISS III LONDON REPORT, *supra* note 62, at 19.

104. *Id.*

also acknowledged that this approach can have only limited success in mission assurance and resilience.

Assistant Secretary Stockton has spoken on this subject in several different venues, including Congressional testimony. "On this issue of great importance to the security of our nation, the Department of Defense is largely in a supporting role. . . . The Department of Defense relies on commercial electric power for nearly 99% of its power needs at military installations."[105] Given the vulnerability of the civilian power grid to e-threats, cyber attack, and other concerns, DOD's Defense Science Board found this situation unacceptable.[106] In a recent report, the Defense Science Board concluded, "[c]ritical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the [commercial electrical power] grid."[107] In other words, the Department of Defense now recognizes a long term blackout as a serious, credible threat to the nation's military capability.

Unable to take on the challenge of addressing e-threats or other national-scale energy security concerns for the nation as a whole, DOD established the Energy Grid Security Executive Council, with experts and senior executives from the Pentagon, DOE, and DHS meeting periodically to help DOD take partial measures in some areas.[108]

What are these partial measures? "Islanding" studies were initiated in the Navy's Dahlgren Mission Assurance Division, in Vandenberg Air Force Base and in the Marine Corps Air Ground Combat Center Base in Twenty Nine Palms, to evaluate developing separate, DOD-unique microgrids at the facility.[109] "The island would be capable of generating and distributing electric power if the grid (outside the region) is disrupted for either short or extended periods of time."[110]

But DOD has made it clear that such measures, without steps to harden the commercial power grid, cannot resolve this national security threat. Referring to ongoing discussions with DOE, DHS, the FERC, and NERC, Assistant Secretary Stockton said, "[a]lthough there are steps the Department can and should take on its own to improve resilience and continuity of operations, achieving more comprehensive electric grid security to ensure critical Department of Defense missions is not something the Department of Defense can do acting alone."[111] Resolving this problem, he explained, will require action from both commercial power companies and other government agencies. "[F]or the Department of Defense to succeed in this challenge, leadership and support from industry

105. *Protecting America's Security Grid: Hearing Before the Subcomm. on Energy and Power, H. Comm. on Energy and Commerce*, 112th Cong. 1 (May 31, 2011) (testimony of Hon. Paul Stockton, Assistant Secretary of Defense, Homeland Defense and Americas' Security Affairs Department of Defense) [hereinafter Stockton Testimony], *available at* http://www.dod.mil/dodgc/olc/docs/testStockton05312011.pdf.

106. DEP'T OF DEF., DEF. SCIENCE BD. TASK FORCE ON DOD ENERGY STRATEGY, MORE FIGHT – LESS FUEL 53-54 (Feb. 2008), *available at* http://www.acq.osd.mil/dsb/reports/ADA477619.pdf.

107. *Id.* at 63.

108. Stockton Testimony, *supra* note 105, at 5-6.

109. *Id.* at 6-8.

110. *Id.* at 6-7.

111. *Id.* at 4.

representatives and interagency partners at various levels of government are imperative."[112]

4. Congress

While most of the expertise related to EMP threats in the last century came from DOD's efforts to protect strategic weapons systems, the first major review of risks and protection operations for critical civilian infrastructures came from a U.S. Congressional initiative. The Congressional EMP Commission (The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack) was established pursuant to title XIV of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001.[113]

The Commission, which published an Executive Summary in 2004 and a final report in 2008, found that HEMP is a potential severe threat to the security and continuity of the United States.

In its Executive Summary, the Commission wrote, "[s]everal potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication."[114]

> EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. EMP will cover the wide geographic region within line of sight to the nuclear weapon. It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of US society, as well as to the ability of the United States and Western nations to project influence and military power.[115]

"EMP effects . . . are not new threats. . . . What is different now is that some potential sources of EMP threats are difficult to deter. . . ."[116]

Since the publication of the EMP Commission's Final Report in 2008, the primary advocacy in Congress for protection of the power grid against electromagnetic threats has come from the House of Representatives. In recent years, Rep. Trent Franks (R-AZ) and Rep. Yvette Clarke (D-NY) have taken a particularly active role, including co-chairing Electric Infrastructure Security Summits that brought senior government representatives of more than twenty nations together to discuss these matters.[117]

In particular, while both Senators and Congressional Representatives have spoken about the need for grid protection against electromagnetic threats, the

---

112. *Id.*

113. Floyd D. Spence Nat'l Def. Authorization Act for Fiscal Year 2001, Pub. L. No. 106-398, tit. XIV, 114 Stat. 1654 (2000).

114. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at 1, Abstract.

115. *Id.*

116. *Id.* at 2.

117. ELECTRIC INFRASTRUCTURE SECURITY SUMMIT: THE FIRST WORLD INFRASTRUCTURE SECURITY SUMMIT (Sept. 2010) [hereinafter EISS I LONDON REPORT], *available at* http://www.eissummit.com/images/upload/conf/media/EISS%20London%20Report_2.pdf; ELECTRIC INFRASTRUCTURE SECURITY SUMMIT: THE 2ND ANNUAL WORLD SUMMIT ON INFRASTRUCTURE SECURITY (Apr. 2011) [hereinafter EISS II WASHINGTON REPORT], *available at* http://www.eissummit.com/images/upload/conf/media/Final%20Report.pdf; EISS III LONDON REPORT, *supra* note 62.

two legislative initiatives introduced over the last several years both came from the House.

In April 2010, Rep. Edward Markey and co-sponsor Rep. Fred Upton introduced H.R. 5026, the GRID Act (Grid Reliability and Infrastructure Defense Act), which would have amended the Federal Power Act to protect the bulk power system and critical defense electric infrastructure against cyber threats, EMP, and other threats and vulnerabilities.[118] The GRID Act passed the House with a unanimous voice vote, but companion legislation in the Senate did not move forward, and the Act did not become law.[119]

In February 2011, Rep. Trent Franks with a bipartisan group of co-sponsors introduced H.R. 668, the SHIELD Act (Secure High Voltage Infrastructure for Electricity from Lethal Damage Act).[120] The Act, reintroduced in 2012, would amend the Federal Power Act to authorize the FERC to take several actions to protect the national power grid from both Severe Space Weather or malicious EMP.[121] The proposed Act would direct the FERC to mandate reliability standards, require power companies to protect EHV transformers, direct DOE to develop expertise for grid protection, and also provide for FERC emergency measures, upon Presidential determination of an imminent threat.[122] The SHIELD Act did not reach the Floor, and did not become law.[123]

5. The Department of Energy

DOE has been one of the primary organizations involved in assessing electromagnetic threats to the U.S. power grid. On June 2, 2010, reporting on a workshop that took place the previous year, DOE, working in coordination with NERC, published a special report assessing serious, less common risks to the U.S. bulk power system.[124] The "HILF Report," (High-Impact, Low-Frequency Event Risk to the North American Bulk Power System) assesses a range of potentially catastrophic risks that could have disastrous impact on the bulk power system, including Geomagnetic Disturbance / Electromagnetic Pulse (GMD / EMP).[125] Participating organizations in the workshop summarized in

118. The GRID Act, H.R. 5026, 111th Cong. (2010).

119. Gar Smith, *Flare-up: How the Sun Could Put an End to Nuclear Power*, 27 EARTH ISLAND J. 1 (Spring 2012), *available at* http://www.earthisland.org/journal/index.php/eij/article/flare-up_how_the_sun_could_put_an_end_to_nuclear_power.

120. SHIELD Act, H.R. 668, 112th Cong. (2011).

121. *Legislation Introduced to Address Vulnerabilities of Power Grid to Cyber Threats*, SUTHERLAND (Feb. 22, 2011), http://www.sutherland.com/files/News/9d1f8cbe-90a9-43c8-978b-1c5ea76cfbdd/Presentation/NewsAttachment/6745a00b-5380-43f8-8a56-4897d0c5b166/LegislationIntroducedAddressVulnerabilitiesPowerGridtoCyberThreatsFeb2011.pdf.

122. SHIELD Act, H.R. 668, 112th Cong. § 3 (as introduced to the Senate, Feb. 11, 2011) (proposing an amendment to the Federal Power Act, 16 U.S.C. § 824 by adding §§ 215A(b)(1), 215A(c)(3)-(4)).

123. William Jackson, *EMP Attack on Power Grid Could Take Down DOD Systems, Experts Warn*, GCN: TECH., TOOLS AND TACTICS FOR PUB. SECTOR IT (Sept. 12, 2012), http://gcn.com/Articles/2012/09/12/EMP-threat-to-power-grid-DOD.aspx?p=1.,1.

124. HILF REPORT, *supra* note 5, at 2.

125. *Id.* at 61-102.

the report included DOD, DHS, the FERC, Congressional Staff, and the Department of Health and Human Services.[126]

The Report's Executive Summary provides a brief review of the overall conclusions:

- Severe Space Weather: "Geomagnetically-induced currents on system infrastructure have the potential to result in widespread tripping of key transmission lines and irreversible physical damage to large transformers."[127]
- HEMP: "The high-altitude detonation of a large nuclear device or other electromagnetic weapon could have devastating effects on the electric sector, interrupting system operation and potentially damaging many devices simultaneously."[128]
- Non-Nuclear EMP / IEMI:

> A coordinated attack involving intentional electromagnetic interference (IEMI) could result in more localized and targeted impacts that may also cause significant impacts to the sector. The physical damage of certain system components (e.g. extra-high-voltage transformers) on a large scale, as could be effected by any of these threats, could result in prolonged outages as procurement cycles for these components range from months to years.[129]

More recently, DOE joined with the FERC and DHS in a major study of electromagnetic threats to the national power grid. This study, conducted by the Oak Ridge National Laboratory, considered IEMI weapons, nuclear HEMP, and Geomagnetic Storms, concluding that, while the cost of damage from an extreme solar event would be very high, costs for implementing protective measures would be minimal.[130]

6. Federal Energy Regulatory Commission

As the federal regulatory body responsible for oversight of the U.S. power grid, the FERC has taken a leading role in assessing electromagnetic threat risks to the power grid, and considering protection options and potential regulatory measures.

In 2011, joining together with DOE and DHS, the FERC participated in a major study performed by the Oak Ridge National Laboratory. The study reviews the threat phenomenology for EMP, IEMI and GMD, the predicted impact on the U.S. power grid and options for grid protection, reaching conclusions very similar to those of the earlier HILF Report and the Congressional EMP Commission.[131]

The report concludes, in its executive summary,

> [t]he cost of damage from the most extreme solar event has been estimated at $1 to $2 trillion with a recovery time of four to ten years, while the average yearly cost of

126. *Id.* at 2.

127. *Id.* at 11.

128. *Id.*

129. *Id.* at 11-12.

130. OAK RIDGE EXEC. SUMMARY, *supra* note 12, at i.

131. *Id.* at i-ii.

> installing equipment to mitigate an EMP event is estimated at less than 20 cents per year for the average residential customer.[132]

With its unique responsibility and technical resources, the FERC's commissioners and technical staff have been called upon frequently to participate in review of electromagnetic threats in Congressional hearings, international summit discussions, cross-government assessments, and many other venues.[133]

In testimony to the House Homeland Security Committee,[134] Joseph McClelland, Director of the FERC's Office of Electric Reliability, said:

> In March 2010, Oak Ridge National Laboratory (Oak Ridge) and its subcontractor Metatech released a study that explored the vulnerability of the electric grid to EMP related events. This study was a joint effort contracted by FERC staff, the Department of Energy and the Department of Homeland Security and expanded on the information developed in other initiatives, including the EMP commission reports. The series of reports provided detailed technical background and outlined which sections of the power grid are most vulnerable, what equipment would be affected, and what damage could result. Protection concepts for each threat and additional methods for remediation were also included along with suggestions for mitigation. The results of the study support the general conclusion that EMP events pose substantial risk to equipment and operation of the Nation's power grid and under extreme conditions could result in major long term electrical outages. In fact, solar magnetic disturbances are inevitable with only the timing and magnitude subject to variability. The study assessed the 1921 solar storm, which has been termed a 1-in-100 year event, and applied it to today's power grid. The study concluded that such a storm could damage or destroy up to 300 bulk power system transformers, interrupting service to 130 million people for a period of years.[135]

The FERC's technical staff has also played an important role. For example, on April 30, 2012, the FERC held an important Staff Technical Conference on Geomagnetic Disturbances to the Bulk-Power System.[136] With an estimated $300 billion in new investment in the transmission system between 2010 and 2030,[137] the conference was intended to evaluate whether regulatory steps should be considered, as the energy sector sets out on this major area of investment. While testimony at the technical conference was wide ranging, there was broad agreement that there are timely steps that should be taken to address this issue. Joseph McClelland, speaking as moderator at the conference, summarized the urgency in an economic context. Even a short term, large area outage, he explained, would be very costly, using the estimated cost of the 2003 North East

---

132. *Id.* at i.

133. *See, e.g.*, EISS III LONDON REPORT, *supra* note 62, at 38.

134. *Hearing Before the H. Subcomm. on Emerging Threats, Cybersecurity, and Science and Technology*, 112th Cong. (Sept. 12, 2012) (testimony of Joseph McClelland, Director, Office of Electric Reliability, Federal Energy Regulatory Commission), *available at* http://www.ferc.gov/EventCalendar/Files/20120912103413-Testimony-McClelland.pdf.

135. *Id.* at 5.

136. Technical Conference Agenda: Staff Technical Conference on Geomagnetic Disturbances to the Bulk-Power System, FERC Docket No. AD12-13-000 (Apr. 20, 2012), *available at* http://www.ferc.gov/eventcalendar/Files/20120420162925-AD12-13-000a.pdf.

137. ELEC. INFRASTRUCTURE SEC. COUNCIL, SUMMARY AND HIGHLIGHTS: FERC GMD STAFF TECHNICAL CONFERENCE 3 (Apr. 30, 2012), *available at* http://www.eiscouncil.org/images/upload/media/FERC_Report.pdf.

blackout for comparison. "We could buy a lot of mitigation for $4-$10 Billion dollars, [the estimated cost of the 2003 North East blackout]," he said.[138]

In October 2012, the process that began with the FERC's studies in this area, and led to the technical conference, resulted in the FERC's publication of a Notice of Proposed Rulemaking addressing proposed, new GMD Reliability Standards.

> Under section 215 of the Federal Power Act, the Federal Energy Regulatory Commission (Commission) proposes to direct the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization, to submit for approval Reliability Standards that address the impact of geomagnetic disturbances (GMD) on the reliable operation of the Bulk-Power System.[139]

This notice called for a two phase standard setting process to address GMD.[140] In a first phase, within a ninety day period, NERC would be required to develop a standard for procedural measures for power grid protection.[141] In a second phase, within an additional ninety days, a second standard would be required, providing for automated measures to protect key power grid components and critical locations.[142]

This new, FERC-proposed process would, if implemented, provide the first North American Grid-wide standards for protection of the bulk power system against GMD threats.

a. The North American Electric Reliability Corporation

While not a U.S. government organization, NERC has been designated as the FERC's Electric Reliability Organization (ERO), responsible to implement federal regulations as they apply to the bulk power system, and the corporation has an important role in implementing regulation of the bulk power system.[143]

NERC has exhibited a range of views on both impact and mitigation approaches for electromagnetic threats. The findings of a major study they participated in, developed, and published in coordination with the Department of Energy, were similar to those of the full list of U.S. government studies summarized above.[144]

Although this is the only published NERC GMD study, the corporation recently published a "GMD Task Force Interim Report," a document arising from GMD task force discussions hosted by NERC.[145] This document, while

---

138. *Id.* at 5.

139. Notice of Proposed Rulemaking, *Reliability Standards for Geomagnetic Disturbances*, 141 F.E.R.C. ¶ 61,045 at P 1, 77 Fed. Reg. 64,935 (Oct. 24, 2012) (to be codified at 18 C.F.R. pt. 40).

140. *Id.*

141. *Id.*

142. *Id.*

143. *Understanding the Grid: Reliability Terminology*, N. AM. ELECTRIC RELIABILITY CORP., http://www.nerc.com/page.php?cid=1%7C15%7C122O (last visited Feb. 13, 2013).

144. HILF REPORT, *supra* note 5, at 54-56.

145. N. AM. ELEC. RELIABILITY CORP., 2012 SPECIAL RELIABILITY ASSESSMENT INTERIM REPORT: EFFECTS OF GEOMAGNETIC DISTURBANCES ON THE BULK POWER SYSTEM (2012), *available at* https://www.frcc.com/Public%20Awareness/Lists/Announcements/Attachments/105/GMD%20Interim%20Report.pdf.

identifying serious GIC-related risks to power grid stability, provides encouragement for a somewhat more hopeful scenario than the NERC/DOE study, asserting, "[t]he most likely worst-case system impacts from a severe GMD event and corresponding GIC flow is voltage instability caused by a significant loss of reactive power support simultaneous to a dramatic increase in reactive power demand."[146]

Such an impact would in itself, of course, be dangerous. Voltage instability leading to voltage collapse and a large regional blackout is clearly unacceptable to the power industry, to society, and to owners of critical assets with acute outage timelines, such as nuclear power generating stations and chemical plants.

The Nuclear Regulatory Commission (NRC), for example, recently responded to a petition raising concerns over a Severe Space Weather-induced scenario of "widespread, prolonged grid failure of sufficient magnitude that normal commercial infrastructure would not be available to resupply diesel fuel."[147] In their response, the NRC said the "scenario is sufficiently credible to require consideration of emergency planning and response capabilities under such circumstances," and the Commission now plans to evaluate these concerns.[148] The NRC indicated the primary concern is the duration of a large regional blackout that might prevent timely deliveries of emergency diesel fuel.[149]

What are those timelines?

> [I]f power from the electrical transmission system is not available, then safety-related backup power systems, typically powered by emergency diesel generators (EDG), are relied on for essential power to safely shutdown the reactor, mitigate accidents, and provide long-term cooling for the reactor core and fuel in the SFPs. These safety-related onsite EDGs are typically maintained with at least a 3 to 7-day supply of fuel and lubricating oil.[150]

"Blackstart" is a term used in the power industry to refer to the difficult process of restarting a large power grid region after a widespread power outage.[151] This is a gradual, time consuming process under the best of circumstances, and it is notable that there are indications the blackstart capability of the nation's restructured power industry has been systematically decaying.[152] Under these circumstances, any widespread power outage could involve unacceptable risk to critical assets with acute timelines.

Nevertheless, although even this "optimistic" voltage instability scenario could entail severe societal risks, upon careful review of the NERC GMD Task Force Interim Report supporting material was not found for what had appeared, on casual reading, to be a definitive assertion that this would be the probable

146. *Id.* at vi.

147. Petition for Rulemaking, Long-Term Cooling and Unattended Water Makeup of Spent Fuel Pools, 77 Fed. Reg. 74,788, 74,790 (Nuclear Regulatory Comm'n, Dec. 18, 2012) (to be codified at 10 C.F.R. pt. 50).

148. *Id.*

149. *Id.* at 74,797.

150. *Id.* at 74,789.

151. BRENDAN KIRBY & ERIC HIRST, MAINTAINING SYSTEM BLACKSTART IN COMPETITIVE BULK-POWER MARKETS (1999), *available at* http://www.consultkirby.com/files/Black_Start_-_APC_99.pdf.

152. *Id.*

outcome of a severe GMD event. According to task force participants, such an assertion would be "a significant departure from all previous drafts of the report and, indeed, from all previous U.S. Government studies."[153] In fact, NERC management itself has been careful to point out that it is premature to take the less catastrophic view implied by the reactive power loss / voltage instability scenario, recognizing that any such definitive conclusion would be premature.[154]

In that regard, speaking at the 2012 FERC GMD Staff Technical Conference, established shortly after the NERC GMD Task Force Interim Report was published, Gerry Cauley, NERC President and CEO, said, "[t]he NERC task force report points out two key risks, one for system disturbance and voltage collapse, and the other for potential equipment damage."[155] Although often characterized in definitive, optimistic terms in media articles, Mr. Cauley said "[t]he report did not claim grid hardware damage would be avoided by voltage collapse."[156] "I think there were some things said earlier in the first panel, about NERC's theory that voltage collapse will save the day. I don't recall seeing that. I don't think that was intended to be the implication of the NERC study."[157]

> I think what we're saying is that there are dueling concerns. The magnitude of a voltage collapse can be significant, as we saw in hydro Quebec, we also know there is evidence of equipment damage, but we need to put each in perspective in terms of what the information tells us, and the magnitudes of each of those two risks, supported by data and historical information.[158]

Characterizing the report as just a starting point, he said, "[t]he intent of the report was to put [twenty] recommendations on the table. I view it as a starting point and a roadmap. It is not the end of the road."[159]

In short, there is broad concurrence that the next Carrington-class Severe Space Weather event represents a serious risk to the nation's bulk power system and power grid. [160] As we have seen, while some power industry representatives have expressed the hope that damage to an unprotected power grid would be limited to voltage collapse, even those who have suggested the scenario are careful to point out that it does not represent their definitive conclusion. The scenario itself, which entails its own serious dangers, and substantial public risk and cost, is contradicted by the major U.S. and international technical studies and we have not found a technical basis for such an assessment.

When dealing with the infrastructure that has become society's life-support system, hoping that the heuristics of a GIC event will cause voltage collapse and

---

153. ELEC. INFRASTRUCTURE SEC. COUNCIL, GEOMAGNETIC DISTURBANCE TASKFORCE: INTERIM REPORT ASSESSMENT 3 (2012), *available at* http://www.eiscouncil.com/images/upload/media/GMDTF%20IRA.pdf.

154. *Id.* at 9.

155. ELEC. INFRASTRUCTURE SEC. COUNCIL, SUMMARY AND HIGHLIGHTS: FERC GMD STAFF TECHNICAL CONFERENCE 7 (2012), *available at* http://www.eiscouncil.com/images/upload/media/FERC_Report.pdf.

156. *Id.* at 7-8.

157. *Id.* at 8.

158. *Id.*

159. *Id.*

160. *See, e.g.*, OAK RIDGE EXEC. SUMMARY, *supra* note 12, at ii-iii.

a regional blackout, in such a way as to somehow prevent significant transformer damage, would represent neither good engineering design nor good public policy.

C. Allied Government Perspectives

As concerns began to grow over the potential vulnerability of rapidly evolving, vital societal infrastructures, most of the early government studies were carried out by U.S. government and public agencies. However, though the United States had a significant head start, these concerns have begun to spread among U.S. allies.

At the urging of concerned senior U.S. and U.K. government officials, the first of a new series of high level summit meetings took place on September 20, 2010.[161] Over the succeeding years, the Electric Infrastructure Security Summit Series has provided a new international infrastructure security framework for coordination and discussion of electromagnetic threats to critical societal infrastructures.[162] These summit events brought together senior administration, cabinet, and legislative officials from the United States, the United Kingdom, and other interested countries, with participation from Secretaries, Assistant Secretaries, and other senior managers from the U.S., the U.K., and other allied Defense, Energy, Security, and Regulatory Utility agencies.[163]

In the sections below we will review at top level some, but by no means all, of the international efforts on e-threat protection. In some cases, such as Israel, civil infrastructure protection efforts are taking place which we will not be able to describe here. Also to be left for another article, some of the world's largest countries are involved in a mix of both offensive EMP weapon development and critical infrastructure protection. In the material below, our primary focus will be to highlight some of the leading, current international efforts in power grid protection.

1. The United Kingdom

Outside the United States, the United Kingdom has become one of the leaders in evaluating e-threats. The U.K. Cabinet Office began working in 2010 to understand the potential impacts of electromagnetic disturbances on all the relevant agencies of government.[164] Since that time, concluding that these threats represent a potential for serious, dangerous impact on British society, the Cabinet Office has included Severe Space Weather in its annual National Risk Register of Civil Emergencies.[165] Looking at this issue as a cross-government problem that puts a number of different infrastructures at risk, the National Risk Register concluded,

---

161. EISS I LONDON REPORT, *supra* note 117.

162. *General Info*, THE ELEC. INFRASTRUCTURE SEC. SUMMIT, http://www.eissummit.com/ (last visited Feb. 14, 2013).

163. EISS I LONDON REPORT, *supra* note 117.

164. U.K. H.C. DEFENCE COMM. REPORT, *supra* note 29.

165. *Id.* at 7; CABINET OFFICE, NATIONAL RISK REGISTER OF CIVIL EMERGENCIES 2012, at 7 (U.K.) [hereinafter U.K. RISK REGISTER], *available at* https://update.cabinetoffice.gov.uk/sites/default/files/resources/CO_NationalRiskRegister_2012_acc.pdf.

> Severe space weather can cause disruption to a range of technologies and infrastructure, including communications systems, electronic circuits and power grids. The 'reasonable worst case' for a severe space weather event is based on the so-called Carrington Event in 1859, which saw some of the largest space weather phenomena ever recorded.[166]

This subject has also become the subject of hearings and evaluations by other U.K. government committees and agencies. For example, on February 8, 2012, the House of Commons Defence Committee, after evaluating extensive testimony, issued a special report, "Developing Threats: Electro-Magnetic Pulses (EMP), Tenth Report of Session 2010–12."[167]

In the introduction, referring to Severe Space Weather, the Committee points out,

> The risks posed by space weather are known and significant, though there is argument about the likely extent of their impact: a severe event could potentially have serious impacts upon UK infrastructure and society more widely. It is essential that this hazard is sufficiently recognised and addressed by the Government and relevant civil bodies.[168]

The Defence Committee also expressed serious concern about the potential risks of malicious EMP.

> However, certain states such as Iran could potentially pose a realistic threat in the future, even if it does not currently do so, if nuclear non-proliferation efforts are not successful. Non-state actors could also pose a threat. While the risk may at present be low, the potential impact of such a weapon could be devastating and long-lasting for UK infrastructure. The Government cannot therefore be complacent about this threat and must keep its assessment of the risk under review. It is therefore vitally important that the work of hardening UK infrastructure is begun now and carried out as a matter of urgency.[169]

The Defence Committee also identified non-nuclear EMP as an important concern. "While existing non-nuclear EMP devices may be crude and limited, the fact that viable devices could be produced by non-state actors is a cause for concern. Even localised damage could have the potential to disrupt activity, especially if combined with other forms of attack."[170]

2. Sweden

The combination of extreme northern latitude and a highly developed, power-grid dependent culture has made Sweden one of the first countries to recognize the importance of space weather. Much of the work on Severe Space Weather going on in Sweden is taking place at the Swedish Institute of Space Physics in Lund, and the Institute, summarizing this long history, notes that,

166. U.K. RISK REGISTER, *supra* note 165, at 7.

167. U.K. H.C. DEFENCE COMM. REPORT, *supra* note 29.

168. *Id.* at 3.

169. *Id.*

170. *Id.*

"Effects of GICs on electrical systems have been reported in Sweden since early 1900."[171]

Illustrating Sweden's awareness and concern over e-threats, Mikael Odenberg, CEO of the National Electric Grid and former Defense Minister of Sweden, speaking at Electric Infrastructure Security Summit II in Washington D.C., offered some historical perspective on this evolving concern.[172] "EMP has been known since 1945, common knowledge since the 1950s. And we had a severe geomagnetic storm hit in the northern hemisphere 150 years ago . . . " he said.[173] "So the new thing is not the EMP. The new thing is not the space weather. The new thing is the vulnerability of modern society."[174]

Mr. Odenberg made Sweden's interest in cooperating to address this threat clear. "[T]o my mind," he said, "there are few emergency scenarios today that require such a gross cooperation as this, which are threatening our electric infrastructure: large serious space weather situation, and electromagnetic pulse."[175]

3. South Africa

Classical CME events create their highest level GIC at high northern latitudes, where the earth's magnetic field is strongest. However, rather surprisingly, since it would not normally be considered at high risk for geomagnetic storm effects, South Africa, a low latitude country, experienced a remarkable series of EHV transformer failures following the geomagnetic "Halloween Storm" of 2003.[176] Fifteen transformers, about 13% of Eskom's EHV transformer fleet, were destroyed.[177] Following investigation by corporate staff, it was concluded that GIC effects were a primary cause.[178]

> A close association has been identified between the theoretical calculation of geomagnetically induced currents (GICs) in a large network, practical measurements of GICs, the results of dissolved gas analysis (DGA) records, and damage in recently failed transformers in Southern Africa. Together these indicate that GICs may contribute significantly to transformer failures on large transmission systems in mid-latitude regions, where GICs are generally thought not to be significant.[179]

This concern was also evident from other events, based on GIC monitors installed at Eskom.

---

171. *Solar Activity and GIC Effects in Sweden*, SWEDISH INST. OF SPACE PHYSICS, http://www.lund.irf.se/HeliosHome/solaractivitygic.html (last visited Feb. 17, 2013).

172. EISS II WASHINGTON REPORT, *supra* note 117, at 9.

173. *Id.*

174. *Id.*

175. *Id.*

176. C. T. Gaunt & G. Coetzee, *Transformer Failures in Regions Incorrectly Considered to Have Low GIC-Risk* 1, 3 (2007) (Presented at the Institute of Electrical and Electronics Engineers Powertech 2007 Conference), *available at* http://www.labplan.ufsc.br/congressos/powertech07/papers/445.pdf.

177. EISS II WASHINGTON REPORT, *supra* note 117, at 12.

178. Gaunt & Coetzee, *supra* note 176, at 6.

179. *Id.* at 1 (Abstract).

> During the strong storm of 31 March 2001 a GIC of only 6 Ampere caused a sixth harmonic in the neutral (which indicates transformer saturation) peaking at 13 Amps. This occurred while the transformer was only utilized at less than 60% of its rated value. This indicates that reactors which are operated much closer to their full rated value could easily saturate and thus be damaged by low levels of GICs.[180]

It is important to note that this level of reactive power did not cause the grid to collapse, thereby saving the transformers from damage.

4. South Korea

In its continuing conflict with North Korea, South Korea has been sensitive to periodic reports of North Korean EMP capability. Beginning with the Congressional EMP Commission's Executive Summary,[181] and later responding to other indications of North Korean interest in EMP, South Korea started its own program, focused on developing robust, IEMI or non-nuclear EMP weapons.[182]

"'We've already developed the technology to create EMPs capable of neutralizing targets within a 100m radius,' an ADD official" told *The Korea Times*.[183] "'The development of an EMP bomb with a range of 1km will be finished by that time.'"[184]

IV. THE INSURANCE SECTOR: A BUSINESS RISK PERSPECTIVE

In recent years, concern over increasing vulnerability of basic societal infrastructures has led a number of private, public, and corporate institutions to perform their own risk assessment. As the business sector most directly concerned with risk-based costs to potential large scale, catastrophic events, the insurance industry has taken a leading role in private sector research into Severe Space Weather.

Working in over 200 countries and territories, Lloyd's, considered to be the world's leading specialist insurance market, "is often the first to insure new, unusual or complex risks."[185] In this regard, Lloyd's published one of the most important recent studies on space weather, and its implications for business sectors.[186]

In the introduction to this detailed study, Lloyd's discusses the issue, the scope of the risk and its potential impact and, based on the study's assessment of

180. J. KOEN & C.T. GAUNT, GEOMAGNETICALLY INDUCED CURRENTS IN THE SOUTHERN AFRICAN POWER NETWORK 5 (2001), *available at* http://web.uct.ac.za/staff/gaunt/CigreSA2001Koen.pdf.

181. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24.

182. Jung Sung-ki, *S. Korea to Develop EMP Bomb by 2014*, THE KOREA TIMES (July 7, 2009), http://www.koreatimes.co.kr/www/news/nation/2009/09/205_48084.html.

183. *Id.* (quoting an unnamed Agency for Defense Development (ADD) official).

184. *Id.* (quoting an unnamed ADD official).

185. MIKE HAPGOOD, RAL SPACE, LLOYD'S 360° RISK INSIGHT BRIEFING, SPACE WEATHER: IT'S IMPACT ON EARTH AND IMPLICATIONS FOR BUSINESS (2010) [hereinafter LLOYD'S 360°], *available at* http://www.stfc.ac.uk/Resources/pdf/7311_Lloyds_360_SpaceWeather_03.pdf.

186. *Id.* at 2.

historical data and projected future risk, recommends that businesses begin planning for the potential long term risks associated with space weather.[187]

"Space weather describes disturbances that occur in near-Earth space, which can disrupt modern technologies. It is a natural hazard to which human civilization has become vulnerable, through our use of advanced technologies. Businesses are exposed to these new risks . . . ."[188]

"Awareness . . . is patchy and is usually raised after problems have occurred, rather than through a systematic approach that anticipates problems and reduces costs through early and well-targeted mitigation measures."[189]

> [A] space weather event could have wider regional and even global impacts: by triggering cascading failures across systems. A key example of this dependency is our reliance on secure electric power. Space weather can (and has) caused significant disruption to supplies on regional scales and could affect national systems over extended periods of time.[190]
>
> Businesses at risk [of major disturbances] from space weather need to plan how they will respond to that risk . . . . It is dangerous to base risk assessment on short-term experience as that may be during periods of mild conditions. Between 2006 and 2010 there has been the lowest level of space weather activity for nearly 100 years. There is also much historical evidence suggesting that severe space weather events have been unusually rare over the past 50 years, and there are concerns that we will see more frequent events in the coming decades.[191]

Lloyd's is not alone, in the insurance and re-insurance sector, in its concerns over space weather. Allianz, Swiss Re, and Zurich have all been involved in their own research and analysis of space weather risks.

Allianz, in a published summary of their assessment, echoed some of the concerns that appeared in the Lloyd's report.

> Our highly technological world is particularly exposed to the electromagnetic effects of space weather. Each solar storm, for example, generates intensive showers of particles and gigantic currents in the ionosphere which induce major alterations in the geomagnetic field. Electric conductors in the changing magnetic field, whether cables, pipes or seawater, run currents called 'geomagnetically induced currents,' or GICs.[192]

"The effects on electrical infrastructure can be profound."[193] "[C]ritical infrastructures, whether they be power generation, telecoms, finance, fuel, food or water, are becoming ever more dependent on electricity and electronics."[194]

Zurich's report reflects similar concerns.

---

187. *Id.* at 5.

188. *Id.*

189. *Id.*

190. *Id.*

191. *Id.*

192. Dr. Rudolf Kreutzer, *Space Weather*, ALLIANZ: GLOBAL RISK DIALOGUE, Spring 2009, at 12, *available at* http://www.agcs.allianz.com/assets/PDFs/GRD/GRD%20individual%20articles/GRD-2009-01-SpaceWeather.pdf.

193. *Id.*

194. *Id.* at 16.

> Compared to disruption of the electrical grid from natural hazards and other sources, GIC related damage and disruption to the power distribution grid has the potential to have a very broad footprint across a large region for an extended period. . . . Such an event does not have any precedence for comparison for the potential severity of impact. It can be considered an unrecognized catastrophic risk due to our increased reliance on technology today.[195]

In a report self-described as "the result of extensive investigations and discussions with may representatives from different sectors," the authors of a Swiss Re report reach a conclusion very similar to the many other studies evaluating space weather concerns.[196] Referring to potential transformer damage due to GIC, the report points out, "[w]hen, in particular, power is demanded from the system, failures may occur in the system and, ultimately, complete blackout."[197]

"In a saturated transformer, the magnetic flux rises to values for which it is not designed. In the worst instance, it may result in fire and the destruction of the transformer."[198]

In the preface of Swiss Re's report, a question is asked that may summarize one of the issues facing the insurance sector: "Are insurance covers, which are mainly limited to sudden and accidental damage, more heavily exposed than before, or less – given the new knowledge about space weather and the possibilities for dealing with it?"[199]

As the many insurance company studies themselves point out, if at least minimal mitigation measures are not taken, this question is likely to be overtaken by a wide range of impacts. Cascading failures could cause serious damage to the critical infrastructures which form much of the foundation of modern societies.

V. OPTIONS FOR PROTECTING THE NATIONAL POWER GRID

Successfully addressing serious societal risks always means striking a balance in a number of dimensions.

What is the proper venue or domain for addressing the risk? If mitigation measures are expensive, are the issues understood well enough to focus limited resources appropriately? To what extent does risk mitigation require an integrated or regulated approach, or can these risks be addressed on a voluntary basis? Are there reasonable mitigation measures available, and is the cost of these measures reasonable and commensurate with the probability and projected cost impact of the risk? Before acting, what level of confidence is needed in understanding potential new risks introduced by the mitigation measures?

---

195. A.V. RISWADKAR & BUDDY DOBBINS, ZURICH, SOLAR STORMS: PROTECTING YOUR OPERATIONS AGAINST THE SUN'S 'DARK SIDE' (2010), *available at* http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/media/solarstorms.pdf.

196. FRANK JANSEN & RISTO PRIJOLA, SWISS RE, SPACE WEATHER: HAZARD TO THE EARTH? 4 (2000), *available at* http://media.swissre.com/documents/pub_space_weather_en.pdf.

197. *Id.* at 25-26.

198. *Id.* at 26.

199. *Id.* at 4.

Addressing e-threat risks in an optimal fashion, as for any other serious societal risks, requires at least a top level effort to find a reasonable balance for each of the dimensions raised by these questions. In this section, we will attempt to provide some top level thoughts in addressing these and related questions.

A. Regulatory Considerations, Options, and Current Status

1. Considerations and Options

It is always tempting, when confronting an issue, to define it as "someone else's problem." The first question that must, therefore, be answered is the "venue question": Where should the issue be addressed?

In the case of e-threats, the answer emerges from an understanding of the nature of the risk. For example, whenever the government cannot somehow prevent or deter a serious societal threat, protection of a critical infrastructure can only take place "where the rubber meets the road," by hardening that infrastructure. Given this, we can restate the question: Is it possible, with adequate confidence, for the government to prevent the threats from happening?

For space weather, of course, this is not really a question. When, as in 1859 and 1921, severe coronal mass ejections head toward the earth, there is no way to prevent their arrival.

For malicious e-threats, the question can be expressed more directly: Given the likely catastrophic consequences, can the nation's defense and security agencies be expected to prevent any EMP attack, either IEMI or HEMP, on the power grid?

For IEMI this would mean near perfect confidence in preventing any malicious use of hand-made or purchased "EMP suitcase" devices, decommissioned ship radars or other, similar systems. For HEMP, it would mean, for example, that the government would assure deterrence of any rogue state or terrorist organization from bringing a freighter with a hidden nuclear-equipped SCUD missile within several hundred miles of the U.S. coastline.

As the Congressional EMP Commission concluded, after receiving testimony from DOD and all other relevant U.S. government agencies,

> What is different now is that some potential sources of EMP threats are difficult to deter—they can be terrorist groups that have no state identity, have only one or a few weapons, and are motivated to attack the US without regard for their own safety. Rogue states, such as North Korea and Iran, may also be developing the capability to pose an EMP threat to the United States, and may also be unpredictable and difficult to deter.[200]

For both Severe Space Weather and EMP, there seems to be little choice. The federal government has made it clear that it cannot assure deterrence of an EMP attack, and the sun, in terms of Severe Space Weather, is unlikely to be deterred. Since there can be no high-confidence basis for assuring these events will always be prevented, e-threat protection of the power grid can be effectively implemented only within that system.

---

200. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at 2.

a. The Analysis vs. Implementation Tradeoff

In confronting serious predicted risks, once the "protection venue" is defined it becomes important to properly focus limited resources. To optimize this investment, finding an optimum balance between expanding risk analysis, and starting efforts to enhance resilience, is a priority.

This decision is almost always a question of cost and complexity. If resilience – risk mitigation – is likely to be complex and expensive, but a precise understanding of that risk is quick, straightforward, and cheap, it makes sense to focus on modeling and analysis to minimize the resilience / mitigation investment. On the other hand if improved precision in understanding the risk will be complex and expensive but resilience is comparatively cheap, most of the effort should go toward implementing resilience. This may be especially true if the resilience helps enhance reliability in other areas.

i. Where does the balance lie for e-threats?

For HEMP or IEMI, vulnerability assessment and threat scenarios projection are both complex subjects, making precision modeling nearly impossible. On the other hand, though the E1 footprint may be huge, within that area only a portion of exposed hardware will be damaged, and E1 protection experts almost invariably recommend the economically conservative strategy of planning for post-event recovery.[201] Prioritized resilience measures can be relatively minimal, ranging from retrofitting critical relays and SCADA controllers to acquisition – and appropriate deployment – of adequate spares. In the case of home-mounted smart meters, contingency procedures could be prepared to assure power is not interrupted.

Thus, for E1, these considerations suggest it may be advantageous to look toward phased E1 resilience measures as a priority, rather than complex and uncertain analysis.

For both Severe Space Weather and EMP E3, enhanced space weather threat analysis and expanded transformer vulnerability assessment will not be quick, straightforward, or cheap. Scientists today are far from achieving a comprehensive theoretical model of the physics of the sun, and a highly divergent transformer fleet means a wide variety in design and damage mechanism. A full inventory of the transformer fleet with as-built assessment and detailed finite element thermal and magnetic susceptibility modeling for each transformer also fail the test of quick, straightforward, or cheap.

If modeling is complex and expensive, the other end of the balance scale is resilience, and there are generally two approaches: procedural protection, and automated, hardware-based protection. Neither approach appears costly.[202]

---

201. Private communication with Davidson A. Scott, P.E., EMP/EMI Consultant to the Defense Department and power corporations; *see also*, EMP COMM'N 2008 REPORT, *supra* note 1, at 47, 54-61.

202. *Threat Posed by Electromagnetic Pulse (EMP) Attack: Hearing Before the H. Armed Services Comm.*, 110th Cong. 2 (July 10, 2008) (statement of Dr. William Graham, Chairman, Comm'n to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack), *available at* http://www.empcommission.org/docs/GRAHAMtestimony10JULY2008.pdf (noting that "It is the consensus of the EMP Commission that the Nation need not be vulnerable to catastrophic consequences of an EMP attack. . . . [T]he Nation's vulnerability to EMP that gives rise to potentially large-scale, long-term

Developing good procedures is a well-practiced, fundamental responsibility of power grid operators: adding an additional procedure is unlikely to be complex. And with only several hundred to one thousand vulnerable EHV transformers, it is difficult to generate high estimates for automated hardware protection, even in the unlikely scenario of uniform, 100% protection.

This would suggest that the proper balance between resilience and modeling may tilt toward the former. However, this conclusion depends on two embedded assumptions: availability, and effectiveness or risk.

To some degree, these assumptions may already be validated. Hardware mitigation measures have been in use for years in some locations in the United States and Canada, primarily series capacitors on long distribution lines.[203] But other, cheaper alternatives like transformer neutral current blockers, though they are generally lower cost, are also more novel, with much more limited test data and grid experience,[204] leaving questions of effectiveness and potential grid performance risks open.

ii. Where does this leave us?

Given the immaturity of solar physics and the complexity of inventory assessment and detailed modeling for the nation's transformer fleet, the question may no longer be "analysis vs. implementation," but rather what, exactly, is the best path toward implementation? While additional modeling and information gathering will always play a role, it may make more sense, as President Obama has suggested,[205] to take concrete steps toward risk mitigation, and resilience. What, however, should those steps be? What is the best mix of procedural and hardware mitigation, and what is the optimum mix of mature hardware approaches (e.g., series compensation) and more novel, potentially cheaper alternatives (e.g., neutral current blockers)?

If the President's guidance is correct, it may be time to consider adjusting the focus: to prioritize development of a full set of questions on series capacitance, current blocker performance, and other resilience measures – to begin defining the questions whose answers will help the energy sector make intelligent decisions on cost effective resilience investments.

b. Setting the Balance: Regulatory Control vs. Voluntary Measures

With any critical infrastructure, lawmakers and regulatory officials face difficult decisions on finding a good balance between regulation and market forces. What does this look like for the nation's power grid?

---

consequences can be reasonably reduced below the level of a potentially catastrophic national problem by coordinated and focused effort between the private and public sectors of our country. The cost for such improved security in the next 3 to 5 years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures threatened.").

203. R. Wamkeue, N. Kandil, J. East, & Y. Boisclair, *Series Compensation for a Hydro-Quebec Long Distribution Line* (2003) (Presented at the 2003 International Conference on Renewable Energies and Power Quality), http://www.icrepq.com/pdfs/WAMKEUE301.pdf.

204. *See, e.g.*, N. AM. ELEC. RELIABILITY CORP., GEOMAGNETIC INDUCED CURRENT (GIC) MITIGATION SYSTEM SUMMARY FOR THE WHITE PAPER, *available at* http://www.nerc.com/docs/pc/gmdtf/NERC%20Mitigation%20System%20Summary%20for%20White%20Paper%20-%20Final.pdf.

205. Showstack, *supra* note 100, at 235.

Market forces, like their physical analogues, operate by causing movement and change. When a negative change drives the market out of some optimum range it causes pain, and gives a competitive advantage to a corporation that works to remove that pain. This process, however, *starts* with that negative change. When dealing with a *predicted* crisis, market forces cannot begin to work until *after* the crisis has hit. And if the pain is bad enough, that may be too late – the market may never recover. Dealing with unusual, predicted crises, like severe e-threats, is thus a legitimate regulatory role.

This can be even more important if, for some structural reason, the market is unable to respond properly, even after the crisis. And this is also a feature of e-threats, where the impact to the power grid is an aggregate effect. Divergent, uncoordinated mitigation efforts by different power companies could, in some cases, actually worsen the problem, especially if it inadvertently shifts a problem from a low-impact zone in the power grid into a sensitive, critical node. Coordination will be a priority.

For both of these reasons, government leadership will likely be important, and a mix of DOE leadership and the efforts of regulatory structures like the FERC will likely be needed to help fill both of these roles. The scope of those roles could, of course, vary depending on demonstrated interest by the commercial sector in taking voluntary steps toward e-threat resilience.

2. Current Status

As indicated above, the level of regulatory involvement in addressing e-threats is likely to be responsive, as is often the case, to the level of voluntary energy sector initiatives. In the case of e-threat protection, that would mean dedicated, proactive efforts on the part of the corporate energy sector, especially given the inter-corporate coordination efforts that are a unique requirement of GMD mitigation.[206] Thus far however, more than eight years after publication of the first major government report on e-threats[207] and two years after the NASA / NAS Severe Space Weather Study[208] and the FERC / DOE / DHS e-threat report,[209] the commercial energy sector has been slow to respond.

Nevertheless, a small but important group of U.S. power companies have begun taking serious, independent steps to secure their portions of the power grid against e-threats. In several cases, large power companies like CenterPoint Energy in Texas and American Electric Power in Ohio have shown vigorous leadership in researching the issues, and in taking prudent steps to ensure new capital and facilities investments are protected against both natural and malicious electromagnetic threats.[210]

206. *See also* Section 2.a.i, *infra* for a more detailed explanation.

207. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24.

208. NASA/NAS STUDY, *supra* note 26.

209. OAK RIDGE NAT'L LAB STUDY, *supra* note 14.

210. *See, e.g.*, *EnergyInSight: A Smart Grid Vision for the Next Generation*, CENTERPOINT ENERGY (2011), http://www.centerpointelectric.com/staticfiles/CNP/Common/SiteAssets/doc/92617%20energy %20insight%20brochure.pdf (highlighting CenterPoint's investment in various new technologies relating to an intelligent grid). Scott Moore, Vice President of Transmission for American Electric Power was a Chair for the High-Impact Low-Frequency Event Steering Committee. HILF REPORT, *supra* note 5.

a. The FERC GMD Notice of Proposed Rulemaking (NOPR)

In regard to the two general areas of concern for e-threat protection, EMP and GMD, the FERC has taken initial steps toward defining a regulatory process to address the latter.

On October 18, 2012, the FERC issued a NOPR on a proposed rule to direct NERC to develop GMD Reliability Standards for the bulk power system.[211] In the NOPR, the FERC calls for both operational procedures and an assessment of approaches to "automatically block geomagnetically induced currents."[212] The NOPR also called for updated GMD withstand standards for transformers and other vulnerable equipment.[213]

With this notice, the FERC is actually responding to several different dimensions of concern that fit the organization's federal mandate.

- Resilience to prevent a potential severe, long term regional blackout: The FERC's core responsibilities include issues, like GMD, that could affect a large segment of the power grid, involving equipment owned and operated by many different corporations.
- National security issues: With both defense critical infrastructures and other vital national assets dependent on secure, continuous power, a wide area, long term blackout becomes a national security issue, which is properly addressed by the federal government.
- Successful grid protection requires interconnect-wide resilience coordination: Individual power companies are unlikely to spontaneously invest in resilience or risk mitigation, since the grid will still go down if most of their colleagues don't spontaneously decide to do the same. In fact, local, haphazard protection of random grid regions can actually worsen the problem, potentially shunting large DC currents from a low-vulnerability protected zone into a critical high vulnerability area. A regulatory process provides one approach to the requisite, grid-wide modeling and coordination.

In laying the notice out in two phases, the FERC apparently recognizes that GMD protection will be a process, not a singular event. Procedural changes, generally inexpensive to prepare, are seen as the first, fairly straightforward step.[214] Automated protection, while far more robust and essential for a really large storm, will take longer to implement.[215] But in both phases the NOPR calls for owners and operators to periodically conduct their own vulnerability assessments for transformers and secondary equipment against standards that reflect uniform evaluation criteria.[216]

Depending on how this approach is implemented in a standard, the intent appears to be to recognize the need for flexibility to address unique variations in

211. Notice of Proposed Rulemaking, *Reliability Standards for Geomagnetic Disturbances*, 141 F.E.R.C. ¶ 61,045 at P 1, 77 Fed. Reg. 64,935 (Oct. 24, 2012) (to be codified at 18 C.F.R. pt. 40).

212. *Id.* at P 1.

213. *Id.* at P 32.

214. *Id.* at P 8.

215. *Id.* at P 23.

216. *Id.* at PP 27-32.

appropriate standards or standard application, associated with unique differences in equipment, configuration, geography,[217] and national asset criticality, as well as variation over time.

i. Summary

The FERC's approach appears to reflect both recognition of its federal mandate to protect the security and continuity of the nation's bulk power system, and sensitivity to the need for a process that can account for different conditions, rather than an oversimplified, arbitrary process. Depending on implementation, this approach could be effective in building GMD protection into the power grid. The test will come, of course, in developing standards and processes that assure effective protection, while properly responding to varying realities and needs among different corporate providers in the energy marketplace.

Whether or not this regulatory approach is adopted, achieving GMD protection for the power grid is likely to mean substantially raising the bar on internal coordination among energy corporations. In the absence of a FERC-NERC regulatory process, this would mean development, and full empowerment, of a freely accepted industry-defined surrogate institution or process to drive grid-wide modeling and coordination, including coordination with the government to protect key national security objectives. To some extent, this could end up looking rather like a special-case, redundant FERC-NERC process.

b. The National Association of Regulatory Utility Commissioners' (NARUC) GMD Resolution

At its 2011 Summer Committee Meetings in Los Angeles, California, the National Association of Regulatory Utility Commissioners (NARUC) passed a resolution "Supporting Protection of Utility Infrastructure Against Electromagnetic Pulse Effects."[218]

The resolution summarized conclusions arising from the many recent government and public agency studies on the national power grid's vulnerability to natural or malicious electromagnetic threats.

"EMP events occur with little or no warning and can have catastrophic effects, including causing outages to major portions of the U.S. power grid possibly lasting for months or longer" the resolution said, referring to periodic severe solar events, HEMP, and IEMI.[219]

> EMP threats have the potential to cause wide-scale, long-term losses with economic costs to the United States that vary with the magnitude of the event but the cost of

217. Rasmus Thorberg, Risk Analysis of Geomagnetically Induced Currents in Power Systems, 21 (2012) (unpublished Master thesis, Lund University), *available at* http://www.iea.lth.se/publications/MS-Theses/Full%20document/5296_full_document_GIC.pdf (discussing latitude, ground composition/ conductivity, and other geographic features can affect local GIC levels).

218. COMM. ON CRITICAL INFRASTRUCTURE, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, RESOLUTION SUPPORTING PROTECTION OF UTILITY INFRASTRUCTURE AGAINST ELECTROMAGNETIC PULSE EFFECTS (2011), *available at* http://www.naruc.org/Resolutions/Resolution%20Supporting%20Protection%20of%20Utility%20Infrastructure%20against%20EMPs.pdf.

219. *Id.* at 1.

> damage from the most extreme solar event has been estimated at $1 to $2 trillion with a recovery time of four to [ten] years, while the average yearly cost of installing equipment to mitigate an EMP event is estimated at less than 20 cents per year for the average residential customer. . . .[220]

Referring to relevant member jurisdiction and responsibilities, the NARUC "recognizes the necessity for the electric grid to be highly resilient to severe space weather and EMP, as defined by the twin goals of non-catastrophic failure and rapid recovery."[221] The resolution also recommends that member states "open dialogues with the utilities that they regulate and with regional transmission organizations that serve their jurisdictions to understand the measures currently undertaken to address this threat. . . ."[222]

The resolution continues by calling for member states to work on expanding e-threat risk assessment best practices, and recognizes the need for investment that "may include design features rendering infrastructure less susceptible to the threat of damage from severe space weather and EMP. . . ."[223] It concludes by advocating federal investment to define hardening requirements, and cost/benefit analysis for the national power grid.

B. Technical Approaches

While it is not the objective of this article to describe detailed e-threat mitigation approaches, a general understanding of the subject is important to provide a sense for the cost and complexity of power grid hardening.

Mitigation measures may generally be defined in two categories: protection against HEMP E1 or IEMI, and protection against Severe Space Weather or HEMP E3.

1. Integrated, Prioritized Power Grid Protection Planning

Given the integrated nature and highly interdependent behavior of modern power grids, the first step in protection of the power grid is development of an overall milestone-driven e-threat grid protection plan. Such a plan would define different protection priorities to different grid nodes or facilities, based on the functional importance of a facility to societal and customer needs, and to power grid continuity and restoration.

While not going into extreme detail, such a plan would drive down to a regional or facility level, providing clearly stated top level requirements or objectives for each region or facility, with these priorities embedded in a time-ordered milestone plan designed to ensure that interim regional measures do not inadvertently temporarily worsen threat sensitivities at key facilities. These requirements will typically be multi-valued, and a particular facility, or a key element of the facility, may be specified at different protection priority levels for different equipment categories.

---

220. *Id.*
221. *Id.* at 2.
222. *Id.*
223. *Id.* at 2-3.

To review these options and to help frame e-threat dialogue more broadly, it may be helpful to define three levels of protection:

- Level I: Comprehensive protection. Best possible protection, intended to allow uninterrupted operation of a facility through an e-threat event.
- Level II: Rapid Recovery. Moderate protection, with facilities designed to allow rapid recovery of normal operation after an e-threat event.
- Level III: Gradual Recovery. Minimal protection, with few facility enhancements, but with pre-planned and properly resourced procedural recovery plans.

In the current situation, with little or no e-threat protection available for the vast majority of the power grid, a likely initial approach would be to ensure that most or all grid facilities meet Level III protection standards, allowing for gradual recovery. In parallel, focused efforts could be defined to bring critical nodes and facilities to Level I or Level II conditions.

2. Severe Space Weather GMD or HEMP E3 Protection

Severe Space Weather-caused GMD and HEMP E3 both can cause very large GICs to flow through the bulk power system. The primary difference relates to warning time.

If adequate satellite-based sensors continue to be available, there should be between minutes and hours of warning time of a potential severe GMD event. Of course, due to limitations in our understanding of how any particular Coronal Mass Ejection (CME) interactions will manifest regionally, such warnings cannot reliably predict whether a large CME will definitely result in large GICs in the North American power grid. But with HEMP E3, there may be little or no warning.

In both cases, however, power grid vulnerabilities and protective measures are essentially identical. Brief, high GIC levels can saturate transformer cores, forcing AC-related flux into transformer windings and support structures not designed for these high fluxes, causing local heating that can damage or destroy the transformer.[224] If GIC levels are higher than AC currents, circuit breaker operation could also be affected, potentially tripping some transformers and causing increased GIC flows into others.

Unlike HEMP however, GMD events can sometimes cause longer duration, lower GIC levels, which can also damage transformers, with degradation potentially taking longer to manifest, over a period of weeks, for example, rather than minutes or hours.

a. GIC Protection Strategies

i. Level III GIC protection

For low level space weather events, the U.S. bulk power system already uses procedural approaches for protection, primarily strategies for unloading some of the most heavily-saturated transformers, reducing power generation at nuclear power plants, for example, while replacing the needed energy by

224. HILF REPORT, *supra* note 5, at 70.

increasing generation at other, more expensive and less vulnerable facilities.[225] For moderate level space weather events, there may be additional procedural approaches which can add resilience to the power grid. Such approaches, generally consistent with a "Level III, Gradual Recovery" approach, would depend on special, highly transportable replacement transformers, such as the "Recovery Transformers" recently tested in a special DOE project, working with CenterPoint Energy in Texas.[226]

ii. Level I and II GIC protection

For Severe Space Weather events and HEMP however, the potential scale of the problem, and the number of affected transformers, would make automated approaches a priority. Corresponding to a Level I or Level II protection, such automated measures would involve pre-designed and installed, automated hardware approaches to block GIC from entering transformers.

One approach to automated protection – depending on GIC detection to de-energize transformers – turns out to be problematic, since existing transformer differential protection approaches actually inhibit relay operation under half-cycle saturation.[227]

Another approach is simply to prevent GIC from entering the transformer in the first place. Using series capacitors in long high voltage lines is one method, successfully in use in Quebec, installed in response to the March 1989 GIC-induced province-wide blackout.[228] Alternatively, GIC current blockers may be installed on the neutrals of EHV transformers, using low Ohm resistors or low voltage capacitor systems. Designs for this latter approach are now available, with one design, ABB's "Solid Ground," having recently completed prototype testing.[229]

While the costs for such automated approaches appear to be modest in comparison with the transformers protected, two considerations will need to be addressed.

- Automated protection placement guidelines: While blocking GIC can protect an individual transformer, it will be important to ensure that such

225. *Id.* at 100.

226. Memorandum from Patricia A. Hoffman, Assistant Sec'y, Office of Elec. Delivery and Energy Reliability on DOE Responses to EAC Work Products to Dep't of Energy Elec. Advisory Comm. (Mar. 2, 2012), *available at* http://energy.gov/sites/prod/files/DOE%20Response%20to%20EAC%20Recommendations%20-%20March%202012.pdf.

227. Russell Neal, William Radasky & John G. Kappenman, *Developing an Actionable EMP/GMD Hardening Program for an Electric Utility, in* IEEE PES GENERAL MEETING: THE ELECTRIFICATION OF TRANSPORTATION & THE GRID OF THE FUTURE 6 (2011) (subscription service), *available at* http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6039153&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6039153.

228. JOHN KAPPENMAN, METATECH CORP., META-R-322, LOW-FREQUENCY PROTECTION CONCEPTS FOR THE ELEC. POWER GRID: GEOMAGNETICALLY INDUCED CURRENT (GIC) AND E3 HEMP MITIGATION 3-1 (Jan. 2010) [hereinafter KAPPENMAN META-R-322], *available at* http://www.ornl.gov/sci/ees/etsd/pes/pubs/ferc_Meta-R-322.pdf (This report is part of the Oak Ridge National Laboratory Study. OAK RIDGE NAT'L LAB STUDY, *supra* note 14).

229. ABB, SOLIDGROUND™ GRID STABILITY SYSTEM: GEOMAGNETIC STORM INDUCED CURRENTS (GIC) AND ELECTROMAGNETIC PULSE (EMP) E3 PROTECTION 3 (2012), http://www05.abb.com/global/scot/scot245.nsf/veritydisplay/295f5a60dd37af99c12579db00542603/$file/SolidGround_2GNM110098.pdf.

protection fits into an appropriate overall plan, to avoid inadvertent transfer of GIC to neighboring, potentially more vulnerable or more important transformers.

- Automated protection performance evaluation: Of the two dominant methods available to power system engineers, one, use of series capacitance on long high voltage lines, is already in use in Quebec, California, and elsewhere.[230] The other, which may have cost and implementation advantages, is use of GIC current blockers. This technology is relatively new, and although at least one candidate system recently successfully went through a series of tests by Idaho National Laboratory, widespread use by the power industry will mandate careful review of those test results.[231] Given the potential utility of this new, automated approach, it will be crucial for power company engineers to define a complete set of risks and concerns with this technology, to allow development of any additional testing and validation.

3. HEMP E1 and IEMI Protection

The primary concern for these high frequency pulse effects is damage or destruction of low voltage electronics, including SCADA controllers, relays, Master and Remote Terminal Units (MTUs and RTUs), and other control and switching center computer hardware.

a. Level III: Gradual Recovery

Level III protection would largely call for defining vulnerable components and systems, and ensuring (a) availability of adequate spares, and (b) well-defined procedures, and associated training, for post-event recovery efforts. An IEMI or even an HEMP E1 event damages only a fraction of exposed equipment. Given this, and the relatively low cost of vulnerable equipment, costs for Level III IEMI / E1 protection are expected to be minimal.

b. Level II: Rapid Recovery

Level II protection, for a limited selection of power grid facilities, would generally include some elements of Level I protection, but would largely be an upgraded version of Level III. For example, a primary difference would be pre-positioning of spares in switching or control stations, along with procedures for switching over from primary to backup / spared components at such stations.

c. Level I: Comprehensive Protection

Level I protection would be designated for critical facilities and nodes, to allow for continuous operation through an e-threat event, or for minimal interruptions. While including Level II and Level III measures, facilities designated for this level of protection would include a variety of additional

230. KAPPENMAN META-R-322, *supra* note 228, at 3-1, 3-4.

231. *Grid Stability System Undergoes Live Grid Testing by Defense Threat Reduction Agency*, TRANSMISSION & DISTRIBUTION WORLD (Oct. 2, 2012), http://tdworld.com/go-grid-optimization/asset-management-service/emprimus-solid-ground-0912/.

measures. These could include shielding enhancements by additions to facility buildings such as, for example, installation of metallic sheeting over roofs, and use of metallic wallboard. Internally, protection can be enhanced, especially for long Ethernet networks and communication lines, by using (properly terminated) shielded cables. Other approaches include filters or ferrites. Where possible, retrofitting with fiber optic cables provides excellent protection. In some cases, for a higher level of protection, properly specified surge arrestors could be used, and vulnerable switches and routers could be replaced. [232]

VI. CONCLUSIONS

The complex, multilayered fabric of modern society is woven from interactive networks of public and private institutions, constantly evolving to respond to changing conditions, technologies, opportunities, and risks. Its primary function is to sustain flourishing, healthy cultures, providing a secure environment for communities to live, grow, thrive, and pursue cherished goals and ideals.

Interwoven within these social networks are the vital systems that sustain them. Food, clean water, sanitation, transportation, communication, financial services, medical care – the list is long. But the warp and woof of this fabric is the infrastructure that supports them all – the power grid.

As one of a very small number of threats with the potential to put at risk vast regions of the national power grid, electromagnetic threats – Severe Space Weather and EMP – are unlike others. With almost every relevant U.S. government agency, allied governments, multi-national insurance companies, and other institutions now all concluding that severe electromagnetic threats must be considered catastrophic risks,[233] properly addressing these threats has become a prerequisite to assuring societal health and security. Facing unknown deadlines for both natural and malicious threats, it is both prudent and urgent that we begin, and proceed with due diligence. The question, of course, is how and where to start.

Seeking an answer to this question may be most effective if we reformulate it. Given the complexity of the national power grid, the level of consensus on a few focused, strategic questions will likely define both the pace and direction of e-threat protection.

A. Asking and Focusing the Important Question: What is the Starting Point for an e-threat Resilient National Power Grid?

1. Where Should Our Efforts be Focused? How Should We Set the Balance Between Modeling and Protection?

It is now nearly ten years since publication of the first major U.S. government report on electromagnetic threats to civil infrastructures.[234] Since

232. Neal, et al., *supra* note 227, at 4 (subscription service).

233. *See generally Risk Assessment and Protection Library*, THE ELEC. INFRASTRUCTURE SEC. COUNCIL, http://www.eiscouncil.com/English/Resources/ResourcesCategory.asp?catId=221 (summarized and catalogued U.S., U.K., and insurance sector reports with links).

234. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24.

that time a steady stream of government studies have appeared, representing nearly every relevant government agency. International bodies have added their voices to this chorus, and the world's most heavily used risk aggregators – the largest insurance and re-insurance companies and markets – have also joined in.[235] With all studies concluding that e-threats represent a serious and potentially devastating risk to modern societies, it is time to begin taking significant steps to protect the power grid.[236]

Modeling and analysis will, of course, continue to be important. But if open-ended threat forecasting and vulnerability modeling efforts are seen as preconditions before even a basic due diligence protection process can begin, meaningful progress will be impossible. Radical improvement in assessing the solar threat would require breakthroughs in solar physics to permit high confidence, long-term Severe Space Weather forecasting – a capability a generation away, at best. Serious improvement in understanding the vulnerability of the U.S. transformer fleet would require comprehensive, detailed vulnerability modeling of all EHV transformers – an enormous undertaking with uncertain payoff – and anything less would have minimal credibility.

For malicious threats, the situation is much the same. Few would suggest U.S. security forces can provide assurances that, through deterrence and security operations, the oceans surrounding our shores will always be swept clean of any potential HEMP threat, and "hoping for the best" has typically not been considered an adequate national security strategy. And with both U.S. and allied governments warning of unprecedented proliferation trends, this situation seems unlikely to improve – or even to remain static.[237]

If we are to begin hardening the power grid within the foreseeable future, the balance will need to shift toward implementation. It is time to turn our attention to planning, implementing, and where necessary developing and testing, cost effective approaches to protect the power grid.

2. Are There Safe, Reliable, and Practical Options for Grid Protection?

There is no shortage of hardware and procedural approaches for e-threat protection. Ranging from enhanced procedures to current blockers, from series capacitance systems to increased spares, some of these approaches are in limited use today, and costs are typically low.[238] Many would have synergistic benefits, such as increasing resilience against cyber or terrestrial weather events. The reason the power grid is not protected is not a lack of urgency – with the impressive, long list of studies, the risks, which are serious, are well documented. It is also not limited availability, effectiveness or cost. The

235. *See generally* U.K. H.C. DEFENCE COMM. REPORT, *supra* note 29; LLOYD'S 360°, *supra* note 185.

236. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at 1.

237. *See generally NATO and Partners Examine Non-Proliferation, Arms Control and Disarmament*, N. ATLANTIC TREATY ORG. (Jun. 16-17, 2011), http://www.nato.int/cps/en/natolive/news_75428.htm.

238. *Threat Posed by Electromagnetic Pulse (EMP) Attack: Hearing Before the H. Armed Services Comm.*, 110th Cong. 2 (July 10, 2008) (statement of Dr. William Graham, Chairman, Comm'n to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack), *available at* http://www.empcommission.org/docs/GRAHAMtestimony10JULY2008.pdf (noting that "[t]he cost for such improved security in the next 3 to 5 years is modest by any standard—and extremely so in relation to both the war on terror and the value of the national infrastructures threatened").

problem is that energy sector stakeholders, perhaps due to a lack of awareness and detailed information, are not yet asking the relevant question.

In fact, the question itself is a large part of the answer. "Given past experience and the potential for additional serious societal damage, are there safe, reliable, and practical options for grid protection?" If this question is asked seriously and urgently by the most relevant corporate and government stakeholders, it will drive the energy sector toward practical and dependable answers and, ultimately, power grid protection. If today the energy sector's understanding of e-threat issues is limited, and failure to both ask and answer hard performance and cost questions has led to vague concerns over unknown risks, the remedy must be an aggressive effort to build awareness, to ask the right questions, and to find dependable answers.

What are the real costs of practical steps toward hardening the nation's power grid? If the costs of at least minimal protection are affordable, as early estimates and industry experience suggest, what are the risks of such measures? And what can be done to better evaluate and manage those risks? Once government leadership and regulation, industry initiatives, or a mix of both make these and similar questions a clear energy sector priority, government agencies, industry associations, and other stakeholders will lay out a path toward satisfying them with serious and compelling answers.

Neither the technologies nor the testing process are mysterious, and examples of most are, in at least some locations, already in place. If we can get the right questions asked, serious work at power grid protection will begin.

3. What Are the Roles of Legislation, Energy Agencies, and Regulation?

Finally, of course, a key question remains: How should the balance be set between legislative efforts, regulatory control, and independent corporate action in addressing the above questions?

With most relevant U.S. government agencies, allied governments and other national and international stakeholders all concluding that e-threats represent a serious risk to civil society, work should begin on protection of the national power grid. The most important elements of such effort could and should be the results of independent corporate energy sector protection action, and it is encouraging that several individual transmission owner/operators have begun taking such steps. However, developing resilience against these threats will require a balanced mix of corporate initiatives, energy agency leadership, and legislative and regulatory measures. Why are these all important?

Ownership and management of the U.S. power grid are complex, and power grid hardware configuration is also highly varied. In this environment, regardless of regulation, proactive efforts by the nation's many power companies will be essential if this problem is to be addressed any time soon.

Nevertheless, it is unrealistic to expect the approximately 3,300 U.S. power companies[239] to each separately decide to take on this challenge as individual corporations. In some states, in fact, existing legal frameworks make it difficult

239. PLATTS, 2013 UDI DIRECTORY OF ELECTRIC POWER PRODUCERS AND DISTRIBUTORS vi (Ellen Flynn Giles ed., 2012), *available at* http://www.platts.com/IM.Platts.Content/downloads/udi/eppd/eppddir.pdf.

for power corporations to seek cost recovery for such resilience investments.[240] And without a top level, nationally mandated plan, e-threat mitigation measures actually taken by any one corporation may have little impact, even on assuring power to their own customers. The impact of both Severe Space Weather and EMP on the bulk power system results from the power grid's organic, integrated architecture, and resilience measures, to be effective, must respond to that reality. GIC, for example, does not begin or end at arbitrary grid ownership lines. In fact, proactive efforts by one company could inadvertently shift GIC to a neighboring, more sensitive portion of the grid.

To effectively and safely protect our organic, integrated power grid, an essential layer of the enterprise – in addition to (and compatible with) corporate initiatives – will be energy agency leadership and regulatory action to mandate standards and define implementation priorities and time-order, to respond to this organic, integrated structure. Such standards will also need to express national-level prioritization of functionally or security-related asset and node criticality. While implementation will likely take place in stages, these stages must be time-phased, and must map directly to national priority assessments.

Crafting standards which (a) address the grid's organic structure, (b) account for evolving mitigation measures, and (c) avoid creating a framework too rigid to respond to differing corporate or geographic needs, will require best-in-class technical input and broad stakeholder review. Just as important, defining implementation priorities and phases that are informed by critical functionality and security requirements will require input from corporate and government stakeholders, representatives of other critical infrastructures, and major bulk power system customers.

B. Prudent Approaches Toward an Answer: The Starting Point For an e-threat Resilient Power Grid

1. Focusing Near Term Efforts, and Setting the Implementation / Modeling Balance

Reviewing the overwhelming body of recent work defining e-threat risks to the power grid, there is a more than adequate basis to begin. And while progress toward an e-threat resilient power grid will be guided by continuing analysis, modeling should be used primarily as a concurrent tool for implementation, not as a substitute. If our primary focus becomes building a monument to advanced solar physics or turning loose an army of thermal engineers on nationwide EHV transformer modeling, we will have taken a wrong turn.

As we have seen in this article, one of the most important drivers for progress in e-threat protection of the power grid will be energy sector initiatives. Given the impressive ownership and management complexity of the U.S. power grid, there is no effective alternative to broadly based, diligent corporate efforts. This, in turn, means a mechanism will need to be found to allow for

240. *See, e.g.*, NAT'L INFRASTRUCTURE ADVISORY COUNCIL, A FRAMEWORK FOR ESTABLISHING CRITICAL INFRASTRUCTURE RESILIENCE GOALS: FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL 26-27 (Oct. 19, 2010), *available at* http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf.

development, tuning, and sharing of best practices, nationally and internationally.

As a first step, most of the effort should be focused on Level III protection, to build-in adequate resilience to support gradual recovery of power grid operation in an affected region. For recovery-critical facilities, Level II protection will allow rapid system-wide repair and restoration after an e-threat event.[241] And, of course, for those facilities judged critical priorities for national or regional health and security,[242] Level I comprehensive protection may be necessary, ensuring either uninterrupted operation, or very fast recovery.

2. Acquiring the Tools: Assuring a Broad Selection of Safe, Reliable, and Practical Choices for Building Resilience Into the Power Grid

While many examples of e-threat protection hardware are available and, to a limited extent, integrated into the bulk power system, some of the most cost-effective tooling is still comparatively new. GIC current blocker and advanced, Level I E1 protection prototypes, for example, have undergone some successful testing, but have little history of use in the power grid, leaving unanswered questions and limiting their utility.[243]

As a practical measure, making such devices available may require additional testing and validation, and this may be an area where a national government agency could effectively step forward to implement a testing program. By planning for comprehensive testing, and by including corporate and user stakeholders in defining test requirements, these devices could be made available for secure integration into the power grid.

3. Legislative, Energy Agency, and Regulatory Roles: Crafting an Optimum Legal Framework for Power Grid Resilience

As mentioned above, there is a fundamental disconnect between, on the one hand, the diffuse legal framework and corporate and management architecture of the power grid, and on the other, its organic vulnerability to electromagnetic threats. While, as we have seen, some proactive energy companies have already implemented protective measures, most have not, realizing that isolated local efforts would become effective only after most other corporations have followed their lead. And, of course, a staged plan for implementing a resilient national power grid will need to respond both to the organic nature of the power grid, and to state and federal assessments of critical priorities.

In addition, due to rapid evolution of the power grid and of e-threat protection measures, realistic labor turnover rates, and changing national and local priorities, this staged process will need to be guided by ongoing, national-level coordination and management.

---

241. EMP COMM'N 2004 EXEC. REPORT, *supra* note 24, at 14.

242. EMP COMM'N 2008 Report, *supra* note 1, at 103, 129, 147 (noting that oil and natural gas companies operate telecommunication facilities, food facilities, and emergency services).

243. *See, e.g.*, *Grid Stability System Undergoes Live Grid Testing by Defense Threat Reduction Agency*, TRANSMISSION & DISTRIBUTION WORLD (Oct. 2, 2012), http://tdworld.com/go-grid-optimization/asset-management-service/emprimus-solid-ground-0912/.

In short, achieving and maintaining an e-threat resilient power grid will require continuing national guidance, management, and monitoring. To the extent there are legal impediments to corporate efforts, these will also need to be addressed. If we are to achieve and maintain a reasonable level of resilience, legislative, regulatory, and energy agency involvement is going to be part of the picture.

Of course, the day to day reality is that the power grid is under the direct control of the many corporations that own and operate it, and the foundation for e-threat resilience remains independent corporate action. But such efforts are unlikely to be broadly implemented until power companies have a sense they will be working in partnership, both together and with the guidance and support of federal and state legislators, energy agencies, and regulators.

C. Looking Toward the Future

It is time, perhaps past time, to begin implementing a broadly based due diligence process to secure the nation's power grid against natural and malicious electromagnetic threats.

If this is to take place it will mean national and international energy corporations, government agencies, and other public and private stakeholders will need to begin turning their attention toward planning, implementation, validation, and national level management.

For implementation, corporate planning will be foundational, and for this a mechanism is needed – with national and international reach – to help in coordination, best practice development, and information sharing. The Electric Infrastructure Security (EIS) Council has recommended the E-threat Protection (E-Pro^{TM}) Handbook as an example of such a mechanism, beginning, as a first step, with a broad international survey of evaluation studies and best practices.[244]

To help develop clear and consistent policies for management of the overall e-threat protection process, national and international government and corporate coordination are also important; the annual Electric Infrastructure Security Summit (EISS) Series[245] has begun providing such a framework, and other measures will be needed as e-threat protection efforts mature.

But the challenge must not be underestimated. As we have seen, rapidly evolving technology has brought with it a new, dangerous vulnerability, threatening an infrastructure so pervasive that its failure could undermine the bedrock on which our societies are built, putting our future at risk. When dealing with threats at this level, public and private stakeholders must be risk-averse.

---

244. ELEC. INFRASTRUCTURE SEC. COUNCIL, EPRO: E-THREAT PROTECTION HANDBOOK, AN EVOLVING, COOPERATIVE, MULTI-LEVEL RESOURCE FOR INFRASTRUCTURE PROTECTION AGAINST ELECTROMAGNETIC THREATS: GUIDELINES, BEST PRACTICES AND BENCHMARKS, *available at* http://www.eiscouncil.com/images/upload/media/epro%20handbook.pdf.

245. *General Info*, ELECTRIC INFRASTRUCTURE SECURITY SUMMIT: THE ANNUAL WORLD SUMMIT ON INFRASTRUCTURE SECURITY, http://www.eissummit.com/ (last visited Feb. 19, 2013). "EISS has become a new international infrastructure security framework, enhancing international cooperation and coordination of efforts to bring this serious vulnerability under control." *Id.*

Only rarely in history do we find nations with the vision, foresight, and initiative to meet such challenges – to perceive and forestall such threats before they happen. There are many examples of failure: sudden developments in military technology, rapidly shifting economic forces, and other factors have often had a shattering impact on nations and empires.

Building the resilience we need will not be easy. On the contrary – it will be a serious test, calling for imagination, courage, and dedication. With good will, and with broad support from the energy sector and the public, the men and women who own and operate the national power grid and their civil and government partners will meet this challenge.