Addressing Electromagnetic Threats to U.S. Critical Infrastructure

JINSA's Gemunder Center EMP Task Force

Co-Chairs Dr. Bryan Gabbard and Ambassador Robert Joseph

September 2015

JINSA

DISCLAIMER

This report is a product of JINSA's Gemunder Center EMP Task Force. The findings expressed herein are those solely of the EMP Task Force. The report does not necessarily represent the views or opinions of JINSA, its founders or its board of directors.

Task Force and Staff

Co-Chairs

Dr. Bryan Gabbard
Executive Vice President, Defense Group Inc.

Ambassador Robert Joseph
Former Under Secretary of State for Arms Control and International Security

Members

Dr. George Baker
Former Electromagnetics Group Leader, Defense Nuclear Agency

Dr. John Foster, Jr.
Former Director, Lawrence Livermore National Laboratory and Member, Congressional EMP Commission

John Kappenman
President and CEO, Storm Analysis Consultants

Amb. Ronald Lehman, II
Former Director, US Arms Control and Disarmament Agency

Richard Murray
Head of Liability Regimes Project, Geneva Association

VADM (ret.) Dr. G. Peter Nanos
Former Director, Los Alamos National Laboratory

Dr. Keith Payne
Former Deputy Assistant Secretary of Defense for Forces Policy

Dr. Robert Pfaltzgraff, Jr.
Professor of International Security Studies, Fletcher School at Tufts University

Thomas Popik
President, Foundation for Resilient Societies

Dr. William Schneider, Jr.
Former Under Secretary of State for International Security Affairs

Dr. David Stoudt
Distinguished Engineer, Naval Surface Warfare Center

Dr. James Tegnelia
Former Director, Defense Threat Reduction Agency

Dr. Richard Wagner, Jr.
Former Assistant to the Secretary of Defense for Atomic Energy

Gemunder Center Staff

Dr. Michael Makovsky
Chief Executive Officer

Ashton Kunkle-Mates
Research Assistant

Jonathan Ruhe
Associate Director

Table of Contents

Introduction

The Congressionally-mandated EMP Commission Reports of 2004 and 2008 concluded that the electromagnetic pulse (EMP) threat to our nation is serious, that it is possible to mitigate the threat, but that little is being done to meet the challenge. Since then, our nation has further increased its reliance on technologies that depend upon the availability of electricity and digital electronics to manage and monitor the network of systems that deliver our basic goods and services. Our system for generating and distributing electricity is the core of this network. Failure here could cascade across other vital national infrastructures such as: telecommunications, transportation, banking, critical medical care, and water filtration and pumping. This could severely disrupt everything we take for granted, from food and water distribution to functioning sewer, medical, healthcare and banking systems.

Of special concern are both natural events and man-made threats that exploit weaknesses based on the very strengths of our modern digital society. For example, solar geomagnetic storms (geomagnetic disturbances or GMD) create immediate and intense current surges that may disrupt electrical and electronic systems, potentially on a continental scale. These storms are part of the sun's normal cyclical activity, making the Earth's recurrent exposure to them a certainty. Additionally, cyber-attacks, intentional electromagnetic interference (IEMI) weapons, and high-altitude electromagnetic pulse (HEMP) attacks produced by the detonation of a nuclear device above the Earth's atmosphere could also cripple our critical national infrastructure and wreak havoc on and endanger the lives of tens of millions of Americans.

Numerous groups beyond the latest EMP Commission have pointed out for decades the grave dangers that these threats pose, particularly HEMP. In addition, both individual experts and senior leaders have called attention to the potentially catastrophic impact on the vital functions of society. However, little has been done to take the necessary steps to protect our infrastructures, and the vulnerabilities only continue to increase. As this dangerous condition grows, the devastation that would follow such an attack multiplies as well, thereby making electromagnetic (EM) attacks an increasingly attractive option for U.S. adversaries. This is compounded by the fact that nuclear proliferation has resulted in new capabilities for those who may be more inclined to exploit our vulnerabilities to EM attack.

Despite this growing danger, mitigating the likelihood and consequences of such an attack could be accomplished with relatively modest investments in infrastructure over the near to medium term, especially when compared to the scale of losses should we continue to do nothing.

Recognizing these trends, JINSA's Gemunder Center for Defense and Strategy established a Task Force to examine the gap between increasing EM threats and increasing infrastructure and societal vulnerability, and to formulate a set of specific recommendations aimed at government and industry, that would begin to close this gap.

With regard to EMP attacks, which are man-made, we reaffirm the basic, three-component strategy: deterrence, active defense and improving the resilience of U.S. infrastructures and society. There is interdependence among these elements. It is not possible to deter all threats, so defenses and resilience are necessary; it is not possible to defend against all threats, so deterrence and resilience are necessary; and it is not possible to make infrastructures completely invulnerable, so deterrence and defense are necessary. None of these three strategy components is adequate by itself.

Each component needs to be improved and integrated as part of a comprehensive national strategy. Deterrence strategies specific to the above threats need to be more fully developed, and defenses need to be made more effective against a wider range of attack scenarios. And, despite some recent steps in the right direction, a great deal more needs to be done to reduce infrastructure vulnerabilities to both natural and man-made dangers. In this report, we address both deterrence and reducing infrastructure vulnerabilities. To this end, the recommendations contained in this report seek to reduce EM vulnerabilities in the nation's critical infrastructures and society, in a manner that is implementable and not cost-prohibitive.

In support of these findings and recommendations, JINSA has posted several relevant documents on its website for this Task Force. These documents have underpinned these deliberations and remain important references, including:

- An internal EMP Task Force memo on feasibility of hardening measures;
- *Solar Storm Risk to the North American Electric Grid* (Lloyd's of London, 2013);
- U.K. government Space Weather Preparedness Strategy 2015;
- Lloyd's City Risk Index *2015-2025*.

What's New

Because there is a long history of inaction in this area, we felt it important to focus our efforts on new developments that expedite solutions. There are significant developments on five fronts that make this a particularly important and productive moment to reevaluate the options available for addressing EM threats.

There are advantages to be gained by addressing the overlapping EM threat spectrum with integrated solutions, rather than treating threats individually.

The new concerns associated with pervasive and still-evolving cyber threats, and the mitigation actions and training protocols being enacted to address these threats, have opened new avenues to address other EM threats, even though the effects of such threats may differ. The certainty of geomagnetic storm activity – and the increasing availability of data on the likely collapse of the power grid during these events – has opened windows into facility hardening priorities and procedures, as well as the value of training designed to improve infrastructure restoration protocols. The similarities between waveforms associated with the late-time component (E3) of nuclear EMP and GMD point to the ability to harden the grid against both effects using the same protection devices.

There are economies of scale that can be used to advantage in hardening selected assets in a manner that addresses multiple threats using the same engineering tools, leaving some threats to be dealt with in ways other than direct hardening.

Deterrence strategies specific to man-made EM threats can add value.

Little attention has been devoted to deterrence strategies specific to HEMP and IEMI attacks, perhaps because of the assumption that pre-existing nuclear deterrence policies during the Cold War were sufficient to address EM threats.[1] With the emergence of new nuclear actors

and new EM threats, however, more emphasis must now be given to EM-specific deterrence. A clear U.S. declaratory statement that the United States will retaliate after any EMP attack in a manner that would overwhelm whatever value the opponent might anticipate gaining from such an attack is an important component of a multi-pronged strategy. This approach must be tailored to address a large variety of such threats. U.S. deterrence would be best served by communicating that any such retaliation will be based not only on immediate and direct U.S. casualties and damage from an EM attack, but also will take into account projections of future casualties resulting from damage to critical national infrastructure over time, and on other physical and economic costs deriving from an attack.

Leveraging the emergence of smart grids, the rapid turnover of electronic systems, and industry initiatives will add value.

The construction of smart grids can ensure that we can have a more complete picture of the grid, including during catastrophes or major attacks. This becomes possible if smart-grid components are required to be survivable. The replacement of outdated systems with these and other advancements provides an opportunity to build EM protection into the grid, without the larger expense of retrofit protection.

Despite the vast installed base of electronic equipment, hardware and software "fixes" should not be overwhelming in cost or convenience. The life cycles of modern electronic systems are relatively brief (a situation ultimately deriving from "Moore's Law") compared to their long-lived mechanical or electro-mechanical predecessors. Hence beginning a process of producing EM-resistant electronic systems and, where appropriate, components and subsystems can have an early and cumulative effect on mitigating the threat to which the nation is exposed. Many important components – such as surge arrestors and transformers – do not follow this pattern and must be treated separately, but these fixes can be prioritized to diminish the vulnerability of the most critical systems first.

The ongoing industry upgrades with new technology also present an opportunity to update and overhaul existing grid elements in a manner that leads to increased resiliency in facing EM challenges.

Public-private partnerships can be leveraged in new ways for improved EM protection.

One fundamental challenge of critical infrastructure protection is the divide between those who are responsible for keeping Americans safe (the government), and those who own and operate the systems that need to be protected (in most cases, private entities). Some progress is being made. As part of an effort to create better critical infrastructure protection standards in the aftermath of 9/11, the Department of Homeland Security (DHS) was created with a mandate to address vulnerabilities of the civil infrastructures. More recently, the National Cybersecurity and Critical Infrastructure Protection Act of 2014 creates new DHS responsibilities that can be expanded and strengthened in a number of ways. Indemnification of utilities for actions they take to mitigate EM threats is a serious problem at the public-private interface. The Price-Anderson Act of 1957, which indemnifies industry in the event of nuclear accidents, could be broadened to include indemnification of industry in mitigating the effects of EM attacks. Nevertheless, existing laws, authorities and organizational structures are insufficient to provide guidance and incentives to motivate action by either side. Here again, while some progress is being made – such as the proposed federal standard that the electric utility industry provide a baseline for protection against GMD effects – more needs to be done.

The public-private interface is also receiving further attention and refinement in the context of cyber-security. Similar solutions should be applied to the broader array of EM threats.

Increased public awareness is essential.

Recent documentaries, news reports, motion pictures and popular novels have raised awareness among the general public of the potential catastrophic consequences of wide-area EM threats. Public officials have become increasingly aware of the need for action through the efforts of several watchdog groups. Furthermore, several states have passed legislation to study the effects and mitigation options and costs. This awareness is resulting in more public pressure for action and greater government appreciation of consequences and a willingness to proceed with real solutions.

Findings and Recommendations

UNDERSTANDING THE THREAT SPECTRUM

Findings

EM threats include an overlapping spectrum of challenges that exploit weaknesses of our modern digital society – weaknesses rooted in the very features that also provide great strength and resilience. Each component of this threat spectrum, including GMD, cyber-attacks, IEMI weapons and HEMP, could severely disrupt the lives of tens of millions of Americans due to existing vulnerabilities in our critical national infrastructure. Of these, GMD and HEMP pose the potential to inflict the greatest devastation by far – including on a continental scale. Because these dangers result from similar EM vulnerabilities, they can be treated most effectively by addressing the full spectrum together synergistically.

Science has the means to estimate credibly the likelihood of a serious GMD, based on scientific observations over the last century and more. Estimates of the probability of exposure to geomagnetic storm-produced environments are grounded on historical solar cycle data, and relate to "when" or "with what magnitude" such events will occur, not "if" they will occur. The likelihood of a serious GMD is assessed by NASA to be approximately 12 percent per decade – certainly high enough to warrant a major national effort to harden the grid.[2]

In contrast, it is virtually impossible to estimate the "likelihood" of an EMP attack on the United States. Executing a man-made EMP attack would be a decision made by human beings in complex, unprecedented and stressful political (and probably personal) circumstances. Unlike natural phenomena, for which science provides a basis for estimating likelihood, there is no reliable methodology for estimating the likelihood of an EMP attack. This likelihood should be treated as being simply indeterminate.

However, though it is not possible to estimate the likelihood of an EMP attack in general, it may be possible to estimate relative likelihoods among different EMP attack scenarios, based on technical capabilities an adversary would need to execute the various attacks. The red-teaming approach we recommend could help in estimating the range of scenarios to be used and their relative likelihoods.

In sum, while it is not credible to assign numerical probabilities for malicious exploitation of EM vulnerabilities, it is possible to identify developments that increase the capacity of a state or group to conduct an EM attack. These include the proliferation of EM attack technology and capabilities, especially to actors with stated hostile intentions toward the United States and its allies and the growing credibility – absent real efforts to bolster U.S. societal resiliency – of the already-widespread perception that U.S. vulnerabilities make an EM attack very likely to accomplish its objectives.

Recommendation: Develop a long-term comprehensive plan to address the full spectrum of interrelated EM threats.

As both technology and the international landscape evolve, so too will the threat spectrum and corresponding U.S. vulnerabilities. It is imperative that planning and policies aimed at maintaining our societal functionality not remain static, but rather evolve to meet new threats. To this end, we recommend Congress expand its efforts to amend Section 707 of the Homeland Security Act of 2002 (P.L. 107-296) – mandating DHS perform a Quadrennial Homeland Security Review – to specifically require the inclusion of full-spectrum EM threats, attendant protective actions and preparedness oversights and evaluation.

Recommendation: Employ red-teaming to improve operational planning processes in a way that integrates the full threat spectrum.

We recommend the development of a more consequence-based red-teaming process to aid in the development of scenarios that can be used for systems planning, performance evaluations and operational protocol developments. The process must underscore the core importance of technical versus political threat forecast drivers, and must set the full spectrum of EM threats within a range of possible scenarios, not simply likelihoods of a given threat occurrence. This process can help spark an important yet balanced debate regarding system priorities and protection requirements among key stakeholders from both the public and private sectors.

DETERRING EM THREATS

Findings

Little attention has been devoted to the specifics of deterring HEMP attacks. Against such an attack, as with any punitive form of deterrent threat, the United States must ensure it could retaliate in a manner that would overwhelm whatever value the opponent might anticipate from such an attack. As such, deterrence against EM attack – just like deterrence against other types of attack – would be predicated on the resilience and diversity of U.S. retaliatory forces. At the same time, a deterrent posture and strategy would need to incorporate capabilities to defend against and mitigate the societal consequences of an EM attack.

Because most forms of EM attack would not target U.S. retaliatory capabilities specifically, but rather the functioning of critical national infrastructure more generally, the value of an attack to a prospective opponent could be diminished by U.S. efforts to minimize the effects of deterrence failure. To this end, efforts to prioritize a protection plan based on societal functionality will bolster EM-specific deterrence. The United States must also ensure it can preserve the functionality of its attribution and retaliatory capabilities in any EM environment.

Recommendation: Develop and implement EM-specific deterrence policies.

The United States needs to understand better how to deter rogue actors such as North Korea and Iran that possess EM attack capabilities. The eccentric or unconventional values and goals of such actors, and their willingness to accept certain costs beyond those acceptable to traditional rational actors, are not new. The United States needs to understand better how to influence and predict the behavior of rogue regimes and increasingly more traditional competitors like Russia and China.

What is new is the potential for such actors to employ EM attack as part of a broader asymmetric offensive strategy. Iranian military strategists are known to have explored seriously the potential for developing HEMP weaponry, and that country already possesses the Middle East's largest ballistic missile arsenal. Even if the recently-concluded agreement on Iran's nuclear program is approved, Iran could obtain a nuclear weapons capability in a matter of months and its ballistic missile force, including its ICBM and satellite launch programs, are not constrained. North Korea possesses a growing nuclear arsenal and is suspected of having cooperated with Russia on HEMP technology. Like Tehran, the regime also has worked to develop long-range ballistic missiles.

U.S. strategists therefore must seek to identify prospective opponents' assets that could be put at risk and the adversaries' likely prioritization and cost-benefit calculations. This will require constructing a more comprehensive set of threat estimates and EM attack scenarios. These must be detailed enough to include considerations of deterrence by retaliation, using the red-teaming and modeling approach mentioned above. Simultaneously, the challenges of deterring rogue adversaries reinforces the value of deterrence by defense and mitigation, since the greater the extent to which the United States can protect against EM attack, the less reliant it must be on deterrence by threat of retaliation. Therefore, we recommend a process and point of authority be established within the U.S. government – perhaps most appropriately under the Secretary of Homeland Security, as proposed in legislation currently in the U.S. House of Representatives – with the responsibility and resources to prepare the plans to execute these actions.

Recommendation: Improve strategic communications to shape perceptions and strengthen deterrence.

The United States must also undertake a program of strategic communications to convey the message that it can defend against EMP attacks, mitigate vulnerabilities if defenses fail, and retaliate against an attack. The credibility of this message will depend on the implementation of the recommendations in this report.

Because prospective EM attackers like Iran and others may attach value to very different sets of assets and goals than the United States or its more traditional adversaries, U.S. declaratory policy must seek to identify and communicate the "right" type of punitive threat to the particular opponent in question. These threats should be based on the opponent's perceived value hierarchy and decision-making processes, as determined by the more comprehensive set of threat estimates and EM attack scenarios described in the recommendation above. While specific forms of threatened retaliation should be tailored to potential adversaries and EM attack vectors, U.S. deterrence would be best served by communicating that any U.S. retaliation will be based on cumulative impact expected over time, and not just the immediate effects.

Declaratory policy – and by extension deterrence credibility – would be strengthened by a consistent, structured whole-of-government coordination of messaging by U.S. officials. Existing authorities for devising and communicating U.S. declaratory policy are too diffuse, leading to conflicting and even contrary statements undermining the coherence of deterrent threats. Statements by officials downplaying the importance or viability of U.S. retaliatory capabilities at all levels – up to and including nuclear weapons – further undermine the credibility of deterrence. Incorporating the EM dimension of deterrence is an important component of the ongoing revitalization of the U.S. strategic posture.

REDUCING VULNERABILITIES TO EM ATTACK

Vulnerabilities to EM attacks and natural EM events can be reduced by hardening the electric grid and the electronic infrastructures, and by executing smart shutdowns on warning of the power grid and other elements of the infrastructure. In both cases, this will require smart reconstitution after an event.

All of these – hardening, smart shutdown and smart reconstitution – will require prioritization among infrastructure functions and improved planning, modeling and exercises. All of the above will require regulatory reform, improved organization and responsibilities and improved public-private relationships.

Finding 1: Hardening

Some degree of technical contention about the feasibility and cost of hardening electrical and electronic systems against EM environments such as EMP or GMD has existed for decades. The conventional wisdom of experts in the field can be summarized as follows:

> It is feasible, and not too costly, to harden small, simple electrical/electronic systems: individual racks of electronics, individual buildings full of racks of electronics and possibly even specific locations like airports.
>
> But no one knows how to harden against loss or degradation of very large networks of electronics – such as the entire national electrical infrastructure, or other kinds of immense infrastructures that depend on the electrical infrastructure, like the information infrastructure and other infrastructures (e.g., the financial or the food distribution infrastructures) that depend on the electrical and information infrastructures. Preserving such functionalities may well be impossible, and even if one spent the immense sums needed to try (possibly hundreds of billions of dollars), we would never know whether we had succeeded, short of being tested by the event.[3]

A strongly held alternative view holds that it is, in fact, possible to harden entire infrastructures, and to do so affordably. In particular, this view believes that the national electric grid can be hardened for perhaps $50 billion spent over about five years – a small fraction of its capitalized cost and an affordable fraction of utilities' annual revenues.[4]

Indeed, several utilities are beginning programs intended to harden selected grid control facilities. We do not know whether their hardening programs include a comprehensive system-level protection and testing program of sufficient fidelity to provide confidence in the hardening measures being undertaken. However, their actions are encouraging.

While we are somewhat skeptical about the feasibility of completely hardening the grid and other elements of the infrastructure, we welcome the utilities' recent efforts, because they might succeed and would not be prohibitively expensive, and because they might have a positive deterrent effect.

Elements of the electronic infrastructure are constantly being replaced and upgraded, which represents a major opportunity to begin building EM protection into the grid incrementally. These replacements will be particularly effective when augmented with system-level testing. System-level testing will be essential to determine the effectiveness of these incremental upgrades.

Recommendation: Seek incremental hardening and threat-level testing.

Rather than pursuing a comprehensive program of hardening all critical infrastructure elements, policymakers should adopt a program to gradually but steadily increase EM protections over the long term, once they identify and address the most important elements needed for societal functionality. An initial goal, subject to further analysis, is hardening roughly 30 percent of the grid in the next decade. The idea is to get above a threshold to ensure a minimal grid remains operable to allow recovery in the case of an EM event.

We also recommend developing the capability to do threat-level testing of large segments of the grid.

Finding 2: Smart Shutdown on Warning

With sufficient warning, the degradation of the technical functionality of the grid can be reduced, perhaps substantially. According to electric utilities, with about 30 minutes warning, the national grid could be reconfigured – that is, segmentally de-energized – which would greatly reduce its vulnerability to a GMD event. When impairment due to the event has passed, the grid would then resume normal operation in hours or days.

This strategy is being explored by the operators of the grid for use in the event of a GMD event. We applaud this, and believe that, though there are differences between GMD and EMP, a strategy of de-energizing parts or all of the grid should be explored as one way to reduce its vulnerability to all EM threats.

There are two major differences between an EMP event and a GMD event: the warning time, if any, would be much shorter for an EMP attack, and in the EMP case (partly because of the shorter times) the system might be more subject to spurious warning, either from sensor malfunction, routine non-threat missile launches or deliberate spoofing by an adversary.

The source of a major GMD event can be seen and identified many hours ahead of time, though precise determination of whether or not the Earth will be impacted can occur only within 30-45 minutes prior to the disturbance. Warning, if any, for an EMP attack would be much shorter. This raises the question whether the grid could be de-energized. We do not know how long it would take to de-energize the grid, but we believe that warning could be available and decisions made in the shorter times available in some EMP attack scenarios. Analogous to this, the U.S. missile defense system has the ability to assess an attack and decide to launch an interceptor in a very short time.

The diversity of missile warning systems has given us the basis to believe the risk of EMP false alarms is manageable.

Recommendation: Develop an early warning and response system.

The appropriate authorities should use existing detection, warning, communication and response processes and systems to allow them to use any advance warning of an impending EM event. Lawmakers should create the necessary legal structures to allow utilities to act quickly to de-energize the grid, as well as to indemnify them against liability. This entire process can and should be carefully planned and exercised regularly nationwide, and locally in the field.

Finding 3: Smart Reconstitution

Meaningful sections of the infrastructure are likely to be damaged by EM events, whether or not smart shutdown has been executed. The tools, technical skills and operational expertise needed to quickly identify damaged elements and take action to mitigate the functional impact of this damage, must be identified and made an intrinsic component of infrastructure contingency planning. Such specialty teams should be exercised regularly and incentivized to deliver performance excellence.

Recommendation: Put in place training and processes for smart reconstitution.

Training, processes and expertise need to be put in place to assess the damage that has been sustained by an EM event, and to decide how best to restore grid functionality.

Finding 4: Prioritization

If the grid and associated infrastructures cannot be completely hardened, some type of analytic and political process will be needed to establish priorities. A prioritization process will also be needed if the grid can be protected by smart shutdown on warning and then restoring its function, as discussed above. In thinking about prioritization, it is important to distinguish between 1) the functionality of the grid in a technical sense – how much power is delivered to what locations at what times – and 2) how the infrastructures support the functioning of society in all its meanings.

Prioritizing among the societal functionalities that would or would not be supported by a degraded electrical grid will involve life-and-death tradeoffs of the most difficult kind. However, the nature of the EM problem demands making such prioritization. It is beyond our expertise to suggest what the political process should be to deal with this problem; we can only recommend that those better suited than we take on this task.

Recommendation: Prioritize among protection initiatives based on an analysis of societal functionality.

We recommend, as a matter of urgency, that government and industry work together to identify the relationships between societal priorities and those steps necessary to protect multiple infrastructures. A political process must then be established to set strategic priorities for systems that must either be protected from EM and related threats or made resilient in

such a manner that their functions can be quickly restored. Once set, these priorities must be supported by organizations and individuals with the responsibility, authority and resources to initiate action and ensure compliance across both the public and private sectors.

Recommendation: Establish a political process for prioritization among infrastructure functions.

Finding 5: Plan, Model, and Exercise

An improved understanding of the "mission-essential" functions is required to develop priorities for infrastructure protection. What services must be available without interruption? Which are acceptable to forego for minutes, hours or days? For example, major metro areas would lose potable water quickly, and perishable foods and medications could be lost if the restoration of power takes longer. It is important to create the legal authorities and political processes for analyzing the societal functionality of key infrastructures and establishing priorities on the basis of those findings.[5]

Determining societal functionalities of the grid will require both an analytic assessment and an assessment of the political processes by which the nation can agree to act upon a given societal prioritization. The analytic assessment will require linking technical models of the infrastructure with models of the functions of society. Technical models of the grid exist, though they may need to be adapted to this problem. Attempts have been made to model the functions of society or certain broad aspects of it – econometric models and agent-based simulations of health care systems come to mind – but we are not aware of any that are suited to this problem.

Concerning EMP threats, a prioritization process has been developed in the military context. Congress and the Pentagon have also begun to grasp other aspects of the EM threat spectrum, such as cyber. The military has also protected strategic weapons and communications systems, and has trained and exercised for the possibility that unprotected electronic systems may not be available. Similarly, in the aftermath of 9/11, federal agencies, local governments and the private sector have held exercises to prepare for future emergencies. There is now a congressionally-mandated, biennial cybersecurity exercise (Cyber Storm) led by DHS that includes state, international and private-sector partners. No similar national-scale attempts to plan, prepare and train for other EM events exist.

Planning, prioritizing and exercises will yield little benefit without the necessary data and understanding of the electric grid, its functioning, connection to other critical infrastructures and vulnerabilities to EM events. We cannot predict how large networks or power grids will be damaged by EM attacks, since such attacks can differ from hurricanes, floods and other natural disasters in extent and scope.

Recommendation: Use models and experiments to understand society-wide vulnerabilities and responses.

The United States needs to expand research to identify priorities for protecting and hardening the electrical infrastructure. This research should address three main objectives. First, the United States must quickly develop a more extensive program of experimentation and analysis

to better understand technical problems and societal priorities and possible fixes for them. Second, it must construct a more comprehensive set of models of the functionality of the grid in extreme EM environments, and the relation between infrastructure function and societal functionality. Third, the United States must improve capabilities and readiness to record, share and use data from natural EM events to support modeling and analysis.

Recommendation: Develop and hold regular national preparedness exercises.

We recommend the Congress mandate that DHS plan for and lead a regular national preparedness exercise to coordinate the response to an EM event. Other federal agencies, local governments and the private sector should be involved. This could include both tabletop and field exercises. The objective should not be to add new layers of bureaucracy, but to help current agencies fulfill their responsibilities.

Analysis and development of lessons-learned from performance in these exercises will be critical. Review should be conducted by DHS and presented to Congress. Such exercises also present a valuable opportunity to increase public awareness.

Finding 6: Strengthen Public-Private Partnerships and Private-Sector Incentives.

Existing laws, authorities and organizational structures are insufficient to provide guidance and adequate incentives to motivate the necessary actions by the government or private sector. Fortunately, progress is being made in thinking through these quandaries when it comes to addressing cyber threats. Similar solutions need to be adapted to the broader spectrum of EM threats to the societal functioning of the grid.

Progress in this area must come in several forms. First, improved government oversight of electric utilities is needed to ensure adequate reliability standards are being developed, implemented and enforced. We believe the evidence of the last several years, and particularly the latest version of Critical Infrastructure Protection (CIP) standards, indicates that the North American Electric Reliability Company (NERC) and the Federal Energy Regulatory Commission (FERC) lack the autonomy, organizational construct and authorities required for this task.

Second, to facilitate incident response and planning, a clear chain of command is needed with well-defined roles and responsibilities, authorities and lines of communication between relevant government agencies and the private sector. Given the important role of the private sector in monitoring and responding to any incident, this cannot be accomplished without first creating effective oversight bodies and reliability standards to govern the utilities. To ensure proper coordination and response measures, this process should be guided by the same authority for constructing EM threat estimates and attack scenarios (see above).

Third, better information-sharing of real data on GMD between the private and public sectors needs to be established. Only limited information-sharing on EM threats exists between the public and private sectors. Legal, statutory, regulatory and licensing requirements for sharing data on the impacts and consequences of GMD can and should be strengthened.

As for incentives, the Price-Anderson Act of 1957 may serve as a framework for developing statutory authorities to indemnify electrical utilities industries from potential legal liabilities associated with grid protection measures (e.g., load shedding). This Act, which was designed

to ensure prompt and equitable compensation in the event of an accident in the nuclear industry, protects the public by establishing "a system of financial protection for persons who may be liable for and persons who may be injured by a nuclear incident." It requires the Department of Energy to include an indemnification in its contracts that involve the risk of a nuclear incident. This indemnification:

1. Provides omnibus coverage of all persons who might be legally liable;
2. Indemnifies fully all legal liability up to the statutory limit on such liability (currently about $10 billion);
3. Covers all Department of Energy (DOE) contractual activity that might result in a nuclear incident in the United States;
4. Is not subject to the usual limitation on the availability of appropriated funds; and
5. Is mandatory and exclusive.

Recommendation: Use the concept behind Price-Anderson as a basis for indemnifying private-sector entities for their actions to mitigate electrical infrastructure vulnerabilities.

Recommendation: Create insurance mechanisms to mitigate vulnerabilities.

We believe the insurance industry should play a constructive role in facilitating this Task Force's recommended grid protection measures. Insurance providers could set basic resilience standards as part of their terms of coverage for utilities companies in the case of an EM event. Moreover, existing public-private partnerships in the United States and Europe that divide the risks of potential terrorist attacks between public and private sectors should be used as a model for cooperation between government and utilities to protect critical infrastructures. To help the insurance industry create proper models for pricing risk associated with possible EM events, these solutions will require progress on information-sharing between the public and private sectors on historical data from GMD.

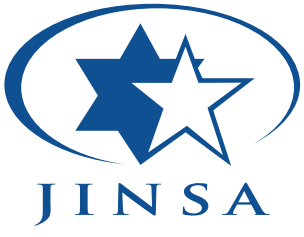
Recommendation: Expand public-private partnerships to improve standards.

We are encouraged to see that several utilities have already begun to harden and build protections into new grid components. Policymakers can ensure these efforts extend to upgrades by adding a hardening requirement to the mandatory Reliability Standards developed by FERC and enforced by NERC. Relevant standards that would require updating should include: Facilities Design, Connections and Maintenance (FAC); Interconnection Reliability Operations and Coordination (IRO); Protection and Control (PRC); and Transmissions Operations (TOP).

Standards should also be updated to enhance resilience. The Congressional EMP Commission estimated that such hardening could be achieved at an additional cost of not more than 1-3 percent of the existing capital investment for equipment upgrades to the electric grid, if hardening is done at the time the unit is designed and manufactured. With those annual investments running about $100 billion, the cost of hardening equipment to ensure resilience in the face of EM events would be on the order of $1-3 billion annually.[6]

Endnotes

1. The cyber community has devoted significant thought to cyber-specific deterrence, precisely because achieving deterrence is difficult and often ambiguous in the cyber domain. The electronic warfare (EW) communities have thought about deterrence for nearly a century, and IEMI bears more resemblance to EW than to HEMP (or even cyber).
2. Peter Riley, "On the Probability of Occurrence of Extreme Space Weather Events," *Space Weather*, Vol. 10, February 23, 2012.
3. For further reading, see the appendices provided on the EMP Task Force's website.
4. Estimates by the Congressional EMP Commission and its members have placed the cost of hardening U.S. critical infrastructures at $10-20 billion over several years. An estimate by the Foundation for Resilient Societies places the topline EMP and GMD protection cost estimate for the electric grid at $10-30 billion (see: "Preliminary Low EMP and GMD Protection Cost Estimate for U.S. Electric Grid & Supporting Infrastructures," Foundation for Resilient Societies, 2015).
5. The National Infrastructure Advisory Council, and advisory body for the Department of Homeland Security, has issued multiple reports in recent years highlighting infrastructural cross-sector dependencies and vulnerabilities, and providing recommendations to improve resilience. See: *NIAC Critical Infrastructure Security and Resilience Research and Development Plan: Final Report and Recommendations* (November 2014), available at: http://www.dhs.gov/publication/niac-cisr-national-rd-plan-final-report
6. Dr. William R. Graham, et al, *Report of the Commission to Assess the Threats to the United States from Electromagnetic Pulse (EMP Attack), Vol. 1: Executive Report* (Congressional EMP Commission, 2004), 14.



1307 New York Ave., NW • Ste. 200 • Washington, DC 20005 • (202) 667-3900
www.jinsa.org