Power Grid Resilience to Electromagnetic Pulse (EMP) Disturbances: A Literature Review

Dingwei Wang*, Yifu Li†, Payman Dehghanian‡ and Shiyuan Wang§
Department of Electrical and Computer Engineering
The George Washington University
800 22nd St NW, Washington, Suite 5900, DC 20052, USA.
{*dingweiwang, †liyifu, ‡payman, §shiyuan1225}@gwu.edu

***Abstract*—Electromagnetic pulse (EMP) disturbances have been observed, along with other cyber and physical attacks, as a potential threat to modern digitized power grids and electronic devices. While the EMP attacks are not lethal to human, they bring extremely harmful and unrecoverable damages to electronics. Irrespective of the type of the EMP attacks, either nuclear or nonnuclear, EMPs are considered among the high-impact low-probability (HILP) events in power grids, detection, modelling, and mitigation against which is a necessity to ensure the grid resilience and is in high demand nationally and globally. This paper will provide a literature review on the EMP threats and includes a background on the EMP weapons, EMP attack theories, EMP detection methods. It will also describe the EMP-engendered damages, as well as protection functions and equipment used to mitigate against the future EMP threats.**

***Index Terms*—High-impact low-probability (HILP) event; resilience; electromagnetic pulse (EMP); EMP detection; EMP protection; EMP mitigation.**

I. Introduction and Background

Electromagnetic pulse, abbreviated as EMP, is a set of burst of electromagnetic radiations generated by a rapid explosion. Broadly defined, an EMP is any transient burst of electromagnetic energy, with a very sharp leading edge building up quickly to a maximum level. Its frequency ranges from direct current (DC)—i.e., zero Hz—to some upper limits depending on the source [1], [2]. Characterized by their magnitudes, frequencies, footprint, and type of energy, there are many different types, such as static electricity sparks, interference from nuclear EMP and non-nuclear EMP weapons, gasoline engine sparks, lightning, electric switching, and geomagnetic disturbances (GMDs) cause by solar corona mass ejections (CMEs) [3], [4].

The EMP is in fact an electromagnetic shock wave [5]. This pulse of energy produces a powerful electromagnetic field, particularly within the vicinity of the weapon burst. The field can be sufficiently strong to produce short lived transient voltages of thousands of volts on exposed electrical conductors, such as wires or conductive tracks on printed circuit boards, where exposed. It is this aspect of the EMP consequence which is of military concern, as it can result in irreversible damages to a wide range of electrical and electronic equipment, particularly computers, radios, or radar receivers. Subject to the electromagnetic hardness of the electronics, a measure of the equipment's resilience to this effect, and the intensity of the field produced by the weapon, the equipment can be irreversibly damaged or in effect electrically destroyed. The damage inflicted is not unlike that experienced through exposure to close proximity lightning strikes, and may require complete replacement of the equipment, or at least substantial portions thereof.

The first found of EMP related project is the discovery of Compton Effect. In 1925, Physicist Arthur H. Compton found unexpected electromagnetic radiation during the study of the nuclear reaction, laying the foundation for its use as an offensive weapon [6]. To nuclear EMPs, there can be found two real nuclear damage incidents in history. In 1961, The Soviet Union hosted an air-explosive nuclear test at an attitude of 35 km over the Novaya island. It was unexpected that the hydrogen bomb not only destroyed almost everything near the explosion, but also caused an impact on electronic systems thousands of kilometers away. Communication systems around that area were interrupted, and the military equipment on the island could not function for a year [6]. In 1962, The United States tested a 1.4 million tons hydrogen bomb over the middle of Pacific Ocean. It radiated a huge amount of gamma rays, damaging the oxygen and nitrogen in that area, and releasing huge amount of electrons. The weapon damaged the Hawaiian street lamp which was 3,000 kilometers away. Even the radio navigation system that far away in Australia was in chaos for 18 hours [6].

Much of the knowledge and understanding of the EMP threat is based upon testing a prior generation of devices and components, some of which are being replaced with newer technologies that have not been yet adequately tested and protected against EMP impacts. This paper presents a literature review on the EMP attacks: EMP classification and its impacts on the power grid are introduced in Section II. The existing EMP threat detection schemes are discussed in Section III. The protection and mitigation techniques against EMPs are presented in Section IV and the conclusion remarks finally come in Section V.

II. EMP Attacks: Classification and Impacts

A. EMP Classification

The EMP attacks can be categorized into two different classes: nuclear EMP (NEMP) and nonnuclear EMP (NNEMP), both of which can damage or destroy electronic devices, but are typically not lethal to human and animals [7].

978-1-7281-0407-2/19/$31.00©2019 IEEE

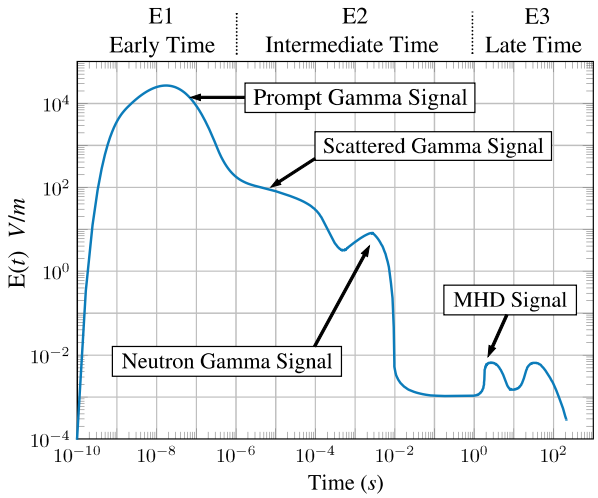

Fig. 1. Nuclear EMP Waveform [7].

1) Nuclear EMP (NEMP): The nuclear type EMP attacks mainly contains high-altitude electromagnetic pulses (HEMP), resulting from a nuclear burst at a very high altitude [8]. The HEMP from a high-yield gamma ray weapon can in principle impact the functionality of power grids, communication infrastructures, computing and electronic processing systems, and ground transportation systems dependent on microprocessors or embedded electrical systems that are susceptible to the disruptive effects of large electromagnetic perturbations. A HEMP comprised of three components defined by an international standard—the International Electrotechnical Commission (IEC) [2]. Such an NEMP waveform is demonstrated in Fig. 1 divided into the following segments:

- E1 pulse is a very rapid and intense electromagnetic field that can induce very high voltages in electrical conductors.
- E2 pulse is generated by scattered gamma rays that produced by neutrons. The E2 wave is similar to lighting strikes and can cause the electric equipment to exceed its designed breakdown current.
- E3 pulse is a slow but lasting pulse, and can last about ten to hundred seconds after the explosion [9], [10].

Another effect of an NEMP attack could be intentional electromagnetic interference (IEMI), which is caused by repeating pulses generated by antennas, with a much smaller intensity and area affected compared to HEMP [11].

2) Nonnuclear EMP (NNEMP): Nonnulear EMP is an EMP characterized with no nuclear elements. Devices that can be a NNEMP weapon include a large low-inductance capacitor bank discharged into a single-loop antenna, a microwave generator, and an explosively pumped flux compression generator [8]. An example of NNEMP is EMP bomb. An EMP bomb contains armature cylinder, a stator winding and high explosive inside the tube. Once the bomb is triggered, the armature cylinder and stator winding will produce huge amount of magnetic field rapidly radiating to surroundings [12]. Compared to NEMP, the NNEMP device (i) is easier to carry and detonate, and (ii) has lower cost [13]. One structure of a NNEMP bomb is shown in Fig. 2.

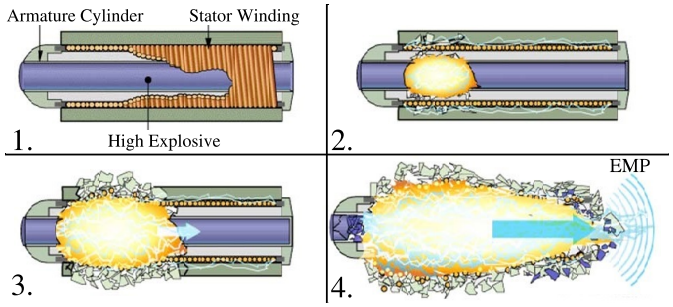

Fig. 2. Explosive pumped coaxial flux compression generator [14].

Another NNEMP is from solar corona mass ejections (CMEs), which can cause changes in the earth's magnetic field (i.e., dB/dt). These changes in turn produce a non-uniform electric field at the surface that usually slowly varies dependent on the deep earth (hundreds of kilometers) conductivity. The electric fields can be modeled as a DC voltage source superimposed on the lines, and cause quasi-DC geomagnetically induced currents (GICs) flowing in high voltage power transmission grid [4].

B. Potential Impacts of EMP on Power Grid

Generally, the EMP attack damage level is classified into four degrees: deny, degrade, damage, and destroy. *Deny level* usually happens at small attacks and the device can be self or manually restored to the initial state as the inner part of the device is not damaged. *Degrade level* requires the device to restart or manually reset in order to get back to the healthy state. The *damage* and *destroy levels* reflect that the devices are temporally or permanently damaged or destroyed and the circuits or printed circuit board (PCB) need to be replaced.

Table 1 describes the equipment status under several types of high-impact low-probability (HILP) EMP attacks. NNEMP attacks have direct and permanent effects on all electric equipment including power grids and grid-dependent devices. Compared to physical attacks, although power grid equipment such as transformers and generators are identically vulnerable, the EMP can bring more dangerous chained effect to devices that are connected to the grid such as water supply, internet, and GPS [7], [15], [16].

Nuclear EMPs (NEMP) may result in damages to power grid elements at the standard damage level of E1, E2, and E3 [9], [16]. E1 damages exceed the device breakdown voltages, E2 results in high induced current running through the wires and the E3 waveform is a long-term low-amplitude pulse lasting 10 to hundred seconds and can induces high currents in long power and communication lines, destabilize or damage the equipment such as transformers and solid state communication line drives [9]. NEMP attacks can bring serious damage to power grid device such as generator stations, supervisory control and data acquisition (SCADA) control systems, power grid control centers; it also has long term effects on internet, cell phone services, and military [2]. Although critical electronic elements in power system are usually contained within some sort of metallic box, they are not designed to protect the electronics from high-energy electromagnetic

TABLE I
POTENTIAL IMPACTS OF HILP EMPS ON CRITICAL INFRASTRUCTURES

Equipment At Risk	EMP (Nuclear)	Solar Storm	Cyber	Physical Attacks	Radio Frequency Weapons
Generator Stations	DPE	DEU	DPE	DPE	DPE
SCADA/Industrial Controls	DPE	DPE	DPE	DPE	DPE
Utility Control Centers	DPE	DPE	DPE	DPE	DPE
Transformers	DPE	DPE	PPE+CE	DPE	DPE
Telecommunications Including Cellphones	DPE	DPE	DPE	CE	CE
Internet	DPE	DPE	DPE	CE	CE
Radio Emergency Communications	DPE	TE	CE	CE	CE
Emergency SATCOM Communications	DPE	TE	CE	CE	CE
GPS	DPE	TE	CE	CE	CE
Transportation	DPE	CE	CE	CE	CE
Water	DPE	CE	PPE+CE	CE	CE

DPE = Direct Permanent Effects.
DEU = Direct Effects Uncertain.
CE = Cascading Effects (if no backup power).
DPE+CE = Potential Permanent Effects plus Cascading Effects.
TE = Temporary Effect (0.5-36 hours) assuming backup power.

pulses that may infiltrate either from the free field or from many cable connections that may compromise electromagnetic integrity. The major concern for SCADA vulnerability to EMP is focused on the early time E1 component of the EMP signal. This is because, even in the power industry, SCADA systems are not directly coupled electrically to the very long cable runs that might be expected to couple to a late-time E3 signal [2].

The strength and effects of NEMP attack depends on the warhead type and yield, and the altitude and latitude of the detonation. An NEMP device can be detonated at altitudes between 30 and 400 kilometers and generates an electromagnetic pulse with amplitudes around tens of kilo-volts per meter and radius of effects from hundreds to thousands of kilometers [17]. Taking E2 waveform as an example, a similar lighting current of 100 KA affects a circle with radius of 50 meters by induces voltages of 15.75 KV on the conductors. This overflows all the breakdown voltage ratings designed for electronic devices. With this incredible over-voltage, the device will create extreme heat due to the inducted current, causing side effects such as burning and explosion [18].

C. Power Grid Resilience to EMPs

Citizens are constantly dependent on reliable and continuous electric power for daily life. If electric power is not accessible even for an hour, the devastating impacts could be catastrophic to multiple infrastructures such as water/food supply and production, financial systems, transportation, and health care [19]–[23]. No infrastructure other than electric power has the potential for nearly complete collapse in the event of a sufficiently robust EMP attack. While a less robust attack could result in less catastrophic outcomes, such outcomes would still have serious consequences that threaten the national security.

The continuous evolution of electronic devices into systems—that once were exclusively electromechanical—enabling computer control instead of direct human intervention and use of broad networks like the Internet, results in even greater reliance on microelectronics and thus the presence and sharply growing vulnerability of the power grid to EMP attacks. Just as the computer networks have opened the possibility to cyber assaults on the power grid or to electrical power system collapse associated with software failure (as during the August 14, 2003, blackout), they have enabled a pathway for EMP attack that is likely to be far more widespread, devastating, and difficult to assess, as it is a magnetic signal that can cause induced currents overrunning in electrical conductors, destroy power transformers [9], [10], and would make it a challenging power restoration [1].

A nuclear device detonates at a precise point in our atmosphere, producing an electromagnetic pulse that can destroy our national grid. Literally, this is the plot of William Forstchen's novel "One Second After", in which, a hostile government attacks the United States by detonating a guided nuclear missile over North Carolina, creating a large-scale electromagnetic pulse. Chaos ensued, including the collapse of nuclear power plants, hunger, disease and collective hysteria [6]. In 1979, President Carter issued an order requiring that every weapon developed by the United States since then must take full account of EMP protection capabilities. The Critical Infrastructure Protection Act passed by the U.S. Congress in 2016 directs the Department of Homeland Security to develop plans to prioritize EMP survivability and recovery capabilities. And on March 26, 2019, President Trump signed an executive order instructing several federal agencies to study the risks of EMP damages to national technology and energy infrastructure and to enhance our ability to respond to such incidents [6].

According to the Washington Examiner, if the U.S. suffered an EMP hit, electricity would be lost, the military's weapons would be downed, 99 nuclear reactors would likely melt down without electricity for cooling, and 4.1 million people living near nuclear reactors would be displaced as radioactive cloud spreads. "An EMP would cause instantaneous and simultaneous loss of many technologies reliant on electrical power and computer circuit boards, such as cell phones and GPS devices," the report says. Military and commercial jets would be degraded, bases would be cut off, and power and GPS would go dark making defense and counter-attacks virtually impossible. The attack would dismantle or interfere with electricity, affecting transportation, food processing and health care. In fact, 90 percent of the population on the East Coast would die in a year of the attack. "Failures may include long-term loss of electrical power (due to loss of emergency generators), sewage, fresh water, banking, land lines, cellular service, vehicles," the report says. Civil unrest is predicted to start within just "hours" of the attack.

The power system has been undergoing dramatic changes in technology and governance for several decades. In most parts of the United States, power is still supplied by regulated, vertically integrated utilities that generate electricity in large

power generators, moving power out from power plant over high-voltage transmission lines, and distribute it to customers and end-consumers. In other parts of the country, electric utilities have been reconstructed to adapt more competitive markets such as wholesale power sales between generators and electricity distribution companies. In the more market-oriented parts of the country, transmission lines between utility buyers and sellers are regulated or publicly owned, as are most distribution systems that provide the poles, wires, and equipment to serve retail customers. However, the flows over such wires and customers' responses are increasingly determined by market forces. Efforts to improve resilience must accommodate institutional and policy heterogeneity across the country. In many countries, minor power grid system components and programs such as distributed generation, demand response, energy efficiency, customer-owned storage, microgrids, and electric vehicles are a rapidly growing part of the overall grid resource that must be planned and managed to maintain overall grid reliability, resilience, and security. Despite such developments, for at least the next two decades, most customers will continue to depend on the functioning of the large-scale, interconnected, tightly organized, and hierarchically structured electric grid. With the vulnerability to EMP attacks, efforts should be made on building in resilience in power grids is becoming more and more critical to every aspect of our economy [24]. Resilience is not just about reducing the probability that power outages will occur, it is also about limiting and lowering down the scope and impact of outages when they actually occur, restoring power rapidly after the event, and learning from the experiences to have more resistant to similar events in the future.

III. EMP Threat Detection in Power Systems

A. Power System under EMP Influence

For CME caused EMP, as it can lead to Quasi-DC GICs in high voltage transmission grid, the flow of such currents into power transmission lines can potentially cause "half-cycle saturation" of high-voltage bulk power transformers. This phenomenon can lead to relay miss-operations, voltage dips, elevated reactive power demand, transformer overheating, disruptive harmonics, aging or malfunction of the electric power devices, and even a total collapse of the grid in the worst case scenarios [25]–[29].

B. EMP Impact Detection

Strategies to enhance electric power resilience must accommodate both a diverse set of technical and institutional arrangements and a wide variety of hazards. There is no "one-size-fits-all" solution to avoiding, planning for, coping with, and recovering from major outages [24]. A sensor developed in [24] contains parts of asymptotic conical antenna, an active integrator and the electro-optical converting circuit that can be used to detect EMP. The sensor uses an asymptotic conical antenna to sense Electric field, and the derivative signal from the antenna is encoded by an active integrator based on a high speed operational amplifier [30]. The CME caused EMP impact is detected through estimating the GICs in a current transformer. The authors in [31] proposed an approach to measure the absorbed reactive power. In [32], the existing current transformers are converted to flux-gate DC current (GIC) sensors by injecting AC excitation currents into their secondary winding; A detection method on the impact of CME caused EMP is developed in [33] by measuring the quasi-DC GIC flowing in the neutral earth points.

IV. EMP Protection and Mitigation in Power Grids

A. Protection Against EMP Attacks

The criteria to evaluate the priority of EMP protection are as follows: (1) assessing the risk to society if the infrastructure is disrupted and (2) comparing the role of infrastructure in basic functions defined in national policies, together with the amount of downtime that can be tolerated. Such policies can be employed to determine which level of EMP protection should be achieved for a particular infrastructure. It is recommended that for any infrastructure supporting life or safety or the economic well-being of the society, at least a Level 1 EMP protection capability should be attained as a near-term goal. If the loss of a particular infrastructure will likely result in a significant loss of life or health or economic well-being, then an EMP protection Level 2 or 3 is recommended. Few infrastructure owners/operators will need to meet EMP protection Level 4 guidelines, as these protections are more expensive and are developed mainly for Presidential support or strategic military missions [17].

A basics scheme for protecting devices against EMP attacks are to encapsulate the equipment in a Faraday cage. A Faraday cage or Faraday shield is an enclosure structure used to block the electromagnetic fields outside the cage. Invented in 1836, a Faraday cage may be formed by a continuous coverage of conductive metal materials. The Faraday cage should be grounded directly [34]. Some implementation examples for protection against EMPs are as follows:

1) *Antenna Protection*: Some standard protectors can be installed on wires to protect against EMP attack. A device called coaxial surge protection (CSP) is a protector for coaxial lines against lighting and also NEMP [35].
2) *Power Supply Cable Protection*: A protector can be used onto mobile installation or fixed applications. These protector series are optimized to protect sensitive devices and systems against the effects of over-voltages and fast transients and especially suited to be used in sensitive and mission-critical defense systems [35].
3) *Surge Protector*: The protector is intended to protect one wire of an analog telephone line or control signals of sensitive telecommunication, sensor or other electronic equipment against destructive over-voltage effects. It can protect earth-free AC or DC power supply lines, which are short-circuit current limited to less than 0.5 A against over-voltage effects caused by NEMP, HEMP or lightning strikes [35].
4) *Modular Attachment Kit*: Abbreviated as MAK, it is an innovative protection concept against lightning strikes and NEMP attacks. The MAK module is commonly

used for mobile or transportable systems such as containers,trucks or tanks that require power supply from external wires and transportable shelters, remote signal, and antenna lines. A MAK box frame is a seamless part of the shield—so it is a Faraday cage— that can block EM waveforms. Mostly, the MAK can protect people from working in the shielded room against the effects of lightning and can simultaneously protect electronic devices against surges due to EMP attacks or conducted electromagnetic interference (EMI) [36].

5) *EMP Shield*: EMP Shield is the world's only public military tested EMP protection technology. The EMP Shield is installed in homes and can detect and protect all the equipment connected to the electrical systems. This equipment can shunt (short) the overflow voltage coming in from the grid and the voltage surges collected within homes. This device is designed to protect an entire home from lightning, CME, power surges, and EMPs [37].

Another approach to protect equipment from EMP attacks is to shunt the overflow current over the wires [38]. Several companies have developed EMP protectors that can be installed either on power grid substations or home power lines [17], [39]. One detailed example is about the CSP simulation of RF front end EMP protection [40]. From the simulation results, three response processes of the protection module is shown as follows: spike leakage, flat top leakage, and reverse pulse. With an input 4 kV square wave pulse signal, the protective module has a fast response and can be operated first; the front stage outputs a spike leakage voltage of less than 200 V, withstanding a large impulse voltage. Following a multi-level step-down process, the protection module controls the spike leakage voltage below 30 V in less than 1 ns, which reveals a promising protection on the later circuit. In addition, if the results are to be further improved, the transmission time of the pulse spikes can be slowed down by changing the circuit board and using microstrip lines of dielectric substrates between each level to achieve the goal of matching between poles.

From the hardware perspective, the following could be pursued to improve the resistance against EMP attacks:

- Design of devices with multi-layer stack and installation of high-speed devices with shortened connections.
- The use of isolated transformer inputs, where at the same time, a common mode choke coil to be connected in series on the input power line of the power chip, and a plurality of small capacitors to be connected in parallel at the output end.
- The use of high-speed optocoupler devices to isolate the system in the grounding metal box where the feeders are wrapped in tin foil.
- Increase in the aperture of the line and install the electromagnetic sealing gasket. For the hole seam that can not be deepened, several small holes can be used instead of punching or adding metal wire mesh.

B. EMP Impact Mitigation

While large failures in bulk power grids are rare, and there is no available record related to EMP attacks, it is essential that the society is prepared for periods of prolonged outage as many vital public infrastructures such as heating and cooling, water and sewage pumping, traffic control, financial systems, and many aspects of emergency response and public security depend on the electric power supply. The effects of power outages vary with weather, for different types and locations of end-users, and over different outage duration [24].

In the event of a HEMP attack and in order to reduce the number of affected systems, the scope of damage should be limited and the ability should be reinforced to bring the systems and infrastructures back online and to the normal operating conditions as soon as possible. In so doing, the following guidelines from [2] should be considered:

- Early detection and solid response plans are essential to preparedness. While detection or prevention of an attack is beyond the purview of private stakeholders, coordination between the military, the power industry, and other affected agencies and first responds are needed to limit the initial damages and initiate procedures for a swift recovery of impacted systems.
- Broader understanding within the private sector of the potential for HEMP threats should lead to the design of more resilient components and systems. In parallel to the hardening of existing systems, stakeholders should guarantee adequate supplies of spare components and emergency operation procedures.
- Post-HEMP plans should focus on swift repair, re-supply, and infrastructure recovery, as well as system-wide power coordination, from the local to national levels.

To mitigate the CME caused EMPs and the consequential GIC impacts, [41] proposed a GIC mitigation algorithm that uses linear sensitivity analysis to find the best switching strategy and minimize the GIC-saturated reactive power loss. In [42] and [43], strategies for placing the blocking devices in transformer neutrals to mitigate the negative GIC impacts in large-scale power systems are presented. The authors in [44] introduced a neutral switching solution that consists of connecting switching devices at the neutral grounding connection point of transformer banks to reduce the GIC impact during GMD events.

V. Conclusion

While the EMP attacks are becoming a new threat to power grids and electronics, the society in general should plan ahead for any type of EMP attacks to the grid and home electronics. This paper demonstrated different classes of EMP threats and mechanisms for detection, protection and mitigation strategies and considerations against EMP attacks in power grids. The current protection mechanisms feature physical equipment based on Faraday cage and EMP shield, and power grid wiring component such as surge protectors. However, the tasks for building more resilience in the grid is still crucial and remain a long way to go. Further plans against EMP attacks could focus on hardware (chips, power supplies, PCB), SCADA and grid control system protection. On the *devices level*, the following practices are suggested: (i) shielding and grounding processing, (ii) limiting the coupling frequency to a narrow band by using separating filters, (iii) using components

which are not easily affected by EMP, like electronic tubes, (iv) considering the replaceability of vulnerable components. On a *system level*, the following actions are recommended: (i) electromagnetic protection to be embedded in the design practices, (ii) selection of frequency hopping spread spectrum communication mode as far as possible, (iii) addition of auto-closed systems to system design, (iv) design of communication networks considering N-1 scenarios. And on a *national level*, efforts should focus on (i) effective emergency plans, (ii) strategies to destroy the enemy's launch platforms, and (iii) appropriate development of EMP weapons to achieve strategic balance. Future research and developments should be focused on developing algorithms for detection of EMP threats, tools for blocking and protection against EMP attacks, i.e., structural resilience, and strategies for swift response and recovery following the EMP attacks, i.e., operational resilience.

REFERENCES

[1] J. S. Foster Jr and *et al.*, "Report of the commission to assess the threat to the united states from electromagnetic pulse (EMP) attack: Critical national infrastructures," Electromagnetic Pulse (EMP) Commission Mclean VA, Tech. Rep., 2008.

[2] Electric Power Research Institute, "Electromagnetic pulse (EMP) and the power grid," August 2013, [Online] Available at: https://www.eiscouncil.org/App_Data/Upload/58a9c013-3188-41c8-8957-4a260ed248bc.pdf, Accessed: 2019.

[3] "A basic primer in lightning effects and protection," [Online] Available at: https://studylib.net/doc/18869279/a-basic-primer-in-lightning-effects-and-protection,Accessed:2019.

[4] T. J. Overbye, " PSERC Tutorial: High Altitude Electromagnetic Pulse (HEMP) Impacts on the Grid ," Tech. Rep., June 2016.

[5] C. Kopp, "The electromagnetic bomb-a weapon of electrical mass destruction," Monash Univ Clauton (Australia), Tech. Rep., 1996.

[6] J. Emanuelson, "EMP history," [Online] Available at: http://www.futurescience.com/emp/EMP-history.html, Accessed: 2019.

[7] U.S. Department of Energy, "U.S. department of energy electromagnetic pulse resilience action plan," 2017.

[8] C. DoD, "Department of defense global information grid architectural vision," 2007, accessed: 2019.

[9] J. Emanuelson, "E1, E2 and E3," [Online] Available at: http://www.futurescience.com/emp/E1-E2-E3.html,Accessed:2019.

[10] J. Venable, "Electromagnetic Pulse Would Devastate Our Power Grid," 2018, the Daily Signal, [Online] Available at: https://https://www.dailysignal.com/2018/12/14/electromagnetic-pulse-would-devastate-our-power-grid-here-are-3-steps-we-must-take-now.

[11] E. S. William Radasky, "Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid," pp. 1–1, 2010, accessed: 2019.

[12] T. Harris, "How e-bombs work," 2003, [Online] Available at: https://science.howstuffworks.com/e-bomb.htm, Accessed: 2019.

[13] K. Berent, "Electromagnetic Pulse (EMP) Grid Resiliency Project," Electric Power Research Institute, Tech. Rep., 2016.

[14] T. Harris, "How e-bombs work," 2003, [Online] Available at: https://science.howstuffworks.com/e-bomb3.htm, Accessed: 2019.

[15] Executive Office of the President, "National electric grid security and resilience action plan," 2016, [Online] Available at: https://www.hsdl.org/?abstract&did=797486, Accessed: 2019.

[16] G. H. Baker and S. Volandt, "Cascading consequences: Electrical grid critical infrastructure vulnerability," May 2018, [Online] Available at: https://www.domesticpreparedness.com/resilience/cascading-consequences-electrical-grid-critical-infrastructure-vulnerability.

[17] National Coordinating Center for Communications (NCC), "Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment," 2019, [Online] Available at: https://www.dhs.gov/sites/default/files/publications/19_0307_CISA_EMP-Protection-Resilience-Guidelines.pdf, Accessed: 2019.

[18] E. Savage, J. Gilbert, and W. Radasky, "The Early-Time (E1) High-altitude Electromagnetic Pulse (HEMP) and Its Impact on the US Power Grid," *Report Meta-R-320 for Oak Ridge National Laboratory*, 2010.

[19] P. Dehghanian, S. Aslan, and P. Dehghanian, "Maintaining electric system safety through an enhanced network resilience," *IEEE Transactions on Industry Applications*, vol. 54, no. 5, pp. 4927–4937, Sept.-Oct. 2018.

[20] B. Zhang, P. Dehghanian, and M. Kezunovic, "Optimal allocation of pv generation and battery storage for enhanced resilience," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 535–545, 2017.

[21] P. Dehghanian, B. Zhang, T. Dokic, and M. Kezunovic, "Predictive risk analytics for weather-resilient operation of electric power systems," *IEEE Trans. on Sustainable Energy*, vol. 10, no. 1, pp. 3–15, 2019.

[22] P. Dehghanian, "Power system topology control for enhanced resilience of smart electricity grids," Ph.D. dissertation, Texas A&M University, 2017.

[23] Z. Tayebi, "The use of panel time-series data in modeling agricultural markets," Ph.D. dissertation, University of Florida, 2019.

[24] *Enhancing the resilience of the Nation's electricity system*. National Academies of Sciences, Engineering, and Medicine, 2017.

[25] D. H. Boteler and R. J. Pirjola, "Modelling geomagnetically induced currents produced by realistic and uniform electric fields," *IEEE Transactions on Power Delivery*, vol. 13, no. 4, pp. 1303–1308, Oct 1998.

[26] T. J. Overbye, T. R. Hutchins, K. Shetye, J. Weber, and S. Dahman, "Integration of geomagnetic disturbance modeling into the power flow: A methodology for large-scale system studies," in *2012 North American Power Symposium (NAPS)*, Sep. 2012, pp. 1–7.

[27] R. A. Walling, "Potential impacts of harmonics on bulk system integrity during geomagnetic disturbances," in *2013 IEEE Power Energy Society General Meeting*, July 2013, pp. 1–5.

[28] V. D. Albertson, J. M. Thorson, R. E. Clayton, and S. C. Tripathy, "Solar-induced-currents in power systems: Cause and effects," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-92, no. 2, pp. 471–477, March 1973.

[29] Xuzhu Dong, Yilu Liu, and J. G. Kappenman, "Comparative analysis of exciting current harmonics and reactive power consumption from gic saturated transformers," in *2001 IEEE Power Engineering Society Winter Meeting. Conference Proceedings*, vol. 1, Jan 2001, pp. 318–322.

[30] X. Kong and Y. Xie, "An active e-field sensor based on laser diode for EMP measurement," in *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)*, Aug 2014, pp. 1–4.

[31] J. G. Kappenman, V. D. Albertson, and N. Mohan, "Current transformer and relay performance in the presence of geomagnetically-induced currents," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-100, no. 3, pp. 1078–1088, March 1981.

[32] P. Ripka, K. Draxler, and R. Styblikova, "Measurement of dc currents in the power grid by current transformer," *IEEE Transactions on Magnetics*, vol. 49, no. 1, pp. 73–76, Jan 2013.

[33] T. Breckenridge, T. Cumming, and J. Merron, "Geomagnetic induced current detection and monitoring," 2001.

[34] N. Chandler, "How faraday cages work," [Online] Available at: https://science.howstuffworks.com/faraday-cage.htm, Accessed: 2019.

[35] Meteolabor, "Lighting and EMP protection devices," 2016, [Online] Available at: http://www.meteolabor.ch/fileadmin/user_upload/pdf/SuccessStory/EMP-Standard.pdf, Accessed: 2019.

[36] ——, "MAK modular attachement kit," pp. 12,13, 2019, [Online] Available at: http://www.meteolabor.ch/fileadmin/user_upload/pdf/SuccessStory/Meteolabor-MAK-Catalog-R2-2019_e_d.pdf.

[37] "The Worlds First Entire Home EMP protection Device — EMP Shield," [Online] Available at: https://empshield.com, Accessed: 2019.

[38] U.S. Department of Homeland Security, "Strategy for protecting and preparing the homeland against threats of electromagnetic pulse and geomagnetic disturbances," 2018, [Online] Available at: https://www.dhs.gov/publication/protecting-and-preparing-homeland-against-threats-electromagnetic-pulse-and-geomagnetic.

[39] ETS-Lindgren, "Solutions for electromagnetic pulse (EMP)," 2018, [Online] Available at: http://www.ets-lindgren.com/sites/etsauthor/General_Brochures/EMP_General_brochure.pdf, Accessed: 2019.

[40] Y.-N. Li and Z.-L. Tan, "front-end electromagnetic protection module based on vhf communication," in *2018 International Conference on Electronics Technology (ICET)*. IEEE, 2018, pp. 142–146.

[41] M. Kazerooni, H. Zhu, and T. J. Overbye, "Mitigation of geomagnetically induced currents using corrective line switching," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 2563–2571, May 2018.

[42] H. Zhu and T. J. Overbye, "Blocking device placement for mitigating the effects of geomagnetically induced currents," *IEEE Transactions on Power Systems*, vol. 30, no. 4, pp. 2081–2089, 2014.

[43] A. H. Etemadi and A. Rezaei-Zare, "Optimal placement of gic blocking devices for geomagnetic disturbance mitigation," *IEEE Transactions on Power Systems*, vol. 29, no. 6, pp. 2753–2762, 2014.

[44] B. Kovan and F. de León, "Mitigation of geomagnetically induced currents by neutral switching," *IEEE Transactions on Power Delivery*, vol. 30, no. 4, pp. 1999–2006, Aug 2015.