Journal of Energy and Power Engineering 19 (2025) 31-35
doi: 10.17265/1934-8975/2025.01.004

The Looming Threat

Blackout of the National Grid and Critical Infrastructure

(A National Security Crisis)

Bahman Zohuri

Ageno School of Business, Golden Gate University, San Francisco 94105, California, USA

Abstract: The national grid and other life-sustaining critical infrastructures face an unprecedented threat from prolonged blackouts, which could last over a year and pose a severe risk to national security. Whether caused by physical attacks, EMP (electromagnetic pulse) events, or cyberattacks, such disruptions could cripple essential services like water supply, healthcare, communication, and transportation. Research indicates that an attack on just nine key substations could result in a coast-to-coast blackout lasting up to 18 months, leading to economic collapse, civil unrest, and a breakdown of public order. This paper explores the key vulnerabilities of the grid, the potential impacts of prolonged blackouts, and the role of AI (artificial intelligence) and ML (machine learning) in mitigating these threats. AI-driven cybersecurity measures, predictive maintenance, automated threat response, and EMP resilience strategies are discussed as essential solutions to bolster grid security. Policy recommendations emphasize the need for hardened infrastructure, enhanced cybersecurity, redundant power systems, and AI-based grid management to ensure national resilience. Without proactive measures, the nation remains exposed to a catastrophic power grid failure that could have dire consequences for society and the economy.

Key words: National grid blackout, critical infrastructure security, EMP, cyberattack resilience, AI-powered grid protection, ML in energy security, power grid vulnerabilities, physical attacks on infrastructure, predictive maintenance for power grids, energy crisis and national security.

1. Introduction

A prolonged blackout of the national grid and other life-sustaining critical infrastructures for over a year poses one of the gravest threats to national security. The possibility of such an event, whether from a man-made attack or a natural disaster, has dire implications for millions of people. Studies indicate that an attack on just nine of the nation’s 55,000 electrical substations within United States as illustrated in Fig. 1 as a sample of electrical grid and sub-station could lead to a catastrophic coast-to-coast blackout, lasting up to 18 months. The consequences would be devastating, affecting essential services such as water treatment, healthcare, communication, and transportation are few that can be named as categorized below and its devastating effect to the society where we live and demand for source electricity transmission from source to consumer, is very high.

2. Understanding the Threats

The threats to the national grid can be broadly categorized into three main types.

(1) Physical Attacks

Deliberate acts of sabotage targeting power stations, transformers, and substations could severely cripple the grid. Small-scale attacks in the past have demonstrated how vulnerable power infrastructure is to organized assaults. Fig. 2 below, is illustration of such physical attack that substation attacks prompt national review of U.S. electric grid (NYSE: DUK) [1-3].

Corresponding author: Bahman Zohuri, Ph.D., adjunct professor, research field: electrical and computer engineering.

Fig. 1 High voltage national grids electricity substation.
(Source: www.wikipedia.org)

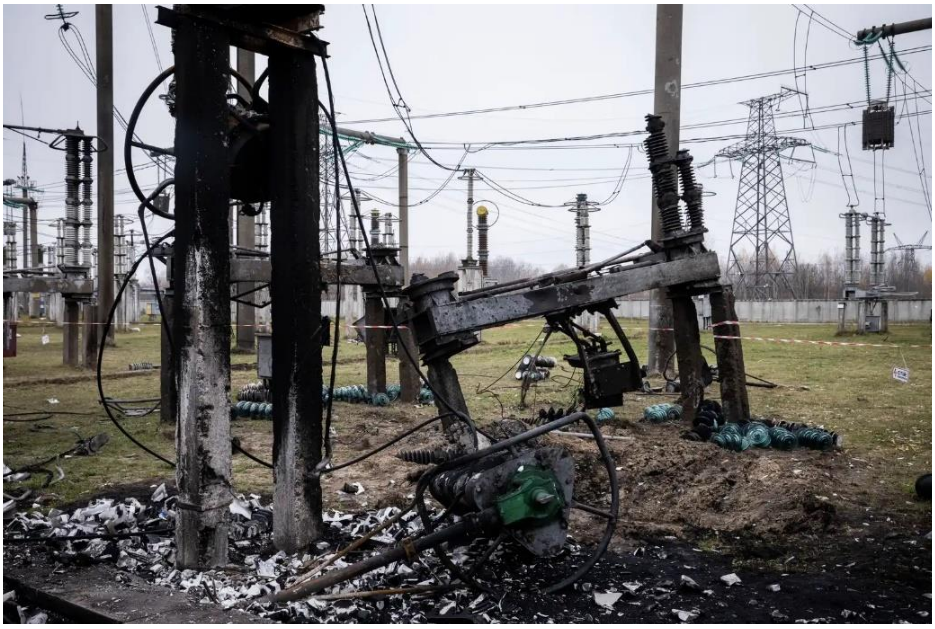

Fig. 2 Substation attacks prompt national review of U.S. Electric Gri.
(Source: NYSE: DUK)

(2) EMP (Electromagnetic Pulse) Events

EMP events, whether from high-altitude nuclear detonations or geomagnetic storms, have the potential to disrupt and damage critical electrical components, leading to a nationwide blackout as illustrated in Fig. 3. Historical instances, such as the Carrington Event of 1859, show the devastating effects solar storms can have on electrical systems [4-6].

(3) Cyberattacks

With the increasing digitalization of power grids, cyberattacks present an ever-growing threat. Malicious actors, including nation-states and terrorist organizations, could exploit vulnerabilities in grid control systems, causing widespread disruptions and potentially irreversible damage. As Fig. 4 illustrates, cybercriminals continue to look for new and innovative ways to infiltrate organizations. As threats continue to grow and evolve, you need to understand what your organization is up against to defend against cybersecurity threats from criminals who exploit vulnerabilities to gain access to networks, data and confidential information [7-10].

Note that: A highly sophisticated, covert danger on a computer system or network where an unauthorized person is able to infiltrate, evade detection, and collect information for political or commercial purposes is known as an APT (advanced persistent threat). The primary goal is usually financial gain or political espionage, and it is typically undertaken out by criminals or nation-states. APTs are still linked to nation-state actors who want to acquire trade secrets or government information, but cybercriminals without any specific affiliation can also utilize APTs to steal data or intellectual property.

An APT typically combines fewer complex techniques to gain access to the system (such as malware and spear phishing) with more sophisticated strategies, such as a good amount of intelligence gathering. The target is compromised, and access is maintained using a variety of techniques.

Fig. 3 Warnings of physical EMP.
(Source: www.wikipedia.org)

Fig. 4 Cyber security attack to the electrical grid and sub-stations.
(Source: www.wikipedia.org)

The most popular attack strategy involves reading an authentication database, determining which accounts have the necessary rights, and then using that information to compromise assets in order to spread from a single machine to a whole network. Within the attacked environment, APT hackers will also install backdoor programs, such as trojans, on hacked systems. They take this action to ensure that they can reenter even if their credentials change later.

The majority of APT organizations are either agencies or affiliates of governments in independent states. A skilled hacker who works full-time for the aforementioned could also be an APT. These state-sponsored hacking groups typically possess the means and skills necessary to thoroughly investigate their target and identify the most advantageous method of entry.

3. Impacts of a Prolonged Blackout

A nationwide blackout lasting over a year would have catastrophic repercussions, including:

- Collapse of water and food supply chains: Without power, water purification and distribution would cease, leading to severe shortages. Food supply chains relying on refrigeration, transportation, and production would also fail.
- Breakdown of healthcare services: Hospitals and emergency medical services would struggle to function without reliable electricity, leading to increased mortality rates.
- Financial and economic devastation: Businesses and financial institutions would experience systemic failures, leading to economic collapse and mass unemployment.
- Civil unrest and national security risks: The absence of essential services would lead to widespread chaos, civil unrest, and a breakdown of law and order.

4. AI (Artificial Intelligence) and ML (Machine Learning): A Defense against Grid Attacks

The integration of AI and ML technologies could play a pivotal role in mitigating and preventing these threats [11]:

- Predictive maintenance and anomaly detection: AI-powered algorithms can analyze vast amounts of data from sensors and detect anomalies in real time, allowing for proactive maintenance and failure prevention.
- Cybersecurity enhancement: AI-driven security systems can identify and neutralize cyber threats before they infiltrate grid networks, significantly reducing the risk of cyberattacks.
- Automated threat response systems: ML models can help automate rapid response mechanisms to physical and digital threats, ensuring immediate countermeasures.
- EMP shielding and recovery strategies: AI can assist in developing adaptive shielding strategies against EMP events and optimizing recovery procedures to restore power more efficiently.

5. Policy Recommendations and Future Directions

To safeguard the national grid from these existential threats, governments and utility companies must:

- Invest in hardened infrastructure: Strengthening substations and transformers against physical attacks and EMPs.
- Enhance cybersecurity protocols: Implementing AI-driven cybersecurity frameworks to protect grid networks from malicious actors.
- Develop redundant power systems: Creating microgrids and decentralized power sources to ensure continued operations during disruptions.
- Implement AI-based grid management: Utilizing AI for real-time monitoring and adaptive response strategies to mitigate failures.

6. Conclusion

The potential for a prolonged blackout of the national grid and other critical infrastructures is a national security crisis that cannot be ignored. Whether due to a physical attack, EMP event, or cyber threat, the consequences would be devastating. However, leveraging AI and ML technologies provides an opportunity to enhance grid resilience and security. Governments, utility providers, and technology leaders must collaborate to fortify the power infrastructure and mitigate these threats before disaster strikes [11-14].

References

[1] Executive Office of the President. 2022. *National Security Strategy*. New York: The White House.

[2] U.S. Department of Energy. 2023. *Grid Modernization and Resilience*. New York: Office of Electricity.

[3] North American Electric Reliability Corporation (NERC). 2023. *2023 State of Reliability Report*. New York: NERC.

[4] EMP Commission. 2017. *Report on the Threat from Electromagnetic Pulse (EMP)*. New York: U.S. Congressional Commission.

[5] National Institute of Standards and Technology (NIST). 2021. *Cybersecurity Framework for Critical Infrastructure Protection*. Gailthersburg: NIST.

[6] Carrington, R. C. 1859. "Description of a Singular Solar Event." *Monthly Notices of the Royal Astronomical Society* 20 (1): 13-5.

[7] National Academies of Sciences, Engineering, and Medicine. 2017. *Enhancing the Resilience of the Nation's Electricity System*. Washington: National Academies of Sciences, Engineering, and Medicine.

[8] Federal Energy Regulatory Commission (FERC). 2022. *Security Measures for the Electric Grid*. Washington: FERC.

[9] International Energy Agency (IEA). 2023. *AI and Machine Learning for Grid Security*. New York: IEA.

[10] Cybersecurity and Infrastructure Security Agency (CISA). 2022. *Critical Infrastructure Risk Management*. Washington: CISA.

[11] Zohuri, B., and Zadeh, S. 2020. *Artificial Intelligence Driven by Machine Learning and Deep Learning*. Hauppauge: Nova Science Pub Inc.

[12] Zohuri, B., and Mossavar-Rahmani, F. 2024. "The Symbiotic Evolution: Artificial Intelligence (AI) Enhancing Human Intelligence (HI): An Innovative Technology Collaboration and Synergy." *Journal of Material Sciences & Applied Engineering* 3 (1): 1-5.

[13] Zohuri, B. 2023. "Artificial Super Intelligence (ASI): The Evolution of AI beyond Human Capacity." *Current Trends in Engineering Science* 3 (7): 1-5.

[14] Zohuri, B. 2023. "The Dawn of Artificial General Intelligence Real-Time Interaction with Humans." *Journal of Material Sciences & Applied Engineering* 2 (4): 29.