# Chapter 33
# The USA Electrical Grid:
## Public Perception, Cyber Attacks, and Inclement Weather

**Eugene de Silva**
*Virginia Research Institute, USA*

**Eugenie de Silva**
*University of Leicester, UK*

## ABSTRACT

*This chapter provides a discussion of the United States (U.S.) electrical grid. In particular, the chapter explicates the vulnerabilities of the electrical grid by placing a focus on public perception, cyber-attacks, and the inclement weather. The authors elaborate on the necessity of contingency plans, heightened security through the utilization of smart grids and microgrids, and improved cooperation between the Intelligence Community (IC) and the public. This chapter further expands on the importance of government agencies establishing community outreach programs to raise public awareness and build a strong relationship between U.S. security agencies and the public. Overall, this chapter highlights the key issues pertaining to the electrical grid, and provides solutions and strategies to resolve them.*

## INTRODUCTION

It has become increasingly apparent that the technologically dependent culture of the United States (U.S.) has heightened risks to national security and intelligence practices. Although the mass majority may not be aware, the threat to critical infrastructure in the U.S. has persisted for years. This chapter explores the vulnerability of the current U.S. electrical grid system, and possible threats that could cripple the entire nation with greater consequences than that have been caused by any of the recent attacks on the U.S. by terrorist/radical groups. The long-term implications and the possible catenation of disasters are discussed whilst also explaining what immediate measures can be taken in this regard.

Due to the overwhelming difficulty in prediction and prevention, cyber-attacks are a particularly effective and dangerous method to gain the upper hand. As technology has advanced, individuals within

DOI: 10.4018/978-1-5225-7912-0.ch033

the security fields have continuously reevaluated their procedures and have sought appropriate mechanisms to protect vital systems from the extreme threats that are cyber-attacks. With a view to enhancing security systems, cyber security officials have honed their skills in order to identify novel measures to detect and deter cyber-attacks; however, protecting U.S. cyber systems is a difficult task, especially due to the sheer size of network systems and the uproar that may result due to public angst toward evolving times that necessitate greater security. However, issues in protecting cyber systems also stem from a lack of trust from the public toward intelligence personnel and agencies that have resulted in poor public relations and have further promulgated a weak intelligence system.

The twenty-first century has witnessed heinous crimes and acts of terror, yet the consequences of these acts will seemingly be lesser in comparison to the effects of possible future cybercrime. An unsecure electrical grid system and a society unwilling to change for their benefit will certainly be the downfall of U.S. society in the near future as U.S. adversaries slowly, but steadily gain the necessary power and knowledge to undermine the integrity of major cyber systems. To turn on any major news outlet on the television in the U.S. is to firstly expose one's self to the partisanship nature of politics and secondly to open one's self to repetitive discussions of the threats posed by state and non-state actors as a result of cyber-attacks. Most recently, the hacking of Sony and the release of allegedly "embarrassing" financial records and incriminating emails highlighted the effects of a cyber-attack even at a considerably low level. It is quite simple to convey the message of the harsh nature of possible cyber-attacks; yet, it is much more difficult to provide a resolution. There are many within the field who seek to improve the stability and security of U.S. cyber systems; however, it certainly seems that the public is wary of the extent to which improvements in the field actually benefit the nation. With this taken into consideration, this chapter also provides a brief reasoning to explain why continuous discussions of the stability of the cyber field to raise awareness will result in heightened cyber standards in the U.S.

The threats of cyber-attacks are undoubtedly present, yet the electrical grid also faces other issues, such as the inclement weather. The effects of climate change, as explained within this chapter, pose major threats to the stability of the electrical grid. The unpredictability of the weather, and the lack of protection from any inclement weather could result in a major breakdown of the grid. The weather, in actuality, may present greater issues than a cyber-attack, due to the inability to avoid weather unlike the ability to deter cyber-attacks that are detected. For example, even if an extreme storm is detected, there is no way to eradicate the storm without allowing nature to run its full course.

Of course, if the weather was simply the issue, then researchers, academics, and practitioners could aim to make this the focus of their investigations to secure the grid. However, this also leads to the issue of political beliefs and ideologies that cause individuals who could play vital roles in the improvement of the system to shy away from the topic. Accordingly, a majority of the U.S. public has apparently dismissed the topic, due to a lack of initiative taken to discuss issues related to the electrical grid. Without much public opinion on the topic, there has been little impetus for politicians to also be involved in the discussion of the issue. The lack of priority placed on this issue by U.S. politicians has also seemingly resulted in limited progress.

## BACKGROUND

It was President Barack Obama who stated that "it is now clear this cyber threat is one [of] the most serious economic and national security challenges we face as a nation" ("Cyber War: Sabotaging the