ISSN: 2708-7786

Cyber Threats to Pakistan's National Power Grid

Authors
Dr. Hammaad Salik[1] , Rao Ibrahim Zahid[2] , Babar Khan Akhunzada[3]

Abstract

As Pakistan continues to experience an expansion of its cyber environment and engagement in the global IT market, the nation remains exposed to a plethora of cyber threats, including cybercrime, espionage, and cyber warfare. The targeting of the country's vital infrastructure, including power and energy systems, military and government networks, and financial institutions, has resulted in a number of cyber-attacks that have led to power outages, financial losses, and disruptions to essential services.[4] The incorporation of technology in Pakistan's electrical power infrastructure has become an indispensable aspect of contemporary society as it enables the efficient management and distribution of electricity; however, it also escalates the potential ramifications of a cyber-attack on these systems in the absence of adequate security measures. Nevertheless, the potential consequences of a cyber-attack on these systems are often overlooked and undervalued due to a lack of awareness and comprehension of the potential risks and a lack of investment and resources devoted to cybersecurity. This paper looks into this aspect in detail.

Keywords: Cyber threat, national security, cyber attacks, power grid, electricity

Introduction

The World Economic Forum (WEF) has acknowledged the increasing frequency and severity of cyber-attacks on critical infrastructure as a “cyber pandemic,” with an increase of 300% in the U.S. itself, particularly in the wake of the COVID-19 pandemic. Targets of these attacks include Operational Technology (OT) which connects Industrial Control Systems (ICS) and critical

[1] Dr. Hammaad Salik is a consultant to the Prime Minister’s Task Force on Knowledge Economy (Pakistan) and a Strategic Warfare Group (SWG) member advisory. Email: salik1@umbc.edu.

[2] Rao Ibrahim Zahid is a Prime Minister’s Task Force on Knowledge Economy (Pakistan) consultant and a member advisory Strategic Warfare Group (SWG). Email: ibrahimzahid1991@gmail.com.

[3] Babar Khan Akhunzada is a cyber wizard and entrepreneur, Founder of SecurityWall, a cyber security firm focused on Digital Risk Protection and Hybrid Auditing approach . Email: founder@securitywall.co.

[4] National Cyber-Forensics and Training Alliance (NCFTA). (2018). Cyber Attribution: Understanding the Challenges and Considerations.

systems that are interlinked and connected widely.[5] These attacks on ICS can potentially disrupt essential services, causing chaos and financial losses for individuals and organizations. The susceptibility of vital infrastructure to cyber incursions, including power grids, presents a formidable threat to the stability and security of nations.[6] Nevertheless, many countries, among them Pakistan, have yet to fully comprehend and tackle the potential ramifications of a cyber-attack on their power grids. Research has indicated a discernible increase in the recurrence and intricacy of cyber-attacks directed at power grids, with nation-state actors being identified as possessing both the technical acumen and strategic intent to carry out such nefarious activities. The power grid, a term synonymous with the electrical grid, represents a labyrinthine network of various technological mechanisms and equipment that generate electricity. These mechanisms are intricately linked within a grid infrastructure, and the grid's operations are constantly monitored through security systems devised to identify any deviation or irregularity in the power flow. A nefarious interference with the power grid can substantially harm all devices interlinked within the grid and those not actively engaged with the grid.[7]

As scholars, it is crucial for us to inquire into the underlying causes and potential consequences of a nationwide blackout, with specific regard to how these factors may vary in relation to the duration of the event. A nationwide blackout, as defined, constitutes a comprehensive disruption of the national power infrastructure, leading to a widespread cessation of electricity supply. The implications of such an occurrence can diverge significantly, depending upon the origin of the blackout and its duration. Among the most common ramifications of a nationwide blackout are:

1. Disruption of essential services: Hospitals, water treatment plants, and other critical infrastructure may be affected, leading to the interruption of essential services such as healthcare, water supply, and communication.
2. Loss of power to homes and businesses: Millions of people may be left without power, making it difficult or impossible to cook, heat, or cool homes and businesses.
3. Economic disruption: Businesses may be forced to shut down, leading to lost productivity and revenue. This can also result in job losses, reduced GDP, and other economic impacts.
4. Traffic and transportation issues: Traffic lights, trains, and other public transportation may stop functioning, causing delays and accidents.
5. Safety concerns: People may be at risk of injury or death due to the lack of power to essential services such as hospitals, elevators, and emergency response systems.

[5] Protecting critical infrastructure from a cyber pandemic
https://www.weforum.org/agenda/2021/10/protecting-critical-infrastructure-from-cyber-pandemic/

[6] Lee, R. M., & Totzke, S. A. (2018). The Impact of Cyberattacks on the Power Grid.

[7] Stockton, P., & Hultquist, J. R. (2016). Cybersecurity in the Electric Power Industry.

6. Security concerns: A nationwide blackout can also provide opportunities for criminals and hostile actors to carry out attacks, looting, or other malicious activities.

From a global perspective, the nations of Russia, the United States, and China possess highly advanced cyber capabilities and have been known to engage in nation-state cyber-attacks.[8] Russia has been associated with a number of high-profile cyber-attacks, including the 2015 assault on the Ukraine power grid, which was the first known instance of a cyber-attack resulting in a power outage. This attack utilized a combination of spear-phishing emails and malware to infiltrate the network and manually operated breakers to shut off power to over 225,000 customers. Russia has also been accused of hacking into the power grid systems of the United States to gain access to control systems.[9] The United States boasts a well-funded and highly skilled cyber-military division known as the United States Cyber Command, which is responsible for defending U.S. military networks and conducting cyber operations. The U.S. government has also invested heavily in protecting critical infrastructure, including the power grid. In 2007, the U.S. Department of Homeland Security (DHS) conducted a demonstration called the Aurora Generator test, which simulated a cyber-attack on a power generator, causing it to malfunction and shut down, resulting in a power outage.[10] This test was significant in that it marked one of the first demonstrations to show that a cyber-attack on the power grid could cause a physical disruption of the power system. China is acknowledged to possess a sophisticated cyber espionage program and has been accused of hacking into power grid systems and other critical infrastructure in the United States.[11] Additionally, China has been actively developing its cyber-warfare capabilities and has been linked to several cyber-attacks targeting the power grid and other critical infrastructure.[12]

[8] Atlamazoglou, S. (n.d.). *Cyberwarfare may decide who wins the great power competition*. The National Interest. Retrieved January 28, 2023, from https://nationalinterest.org/blog/reboot/cyberwarfare-may-decide-who-wins-great-power-competition-199404

[9] Park, D., & Walstrom, M. (2017, October 11). *Cyberattack on critical infrastructure: Russia and the Ukrainian power grid attacks*. The Henry M. Jackson School of International Studies. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/; Perez, Evan. “U.S. Official Blames Russia for Power Grid Attack in Ukraine.” CNN. 02-11-2016. http://www.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html

[10] Waltman, C. (2016, November 14). *Aurora: Homeland Security’s secret project to change how we think about cybersecurity*. Muck Rock. https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/

[11] Press Release. (2014, May 19). *U.S. charges five Chinese military hackers for cyber espionage against U.s. corporations and a labor organization for commercial advantage*. Department of Justice - Office of Public Affairs. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[12] Bateman, J. (2022). *Preventing Chinese Sabotage in a Crisis*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/04/25/preventing-chinese-sabotage-in-crisis-pub-86922

The recent blackout that occurred in Pakistan on January 23rd, 2023, has brought to light the vulnerability of the country's power grid to potential cyber-attacks. This is not the first incident of such an attack, and the last was witnessed in January of 2021, when the nation of 220 million stood still, engulfed in total and utter darkness.[13] In the more recent instance, the Ministry of Energy initially attributed the outage to a technical failure and then sought to downplay the outage as an intentional turn-off as part of the energy-saving initiative in the face of the current energy crisis.[14] Through an examination of analogous case studies pertaining to prolonged power grid failures, a distinct causal factor has been identified. While previous instances of widespread blackouts have been attributed to "technical" causes, a closer examination reveals that the underlying technicality lies within the realm of cyber security and that the recent incident may have resulted from a malicious cyber-attack. The “cascading effect” on the grid that followed can be described as a power outage occurring in one area and causing a domino effect, leading to power outages in other areas.[15] This can happen for several reasons, such as equipment failure, human error, or a cyber-attack. When a power plant or transmission line goes down, the sudden loss of power can cause power to be redirected to other areas, leading to an overload, and causing additional power plants or transmission lines to fail.[16] This chain reaction can quickly spread throughout the power grid, causing a widespread blackout. Moreover, if the grid is not configured with adequate protection and control mechanisms, the cascading effect can cause damage to the grid infrastructure that may take weeks or months to repair. However, it is not only the physical failures that pose a threat to the power grid and the cyber threats. Several cyber threats can affect Pakistan's power grid, including:

1. Advanced Persistent Threats (APTs): APTs are targeted attacks typically launched by nation-state actors with the intent of gaining prolonged access to a network or system, which can be leveraged to steal sensitive information, disrupt operations, or cause physical damage to critical infrastructure.
2. Distributed Denial of Service (DDoS) attacks: DDoS attacks inundate networks or systems with traffic through compromised devices, potentially causing unavailability of power grid operations or physical damage to infrastructure.
3. Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) attacks: ICS and SCADA attacks target the systems and networks that regulate and

[13] Salik, H., & Zahid, R. I. (2022, January 31). *When the lights go out: A cyber attack, A nation unprepared*. South Asia Journal. http://southasiajournal.net/when-the-lights-go-out-a-cyber-attack-a-nation-unprepared/

[14] Pakistan’s energy minister sought to downplay a power outage that left 220 million people without power https://qz.com/pakistan-outage-power-blackout-1850017609

[15] Schäfer, B., Witthaut, D., Timme, M. *et al.* Dynamically induced cascading failures in power grids. *Nat Commun* 9, 1975 (2018). https://doi.org/10.1038/s41467-018-04287-5

[16] Rittinghouse, J. W., & Ransome, J. F. (2010). Scada Systems and Cyber Security.

oversee critical infrastructure, such as power plants and transmission lines, which can lead to physical damage or impede power grid operations.

4. Phishing and social engineering attacks: These attacks utilize email and phone phishing to deceive individuals into revealing sensitive information or installing malware, which can be employed to pilfer sensitive information or gain access to power grid systems.
5. Ransomware attacks: These attacks, which use malware to encrypt a network or system's files and demand a ransom in exchange for the decryption key, can disrupt power grid operations or cause physical damage to infrastructure.

Recent case studies of prolonged power grid failures have led to reevaluating the underlying causes of such incidents. While traditional explanations have often cited technical issues as the primary cause, there is growing evidence to suggest that the technicality of these failures may be rooted in the cyber realm. This is particularly evident in the case of the Indian state-sponsored Advanced Persistent Threat (APT) group known as "SideWinder," which is suspected of being responsible for the recent power outage in Pakistan. The group, which has also been referred to as "Razor Tiger," "T-APT-04", and "RattleSnake," is presumed to be responsible for the recent power outage in Pakistan. Although conclusive attribution will still need to be conducted,[17] fragmented evidence of the attack has surfaced. This evidence includes the dissemination of Pakistan’s NTDC's Grid Station Information System (GSIS) dashboard screenshots on Telegram groups. These screenshots reveal informative details of the affected power grid's Asset Management System (AMS). Before this incident, SideWinder had been identified as having targeted Pakistan’s National Electric Power Regulatory Authority (NEPRA) through malware known as "WarHawk." Specifically, this malware was employed to infiltrate the NEPRA official website and spread malware by distributing a legitimate government advisory.[18]

For the defenders of the grid in Pakistan, it is crucial to understand that nation-state actors and APTs are intentionally seeking the initiative to conduct cyber operations below the threshold of an armed conflict. These operations, short of an armed conflict, provide strategic benefits by allowing nation-states or organizations to gather intelligence, disrupt a target's operations, or influence their decision-making without escalating the situation to a full-scale military conflict in, through, and from cyberspace. This allows these nation-state actors and state-sponsored APTs to persistently redistribute power in the international system by influencing the strategic decision calculus of an opponent and allowing cumulative gains to be made.

Additionally, it allows for a more covert and deniable approach, making it more difficult for the targeted nation or group to respond or attribute the attack to a specific source. We, as authors, also posit that Pakistan's critical infrastructure, specifically the power grid, serves as a

[17] Kochin, M. S., & Larson, M. L. (2017). Proving and Disproving Cyber Attacks.

[18] New WarHawk malware spread by the SideWinder APT in Pakistan
https://izoologic.com/2022/10/27/new-warhawk-malware-spread-by-the-sidewinder-apt-in-pakistan/

convenient "cyber test bed" for testing and examining various techniques in cyber warfare.[19] This is primarily due to inadequate laws and regulations to safeguard against cyber-attacks, coupled with the power grid's apparent ease of access and susceptibility. Furthermore, the potential for significant real-world consequences stemming from a successful cyber-attack on the infrastructure further exacerbates the vulnerability of Pakistan's power grid. This notion is supported by various reports and studies highlighting Pakistan's weak cybersecurity framework, lack of regulations, and inadequate incident response capabilities.

As cyber threats continue to evolve and target critical infrastructure, organizations in the industrial control systems and energy sectors must remain vigilant in their defensive strategies to protect against advanced persistent threat (APT) groups and other malicious actors. However, it is crucial to consider the defense mechanisms and understand the potential causes and effects of cyber-attacks on Pakistan's critical infrastructure, particularly its power grid. The consequences of such incidents can be severe and far-reaching, and proactive measures must be taken to mitigate these risks. One such measure is the regular assessment of potential vulnerabilities and the development of adequate incident response plans. Furthermore, education and awareness campaigns can increase public understanding of the potential risks and consequences of cyber-attacks. International partnerships and collaborations can aid in sharing information and best practices.

It is also important to note that identifying and attributing cyber-attacks is a complex task that requires significant resources and expertise. The testimony of cybersecurity experts may be the only way to confirm the occurrence of a cyber-attack in the absence of conclusive evidence. Despite recognizing the potential threat of cyber-attacks on critical infrastructure and establishing government bodies such as the National Cyber Security Authority (NCSA) and the National Response Center for Cyber Crimes (NR3C), Pakistan's cyber security infrastructure remains in a nascent stage of development. A significant increase in resources and investment must be directed toward advancing cybersecurity measures to enhance the nation's resilience to cyber-attacks and improve its ability to respond and recover from such incidents. Additionally, fostering a culture of proactive risk management and disaster anticipation is crucial in mitigating the impact of a potential cyber-attack on the power grid.

[19] "Cyber test bed" is a simulated or emulated environment that is used to test and evaluate the performance, security, and functionality of various types of cyber systems, such as networks, software, and hardware.