What Are the Potential Cybersecurity Vulnerabilities and Cybersecurity Risks Associated with Electrical Grids in The United States?

Stephen Cobb

ODU

The social implications that arise from the vulnerabilities and risks of the electrical grid is that if attacked and power goes out for a decent amount of time society in the United States would not know what to do. From having power in our homes to all the electricity that helps other things function like gas pumps, electricity is essential and without it people would not know what to do. If the power grid is attacked and power goes out, then life would most likely come to a stop. Back in the first 8 months of 2022 the power grid was attacked over 100 times. Most attacks are physical as in domestic terrorist either shooting or do what ever to disrupt power plants, and an attack like that could take multiple weeks or months to repair. Imagen life without power for that long.

Cyber threats are getting bigger and bigger these days and with the modernization of the power grid cyber attacks can be foreseen in the future. Using the confidentiality, integrity, and availability triad (CIA triad) is very important because the more downtime the power grid has the more of it that is getting affected. “With respect to the former, a cyberattack could cause power losses in large portions of the United States that could last days in most places and up to several weeks in others. The economic costs would be substantial. As for the latter concern, the U.S. response or nonresponse could harm U.S. interests. Thus, the United States should take measures to prevent a cyberattack on its power grid and mitigate the potential harm should preventive efforts fail,” (Knake). The economy would be in shambles if the power were to go out for day or months because most of society would not know what to do. Some other examples of why our society could not function without electricity is for one grocery stores couldn’t heat or freeze food, the way to pay for things are mostly electronic, and hospitals would barley be able to function. “Infrastructure would also be affected by power outages. Traffic control systems and fuel distribution networks would stop working. Water would flood the streets due to inefficient

and completely missing pumping. Ploughing and cleaning of the roads would also be out of order, which would result in large scale problems during the wintertime," (Haro, ECT…).

The policy of protecting the power grid is stated in the National Cybersecurity Strategy "ESTABLISH CYBERSECURITY REGULATIONS TO SECURE CRITICAL INFRASTRUCTURE," (Biden). This is important because it shapes the culture around protecting the power grid from cyber-attacks and cyber terrorism. The cultural and subcultural influence around the power grid is simple, in this day and age electricity is everything it is in cars, houses, streetlamps, and banking without it most would not know what to do because most have never lived a life without it. The upgrading the power grid to be resilient to cyber-attacks is essential for the future because an attack can result in a large-scale blackout for a long period of time. There are multiple measures that can be taken like better communication between critical infrastructure, "Data exchange between office network and PCN should only be handled through a dedicated data exchange server, where every file is checked for malware before being passed through. Sometimes, though, as seen in the Ukraine attacks [21], there are other communication channels, such as VPNs, which allow direct communication between the office network and the PCN or remote maintenance lines for vendors or contractors," (Krause ECT…). Determining the weakest link and eliminating it can be another solution because an attacker does not have to attack the biggest grid, it can be a small grid with not that much cyber security because the operators think nothing will happen but in reality, the attacker is gaining access to it and that can open the door for larger grids and can lead to a mass black out. There needs to be solutions made for all the interconnected grids to where all stations have their own security management and is not ran by the bigger operators. The cybersecurity vulnerabilities for power grids can be

mitigated if systems are constantly updated. If a mass blackout were to happen society would be in shambles.

Works Cited

Biden, J. (2023, March 17). *National Cybersecurity strategy*. The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Härö , E., Järvensivu, S.-M., Alilehto, J., & Haravuori, P. (2023, March 16). *Report: Electricity: How long could we survive without it?*. Sweco Group. https://www.swecogroup.com/urban-insight/energy/report-electricity-how-long-could-we-survive-without-it/#:~:text=There%20are%20important%20functions%20in,activities%20which%20are%20increasingly%20electronic.

Knake, R. (2017, April). *A cyberattack on the U.S. Power Grid*. Backend-live. https://backend-live.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021, September 16). *Cybersecurity in power grids: Challenges and opportunities*. MDPI. https://www.mdpi.com/1424-8220/21/18/6225