Shamya Curtis

CYSE 200T

Professor Matthew Umphlet

November 17, 2025

The Vulnerabilities of Critical Infrastructure

Critical Infrastructure refers to systems, facilities, and assets that are vital to the functioning of society and the economy (*What Is Critical Infrastructure?*, 2023). There are many critical infrastructure sectors, such as energy, food, agriculture, healthcare, and public health. These systems and networks are crucial components of society; they enable everyday life through services like electricity and water. Some infrastructure supports national security, including the military and communications. The problem is that these systems have become vulnerable to threats such as cyberattacks, physical attacks, and natural disasters, which can compromise public safety, security, and economic stability. The main threat to critical infrastructure is cyberattacks, given its reliance on digital systems; hackers can gain control or disrupt essential services. Cyberattacks can have devastating effects; for example, an attack on a water plant can contaminate the water supply, leaving a city or state without water. There are solutions to protect critical infrastructure, such as improved employee training, given that human error is one of the most significant risks. Another solution is incident response planning, so the operators can be prepared for when an attack happens and reduce damage. AI can be used for threat detection and to analyze large amounts of data. In order to protect critical infrastructure, we must strengthen cybersecurity controls, implement real-time monitoring, and secure ICS/SCADA systems.

Risks and Threats to Critical Infrastructure

Critical Infrastructure faces many threats and risks due to being under-equipped in the cybersecurity aspect. Factors such as digitalization and automation affected the operational technology by making them more vulnerable to attacks. Malicious actors and state hackers are used to target operational networks. The Economic Forum stated, "connectivity has increased convenience and efficiency, it has also dramatically expanded the attack surface available to malicious actors. Sophisticated state-sponsored hackers and other bad actors now routinely probe and target OT networks, seeking vulnerabilities that they can exploit to cause catastrophic disruptions" (*What Is Critical Infrastructure?* 2023). Hackers use tools such as Artificial Intelligence to automate attacks, making them more efficient. A cybersecurity report referenced The World Economic Forum's Global Cybersecurity Outlook 2025, which shows "escalating geopolitical tensions and increasingly sophisticated threats such as ransomware, AI-driven phishing, and supply chain attacks pose significant risks to sectors like energy, water, and communications."

Hackers can disable essential services that people rely on every day. Attacks on electrical grids can lead to power outages or contaminate water supplies. The effect of cyberattacks on critical infrastructure includes service disruptions, delayed operations, and economic damage. Cyber criminals can easily access systems due to outdated software and weak password habits. "On 18 January 2024, the group accessed control systems at two Texas water facilities and tampered with their water pumps and alarms, causing water to run past designated shutoff levels and overfill storage tanks." ("Investigating Potential Vulnerability of Critical Infrastructure and Way Forward – Recommendations to Enhance Security and Resilience," 2023). This event shows how hackers can compromise these vital systems and cause serious harm.

Solutions on how to protect Critical Infrastructure

1 To protect critical infrastructure from cybersecurity threats, multi-factor authentication is implemented to prevent unauthorized access. In a cybersecurity news article, the author explains multifactor authentication, stating, “Require multiple forms of verification before granting access to critical systems, adding layers of security beyond simple password protection.” Enabling multi-factor authentication can decrease the risk of hackers accessing systems. Poor password habits are a main cause of vulnerabilities in critical systems. Another way to safeguard critical infrastructure is to develop a flexible framework that manages cybersecurity risks and provides guidance. The National Institute of Standards and Technology states, “To strengthen the resilience of this infrastructure, the Cybersecurity Enhancement Act of 20142 (CEA) updated the role of the National Institute of Standards and Technology (NIST) to 'facilitate and support the development of' cybersecurity risk frameworks.” Using a practical framework can offer clear guidelines and best practices to improve security and lower risks. Another solution is to adopt advanced technologies like Artificial Intelligence. Employing such advanced technologies can help protect these systems. “We can employ artificial intelligence (AI) for real-time threat detection and response. AI algorithms analyze vast amounts of data to identify patterns indicative of cyber threats, allowing for swift action.” (Chambers, 2025). AI can detect threats quickly, enabling earlier intervention and preventing significant damage.

Conclusion

Critical infrastructures are vital to society and must be safeguarded. They provide essential services that support daily life, public safety, and national security. Without them, the modern world cannot function. As technology advances, critical infrastructure becomes more susceptible. From outdated software to weak password practices, these systems face significant risks due to

inadequate cybersecurity policies and standards. This matters because these services include clean water, energy, healthcare, and communication. Therefore, protection for these sectors is crucial.

Works Cited

What is critical infrastructure? | ibm. (2023, July 5). https://www.ibm.com/think/topics/critical-infrastructure

The dangerous blind spot in critical infrastructure cybersecurity. (2025, October). World Economic Forum. https://www.weforum.org/stories/2025/10/dangerous-blindspot-in-infrastructure-cybersecurity/

Advisory, C. (n.d.). Securing Critical Infrastructure – Lessons From Recent Cyber Attacks. *Cybersecurity News* . https://cybersecuritynews.com/securing-critical-infrastructure/

Investigating potential vulnerability of critical infrastructure and way forward – recommendations to enhance security and resilience. (2023). *Biomedical Science and Clinical Research*, *2*(1). https://doi.org/10.33140/BSCR.02.01.03

National Institute of Standards and Technology . (n.d.). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology* , *Version 1.1*.

Chambers, S. (2025, November 11). *Cybersecurity in critical infrastructure: Key considerations for protecting vital systems*. DeepThreatAnalytics.Com. https://www.deepthreatanalytics.com/network-security/cybersecurity-critical-infrastructure-key-considerations/