Article 2 Review

The article *"Cybersecurity Risks in Critical Infrastructure Systems"* looks at the weaknesses in important systems like power grids, water supplies, and transportation networks. The main idea is that these systems are being targeted more by cyberattacks, and a big reason for that is that many of them were built before modern cybersecurity threats existed. Because of that, they're often not prepared for today's types of attacks.

Source:
https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/508/149

The article is based on a qualitative review of existing research and real-world cases, rather than new experiments. The authors use past studies, government reports, and examples of actual cyber incidents to find common problems in critical infrastructure systems. From this, they point out issues like outdated software, weak system protections, and poor network security in systems like SCADA.

From a social science perspective, the article connects to ideas like social control, risk, deviance, institutions, and globalization. These systems are part of everyday social life, so when they fail, a lot of people are affected. Cyberattacks are considered deviant behavior because they break rules and disrupt systems society depends on. The article also shows how risk is increasing as society becomes more dependent on technology, and how globalization makes it easier for attacks to come from anywhere in the world.

The article also relates to marginalized groups, since people in low-income areas, rural communities, and older populations are often hit hardest when infrastructure goes down. They usually have fewer resources to recover quickly or protect themselves from disruptions, which can make the impact even worse.

The study highlights that cybersecurity isn't just a technical issue it's a social one too. Protecting critical infrastructure is important because it affects everyday life, public safety, and how stable society is as a whole.