

Cybersecurity Threats to Critical Infrastructure in the Age of IoT

Tyler Provencal

Old Dominion University

IDS 300W: Interdisciplinary Research, Process, and Theory

Patricia Oliver

December 2, 2025

Abstract

Critical infrastructure systems, such as energy grids, water treatment facilities, transportation networks, and healthcare organizations, rely increasingly on Internet of Things (IoT) sensors. While these technologies increase efficiency and responsiveness, they also offer new cybersecurity vulnerabilities that have far-reaching societal implications. This study investigates cybersecurity vulnerabilities to vital infrastructure using an interdisciplinary approach that combines engineering, computer science, political science, economics, and ethics. Engineering and computer science highlight flaws in IoT device architecture, unsecured protocols, and holes in industrial control system (ICS) security. Political science and public policy handle national security concerns, international cyber norms, and regulatory issues. Economics examines the financial consequences of cyberattacks, as well as the costs of mitigation and resilience. Ethics emphasizes organizations' responsibilities to preserve public safety when system breakdowns imperil lives. By combining these viewpoints, this study demonstrates that cybersecurity for IoT-enabled critical infrastructure necessitates more than technical fixes—it necessitates coordinated policy, investment, and ethical accountability. An interdisciplinary framework provides the most comprehensive approach to understanding and combating emerging cyber dangers.

Full Title of Your Paper

As digital systems grow more integrated into everyday life, critical infrastructure has emerged as one of contemporary society's most technologically dependent industries. Power grids, water systems, hospitals, and transportation networks are increasingly reliant on networked sensors, industrial control systems, and IoT devices to function properly. While these technologies boost system performance, they also expose critical services to unprecedented cybersecurity threats. Infrastructure disruptions are no longer restricted to physical failures; a single hack can bring down hospital networks, poison water supplies, or cripple electricity grids, affecting millions of people (Lee & Assante, 2019). Because of the complexity of these systems and the potentially disastrous repercussions of failure, cybersecurity threats to critical infrastructure necessitate an interdisciplinary approach rather than a solely technical explanation.

An multidisciplinary approach is required because no one profession can effectively explain—or solve—the issues raised by assaults on IoT-enabled infrastructure. Engineering and computer science detect flaws in device design, unsecured communication protocols, and weaknesses in SCADA and ICS settings that manage infrastructure operations. Political science and public policy offer insights into national security problems, regulatory gaps, and the geopolitical incentives driving state-sponsored cyberattacks. Economics addresses the financial hazards connected with cyber events, such as system unavailability, ransom payments, and the exorbitant cost of infrastructure upgrade. Ethics helps by addressing the moral responsibility of governments and private operators to safeguard the public from avoidable damage. These perspectives work together to provide a comprehensive picture of why IoT systems remain susceptible and what can be done to secure them.

Engineering and computer science provide the framework for understanding technical vulnerabilities. Many IoT devices used in critical infrastructure are designed with poor security due to cost, processing power constraints, or legacy compatibility needs. As a result, attackers frequently target weak authentication, outdated firmware, and unencrypted communication routes (Aheleroff et al., 2020). Industrial control systems pose additional hazards since many were designed decades before cybersecurity became an issue. These systems were previously isolated, but increased digitalization has connected them to corporate networks and, in some cases, the internet. This connection greatly increases the attack surface. The 2021 ransomware attack on Colonial Pipeline illustrated how a single hacked password in an IT system may shut down fuel distribution over the East Coast, demonstrating the vulnerability of infrastructure depending on digital control systems (Krebs, 2021). As a result, technical vulnerabilities are inextricably linked to vital infrastructure operations.

Political science and public policy provide a national security component to these vulnerabilities. Attacks on essential infrastructure are no longer limited to criminal organizations; nation-states are increasingly using infrastructure to project power or destabilize enemies. The assaults on Ukraine's power grid in 2015 and 2016, which were linked to Russian state-sponsored actors, demonstrated that digital threats can have physical effects, leaving hundreds of thousands without power (Greenberg, 2019). Such occurrences underscore the necessity for worldwide standards and domestic rules managing infrastructure security. However, rapid technological innovation makes it challenging for legislators to stay up. In the United States, organizations such as CISA and NIST establish rules, but enforcement varies by sector,

and many private operators lack incentives to replace outdated systems. Policy, therefore, plays an important role in defining the cybersecurity landscape.

Economics adds another level of complication. Cyberattacks on infrastructure are among the most financially destructive incidents that a business may experience. Recovery from ransomware attacks can cost millions in terms of system repair, lost productivity, and regulatory fines. The global economic impact of cybercrime is expected to approach \$10 trillion per year by 2025 (McAfee, 2020). For infrastructure operators, cybersecurity investments compete with other operational requirements, and financial constraints frequently hinder the replacement of obsolete equipment. Economic imbalance across sectors means that some infrastructure, such as rural water systems, may receive much less protection than others. An economic lens demonstrates how financial restrictions influence security decisions and why cybersecurity investment remains low despite obvious concerns.

Ethics complements the transdisciplinary framework by emphasizing public safety. Critical infrastructure failures endanger people's lives. A hack that disables hospital IoT equipment or disrupts emergency response communication systems can result in preventable fatalities. Organizations that refuse to invest in cybersecurity while knowing the risks breach their ethical commitment to safeguard the public (Spiekermann, 2019). Ethical analysis raises problems concerning accountability: Who is to blame when a cyberattack hurts the public: the attacker, the infrastructure operator, the policymakers who failed to regulate, or the device manufacturers? These questions demonstrate that cybersecurity is both a technical and a moral issue.

Across fields, numerous common motifs arise. Each profession recognizes that IoT devices have significantly increased the threat surface of critical infrastructure beyond what standard security systems can defend. All disciplines see system interconnection as both a strength and a vulnerability—efficiency rises, but so does risk. The fundamental source of conflict is cost and responsibility. Engineering may urge thorough improvements, but economics focuses on financial restrictions; officials may advocate for stronger rules, but private operators may object owing to cost or feasibility. Ethics advocates for public safety, even if it is costly or difficult. These tensions highlight why interdisciplinary collaboration is essential.

Finally, cybersecurity concerns to critical infrastructure in the age of IoT cannot be solved solely by technology. The technical flaws of IoT devices combine with political, economic, and ethical issues, shaping both risks and potential remedies. By combining knowledge from several disciplines, society can gain a greater understanding of the complexity of these risks and build more effective prevention, response, and resilience methods. As infrastructure evolves, interdisciplinary research will remain critical to protecting the systems that sustain daily living.

References

- Aheleroff, S., Xu, X., Lu, Y., Aristizabal, M., Velásquez, J. D., Joa, B., & Valencia, Y. (2020). IoT-enabled smart appliances under industry 4.0: A case study. *Advanced Engineering Informatics*, 43, 101043.
- Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Doubleday.
- Krebs, B. (2021). Colonial Pipeline ransomware attack: What we've learned. *Krebs on Security*. <https://krebsonsecurity.com>
- Lee, R. M., & Assante, M. J. (2019). Analysis of the cyber attack on the Ukrainian power grid. *SANS Industrial Control Systems Defense Reports*.
- McAfee & CSIS. (2020). *The hidden costs of cybercrime*. McAfee.
- Spiekermann, S. (2019). *Ethical IT innovation: A value-based system design approach*. Taylor & Francis.