Protecting Infrastructure Using Cybersecurity and GIS

Marie Madeleine Anita Bekono

Old Dominion University

GEOG 495: GIS For Cybersecurity

DR. Jennifer L. Whytlaw

12/12/2024

Protecting Infrastructure Using Cybersecurity and GIS

Critical infrastructures, such as energy grids, water systems, transportation networks, and communication systems, form the very foundation of modern societies. These systems are increasingly dependent upon Geographic Information Systems-or GIS-for real-time monitoring, planning, and management. GIS integrates spatial data, providing critical insights into the locations, conditions, and vulnerabilities of infrastructure. This reliance also introduces significant cybersecurity risks, including unauthorized access, data breaches, and system disruptions.

The integration of GIS and cybersecurity primarily thrusts to the frontline demanding protection measures that would function reliably and safely for this infrastructure. Cyber-attacks on important infrastructures of recent times, such as that on the Ukrainian power grid, show how such threats have enormous capability. The paper hence relates to the point where geospatial technologies and cybersecurity converge when innovation in protection measures keeps one step ahead to guard critical infrastructural systems against cyber-attack effects with the sustainability of operational efficiencies there.

Recent research underlines the role of GIS in protecting critical infrastructure. Kim et al. (2023) conducted a state-of-the-art review regarding cybersecurity and cyber forensics in smart cities, addressing the role of integrated GIS in urban infrastructure protection. Batty (2019) discusses the use of real-time GIS in smart city environments with an emphasis on transportation systems, while stressing the need for timely geospatial data when it comes to infrastructure management. Almeida (2023) discusses some of the challenges in cybersecurity within smart

cities and identifies the role of GIS in monitoring and securing the urban infrastructures. Ahmadi-Assalemi et al. (2020) investigate cyber resilience and incident response in smart cities, hence providing valuable insights into how GIS can be integrated for effective monitoring and response strategies. Blatt (2012) discusses ethical and privacy concerns in GIS applications-a very important consideration when considering the cybersecurity of geospatial data. These studies collectively bring forth the critical importance of integrating the use of GIS and cybersecurity in protecting important systems.

Mapping and spatial planning were the major applications of GIS in infrastructure management during the initial years of its adoption. Since most of the systems operated in isolation, cybersecurity was not considered a big issue. But with the expansion of digital transformation and interlinking of systems, the vulnerabilities started to appear. A cyberattack on the power grid in 2015 Ukraine, which left several thousand without electricity, shed light on the crucial shortcomings within SCADA, or supervisory control and data acquisition, as that term would go on to become better known. The object of the attack became literally the very point where different concerns have been shown.

Nowadays, the real-time monitoring system uses integrated GIS data from IoT sensors, which can present, on performance grounds, pipeline, bridge, and power grids by the operators of those respective structures. Threat detection has gone high with geofencing technologies that establish virtual boundaries in the event of unauthorized access, sending out alerts. As a result, managers of such infrastructures can understand natural calamities or other cyber threats using the tools of GIS-based visualization for effective resource allocation.

Still, over the years, hackers managed to develop advanced ways of hacking GIS vulnerabilities, hence keeping cybersecurity at the frontline of interests.

Looking ahead, emerging technologies in infrastructure management promise to take it into new dimensions. It would leverage artificial intelligence through the inclusion of predictive algorithms analyzing geospatial data to foresee risk well before it materializes. It allows for safe methods of verification and storage in the Blockchain, reducing the possibility of tampering or unauthorized access to the GIS data. Quantum computing has also spurred the development of quantum-resistant algorithms, even as it was earlier seen as a possible threat to existing methods of encryption. As smart cities and interconnected systems evolve further, so will the role of GIS in infrastructure management, making innovation in cybersecurity practices imperative.

This integration of GIS and cybersecurity brings up various ethical and professional issues. Ethically, while it is as much about keeping the public safe in times of emergencies, it also causes concerns with regards to the privacy of individuals. For example, data gathered for infrastructure management could also be used for mass surveillance, violating individual rights. This balance of security with respect for privacy needs to be maintained through strict adherence to data protection laws and transparency in collection and use of geospatial data by governments and organizations.

Organizations that professionally manage critical infrastructure are supposed to adopt established cybersecurity frameworks to mitigate risks. Frameworks such as the NIST Cybersecurity Framework and ISO 27001 provide guidelines related to securing GIS systems and protection of sensitive data. Equally important is workforce training; with rapid evolution in technologies, professionals must keep up with emerging threats and best practices. The protection, therefore, necessitates a necessary collaboration of GIS and cybersecurity professionals to ensure that it extends holistically.

In my opinion, the implications of integrating GIS with cybersecurity are immense from an ethical and professional point of view. While technology advances create new opportunities, the technological innovations must be responsibly put into practice. Ethical use of data should, therefore, be a core activity of governments, private organizations, and research institutions; more so, investing in secure and innovative solutions to answer new challenges of infrastructure management.

The protection of critical infrastructure is one of the most complex and sensitive missions in the modern digital world. Coupled with cybersecurity, GIS provides an effective suite of tools for monitoring, managing, and protecting such systems. The analysis of geospatial data for the detection of weak spots is what GIS and cybersecurity together can do to make infrastructure resilient. Yet, challenges remain in the form of cyberattacks and ethical concerns, which need to be taken into consideration through proactive measures and continuous innovation. As smart cities and the all-inclusive system continue to be on the rise, collaboration in operation between GIS and cybersecurity professional expertise will be crucial in ascertaining safety and surety in critical infrastructure.

References

Blatt, A. J. (2012). Ethics and privacy issues in the use of GIS. *Journal of Map & Geography Libraries*, *8*(1), 80–84. https://doi.org/10.1080/15420353.2011.627109

Bridgelall, R. (2022). Perspectives on securing the transportation system. *Vehicles*, *4*(4), 1332–1343. https://doi.org/10.3390/vehicles4040070

Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive literature review and survey. *Sensors*, *23*(7), 3681. https://doi.org/10.3390/s23073681

Li, W., Batty, M., & Goodchild, M. F. (2019). Real-time GIS for smart cities. *International Journal of Geographical Information Science*, *34*(2), 311–324. https://doi.org/10.1080/13658816.2019.1673397