GIS Odyssey Journal

2026 • Volume 6 • Number 1

https://doi.org/10.57599/gisoj.2026.6.1.45

Gokhan Balik[1]

INTEGRATING GIS AND CYBERSECURITY: SPATIAL INTELLIGENCE FOR CRITICAL INFRASTRUCTURE RISK AND RESILIENCE

Abstract: As digital networks become increasingly intertwined with physical infrastructure, cybersecurity must account for location, interdependence, and operational context. Geographic Information Systems (GIS) provide a valuable framework by integrating spatial, attribute, and temporal data within a single analytical environment. This article presents a structured literature review of GIS-enabled cybersecurity research, focusing on critical infrastructure, smart cities, and resilience planning. The review synthesizes peer-reviewed studies, technical standards, and selected institutional materials to examine how GIS supports threat visualization, vulnerability assessment, dependency mapping, situational awareness, governance, and risk communication. The review suggests that GIS is most valuable where cyber risk has clear spatial, infrastructural, and operational dimensions, particularly in critical infrastructure protection and urban cyber-physical systems. However, the evidence base remains uneven. Visualization and situational awareness applications are relatively mature, while ontology-based modeling, blockchain-based trust, and some AI-driven functions remain emerging and require further operational validation. The article also argues that GIS platforms should be treated as strategic digital assets requiring dedicated cybersecurity protection and concludes with implications for secure GIS governance and future research on geospatially informed resilience frameworks.

Keywords: GIS, cybersecurity, critical infrastructure, spatial intelligence, risk, resilience

Received: 14 April 2026; accepted: 1 May 2026; revised: 5 May 2026

[1] Webster University, George Herbert Walker School of Business & Technology, Department of Computer and Information Sciences, St. Louis, MO, United States, ORCID ID: https://orcid.org/0000-0003-0155-6118, email: gokhanbalik@webster.edu; gokhanbalik8@gmail.com

Introduction and state of the problem

Cybersecurity is no longer limited to isolated information systems. Modern cyber incidents affect geographically distributed assets, operational networks, and critical services that depend on power, communications, transportation, cloud platforms, and industrial control systems. For this reason, the distinction between digital and physical security has become blurred, particularly in critical infrastructure where disruption in one location can trigger wider operational and societal consequences. Current literature therefore argues that cyber defense should be treated not only as a technical function but also as a spatial and organizational problem (Arvidsson et al., 2021; Esri, 2015; Veerasamy et al., 2022).

Geographic Information Systems (GIS) provide a useful foundation for addressing this problem because they combine location, attributes, and time in a single analytical environment. Prior research shows that geospatial data can support cyber threat tracking, pattern detection, visualization, situational awareness, cyber intelligence, and decision making. Research has also shown that GIS can help identify cybercrime hotspots, analyze malicious URL clusters, support access control using geographic context, and improve response to incidents affecting distributed infrastructure (Amin et al., 2021; Vasdev, 2020; Veerasamy et al., 2022). In this sense, GIS extends cybersecurity analysis beyond logs and alerts by adding the questions of where events occur, how they evolve, and how assets and systems are interconnected.

A second line of research emphasizes the relationship between cyberspace and physical infrastructure. The geospatial perspective argues that cyberspace is not purely virtual because every data flow ultimately depends on devices, network links, facilities, and users located in space and time. The concept of the Cyber Supply Line illustrates this point by showing that data movement depends on chains of devices and connections whose failure can affect mission performance. This argument is reinforced by work on critical infrastructure interdependencies and risk governance, which shows that geospatial analysis is important for understanding cascading effects across interconnected systems (Arvidsson et al., 2021; Esri, 2015; Lewis, 2020). Recent work in cyberspace geography further argues that cyberspace has distinct geographical properties, including the uneven spatial distribution of infrastructure, regional variation in information resources, and geographically patterned online behavior. This work also suggests that spatial correlation, spatial heterogeneity, and geographical similarity remain analytically useful in cyberspace, supporting the use of GIS methods for visualization, geographic knowledge graphs, and behavior analysis (Jiang et al., 2023).

A broader critical infrastructure perspective reinforces this argument by showing that infrastructure protection has evolved from a narrow focus on disaster recovery and terrorism response into a more comprehensive concern with risk, resilience, interdependence, and cybersecurity across a networked national system. Lewis (2020) argues that modern society depends on complex infrastructures whose fragility is often rooted in the way systems are connected rather than only in the weakness of individual components. In his account, modernity means connectivity and connectivity means

complexity, and that complexity is itself a major source of systemic risk because collapse can be embedded in the architecture of infrastructure itself. This perspective supports the use of GIS in cybersecurity because spatial analysis becomes more valuable as infrastructures grow more interconnected, geographically distributed, and vulnerable to cascading consequences that extend beyond a single facility or sector.

The state of the problem is especially visible in smart cities and other sensor-rich environments. Smart infrastructures rely on large numbers of connected devices, platforms, and automated services that generate both cyber exposure and spatially distributed vulnerability. Research highlights risks such as ransomware, denial of service attacks, manipulation of sensing data, insecure Internet of things (IoT) services, and attack propagation across interconnected urban systems (Andrade et al., 2020; Joshi et al., 2026; Kalinin et al., 2021). At the same time, studies on anomaly detection, Global Positioning System (GPS) spoofing, and blockchain-based trust models show that location-aware systems require stronger methods for verifying integrity, detecting abnormal behavior, and protecting real-time geospatial data streams (Islam et al., 2025; Shabbir et al., 2023; Shafique et al., 2021; Tian et al., 2023). GIS data also plays an increasing role in wireless security, secure software development, and digital forensics, where location precision and metadata influence both technical interpretation and legal reasoning (Dragos & Schmeelk, 2021). These developments make GIS increasingly relevant not only for mapping threats but also for supporting resilience in complex cyber-physical environments.

Despite growing interest, the literature remains fragmented. Some studies focus on cyber threat visualization, others on GIS system security, smart city risk, ontology-based governance, GPS spoofing, or critical infrastructure dependency analysis. As a result, GIS is variously treated as a mapping interface, an analytical environment, or a software platform requiring its own secure development and operational controls (Besiekierska & Czaplicki, 2022; Kiedrowicz et al., 2025; Sobeslav et al., 2026; Stanik & Kiedrowicz, 2022a). Seven studies also show that the field increasingly addresses legal duties, incident management procedures, practical methods for detecting cyber threats, the integration of cybersecurity standards, contingency planning, cyber resilience building, and certification artifacts in GIS environments, but these discussions are still unevenly integrated with broader GIScience and infrastructure resilience research (Besiekierska & Czaplicki, 2022; Górny, 2025; Kiedrowicz, 2025; Miłek, 2025; Stanik & Kiedrowicz, 2025; Kiedrowicz & Stanik, 2024; Stanik & Kiedrowicz, 2022b).

This article addresses that gap by examining the integration of GIS with cybersecurity through the lens of spatial intelligence for critical infrastructure risk and resilience. It provides a structured synthesis of GIS-enabled cybersecurity research across five interconnected functions: spatial framing of cyber risk, threat visualization and situational awareness, dependency analysis for critical infrastructure, smart city and artificial intelligence (AI) enabled monitoring, and governance constraints affecting secure GIS implementation. By integrating GIS, cybersecurity, critical infrastructure, and resilience in a single review, the article positions GIS not as a supplementary mapping

tool, but as an analytical and decision support environment whose value depends on operational context, evidence strength, and governance maturity.

Material and methods

This study was designed as a structured literature review of the integration of GIS with cybersecurity. This approach is essential because the topic is highly interdisciplinary – spanning GIScience, cybersecurity, critical infrastructure, risk governance, and smart city research—with critical knowledge and insights scattered across journals, conference proceedings, technical reports, standards, and selected institutional case studies rather than a single, consolidated research stream.

The literature search drew on major scholarly databases and publisher platforms included in the search, including Scopus, Web of Science, Google Scholar, IEEE Xplore, SpringerLink, and ScienceDirect, together with targeted searches of authoritative institutional repositories for standards and technical guidance. Search results were first screened by title and abstract for relevance to GIS and cybersecurity integration. Duplicates and clearly irrelevant records were removed, after which the remaining sources were reviewed in full text against the inclusion and exclusion criteria. Where multiple sources covered similar points, preference was given to the most directly relevant, methodologically clear, and up to date studies. The search strings combined the exact core terms “GIS cybersecurity” and “cybersecurity spatial”. The review focused primarily on literature published from 2020 to 2026, but earlier foundational sources were retained when they provided concepts still central to the field, especially the geospatial layer model of cyberspace, conceptual work on the geographical properties of cyberspace, and early spatial analyses of cyber incidents (Esri, 2015; Hui et al., 2015; Jiang et al., 2023). The literature search was current as of 12 April 2026. After applying the inclusion and exclusion criteria described above, 34 sources were retained for the final thematic synthesis.

Sources were included if they met one or more of the following criteria: they addressed GIS, geospatial data, spatial analytics, or location intelligence in cybersecurity contexts; examined cyber risks affecting geographically distributed systems such as critical infrastructure, smart cities, industrial control environments, or location-dependent platforms; proposed spatial methods for threat detection, anomaly analysis, risk assessment, or resilience planning; or provided authoritative technical guidance directly relevant to secure GIS platforms, software assurance, certification, infrastructure dependency analysis, or public cyber threat visualization. Preference was given to peer-reviewed and indexed sources. Practitioner and institutional materials were retained only where they offered distinctive conceptual framing or applied case evidence not adequately captured in the scholarly literature, including live threat maps and large scale breach visualizations used to communicate cyber risk to expert and non-expert audiences. Foundational monographs were retained where they provided systems-level insights into critical infrastructure risk, resilience, interdependence, and governance (Clarke et al., 2025; Esri, 2015; Information is Beautiful, 2024; Lewis, 2020).

Sources were excluded if they addressed cybersecurity without a spatial component, treated GIS only as a generic software category without cybersecurity relevance, duplicated stronger sources, or showed limited relevance to critical infrastructure, smart city systems, or geographically distributed cyber risk. Materials using the acronym GIS for non-geospatial concepts were reviewed but excluded where conceptual ambiguity outweighed analytical value.

Following screening, the selected sources were organized into five analytical themes: spatial foundations of cybersecurity; threat visualization and geospatial situational awareness; critical infrastructure and dependency analysis; smart cities and emerging technologies; and governance, software assurance, and operational limitations, including standards integration and contingency planning. This thematic structure reflects dominant research patterns across the reviewed literature and allows the discussion to move from conceptual framing to applied use cases and implementation constraints (Arvidsson et al., 2021; Joshi et al., 2026; Stanik & Kiedrowicz, 2022a) (Table 1).

The selected materials were examined through qualitative thematic synthesis. For each source, the following elements were recorded: publication type, year, application domain, geospatial component, cybersecurity function, and major contribution. Sources were then compared to identify recurring ideas, differences in evidence strength, and unresolved challenges. Particular attention was paid to how each source positioned GIS within the cybersecurity workflow: as visualization support, as a tool for risk and dependency analysis, or as part of a broader governance and resilience framework involving standards integration, incident management, contingency planning, and certification artifacts (Amin et al., 2021; Clarke et al., 2025; Esri, 2015; Górny, 2025; Kiedrowicz, 2025; Kiedrowicz et al., 2025; Kiedrowicz & Stanik, 2024; Stanik & Kiedrowicz, 2025; Stanik & Kiedrowicz, 2022b; Veerasamy et al., 2022).

This review has several limitations. It is a structured review rather than a full systematic review or meta analysis. The field remains relatively new and interdisciplinary, meaning that peer-reviewed evidence coexists with standards, institutional case studies, and applied technical reports. In addition, some emerging topics, such as ontology-driven smart city governance and transportation cybersecurity clustering, are recent enough that the evidence base is still developing (Joshi et al., 2026; Sobeslav et al., 2026). These limitations do not prevent meaningful synthesis, but they do require cautious interpretation of maturity, generalizability, and operational readiness.

Results and discussion

Spatial foundations of cybersecurity. The reviewed literature consistently shows that the integration of GIS with cybersecurity begins with a shift in perspective: cyber threats must be understood not only as logical or software events but also as phenomena tied to physical devices, communications infrastructure, and operational locations. Several sources argue that cyberspace depends on a geographic layer because

Table 1. Analytical themes and main literature contributions

Analytical theme	Key studies	GIS function	Cybersecurity function	Main limitation
Spatial foundations of cybersecurity	Arvidsson et al. (2021); Besiekierska & Czaplicki (2022); Esri (2015); Jiang et al. (2023); Lewis (2020); Miłek (2025); Veerasamy et al. (2022)	Spatial framing of assets, networks, dependencies, legal information infrastructure, cyber awareness, conceptual properties of cyberspace, networked infrastructure systems, and structural complexity	Shared situational awareness, mission impact interpretation, legal and administrative duties, conceptual grounding for geographic thinking in cyberspace, and resilience framing of interdependent infrastructure	Heavy reliance on conceptual and cross field synthesis, plus national context specificity
Threat visualization and geospatial situational awareness	Aldabbagh & Ilyas (2021); Amin et al. (2021); Check Point Software Technologies (2026a, 2026b); Howley (2015); Hui et al. (2015); Information is Beautiful (2024); Vasdev (2020)	Mapping, clustering, spatial statistics, public cyber threat maps, and longitudinal breach visualization	Threat detection support, prioritization, situational awareness, and risk communication	Geolocation uncertainty, vendor framing, and limited attribution value
Critical infrastruc-ture and dependency analysis	Arvidsson et al. (2021); Clarke et al. (2025); Lewis (2020); Malatji et al. (2022); Stanik & Kiedrowicz (2025)	Dependency mapping, consequence analysis, network fragility assessment, and topology aware bottleneck identification	Resilience planning, capability framing, standards integration, and cascading consequence interpretation	Mixed evidence base with limited GIS specific empirical validation
Smart cities and emerging technologies	Andrade et al. (2020); Islam et al. (2025); Joshi et al. (2026); Kalinin et al. (2021); Tian et al. (2023)	Monitoring distributed urban systems	Anomaly detection, integrity, and adaptive risk response	Many results remain sector specific or emerging
Governance, software assurance, and operational limitations	Dragos & Schmeelk (2021); Górny (2025); Lewis (2020); National Institute of Standards and Technology (2022); Kiedrowicz (2025); Kiedrowicz et al. (2025); Kiedrowicz & Stanik (2024); Sobeslav et al. (2026); Stanik & Kiedrowicz (2025); Stanik & Kiedrowicz (2022a); Stanik & Kiedrowicz (2022b)	Platform governance and data stewardship, digital forensics support, coordinate integrity, incident response, standards integration, contingency planning, certification documentation, and inter-organizational coordination	Software assurance, incident management, risk management, legal and investigative defensibility, recovery planning, audit readiness, and public private governance	Organiza-tional maturity, interopera-bility, standards alignment, precision handling challenges, and uneven institutional capacity

Source: Author's own elaboration based on cited literature

data exchange ultimately relies on devices and electromagnetic transmission paths that exist in space and time. This view challenges the assumption that cyber defense can be addressed only through traditional information technology controls and supports the use of GIS as an integrating environment for cyber-physical risk analysis (Arvidsson et al., 2021; Esri, 2015).

Within this perspective, geospatial data contributes three forms of value to cybersecurity: location, attributes, and time. These components allow cyber events to be analyzed not only according to type and severity but also according to where they occur, what assets they affect, and how they evolve over time. Prior work has shown that geospatial analytics can reveal relationships and trends that remain difficult to detect in tabular or purely textual data. This finding is important because it shows that GIS is not limited to cartographic display. Instead, it can function as an analytical environment that supports interpretation, prioritization, and decision making (Veerasamy et al., 2022; Vasdev, 2020).

Recent research expands this framing by emphasizing that spatial information services are also embedded in legal and administrative systems. Besiekierska and Czaplicki (2022) show that public spatial information infrastructures carry explicit cybersecurity obligations and that weaknesses in information security management, backup policy, and training can directly undermine the reliability and continuity of spatial data services. This perspective strengthens the argument that spatial information is not merely a technical layer but part of a regulated public information environment in which cyber failure has service, governance, and public trust consequences. Miłek (2025) extends this perspective by arguing that geospatial data should also be treated as an active source of cyber awareness rather than only a protected asset. Her analysis suggests that GIS supports threat tracking, geospatial data fusion, visual analytics, cyber intelligence, threat prioritization, and collaboration across security actors, which reinforces the claim that spatial context can materially improve cyber situational awareness when combined with other analytic tools.

A complementary conceptual strand comes from cyberspace geography. Jiang et al. (2023) argue that cyberspace retains distinct geographical properties because its physical infrastructure, information resources, and behavioral patterns remain unevenly distributed across regions and closely linked to real geographic and socioeconomic environments. They further propose that the three laws of geography remain analytically useful in cyberspace: spatial correlation still matters, spatial heterogeneity remains visible in network resources and digital divides, and geographically similar environments tend to generate more similar patterns of cyberspace behavior. This perspective gives stronger theoretical grounding to the claim that GIS is relevant to cybersecurity not only because data can be mapped, but because cyberspace itself exhibits analyzable spatial properties.

At the same time, the strongest claims in this area remain conceptual rather than empirically standardized. The geospatial layer model and the Cyber Supply Line concept provide useful framing devices, but much of the supporting discussion still depends on foundational white paper logic and cross-field synthesis rather than repeated

comparative testing across sectors (Arvidsson et al., 2021; Esri, 2015). For this reason, the current evidence supports the value of GIS as a spatial framing tool, while more empirical work is still needed to determine which spatial representations produce the greatest operational benefit in practice.

Threat visualization and geospatial situational awareness. The reviewed studies show strong agreement that one of the most mature applications of GIS in cybersecurity is the visualization of threats and vulnerabilities. Threat mapping allows analysts to locate attack origins, affected assets, and clusters of suspicious activity in ways that are more intuitive than conventional tables or logs. The literature suggests that visual representation can improve anomaly recognition, support faster interpretation of large datasets, and strengthen organizational awareness of emerging cyber patterns (Vasdev, 2020; Veerasamy et al., 2022).

Applied studies in this area vary in data realism and methodological strength. Hui et al. (2015) used university intrusion logs geocoded through Geographical Internet Protocol (GeoIP) tools and analyzed them with spatial statistics, providing one of the more concrete examples of GIS-based cyber event analysis in an operational context. By contrast, Aldabbagh and Ilyas (2021) demonstrated smart city intrusion mapping through GeoCluster and spatial statistics but relied on more limited validation. Together, these studies suggest that spatial cyber monitoring is feasible and methodologically adaptable, but the strongest support currently comes from event mapping and exploratory clustering rather than from standardized predictive workflows (Aldabbagh & Ilyas, 2021; Hui et al., 2015).

The literature on malicious URL clustering also supports the value of spatial analysis. Amin et al. (2021) show that cyber threats can display meaningful geographic patterns, which in turn can inform relative risk assessment and resource prioritization. Although geographic origin does not provide definitive attribution, spatial distribution still offers useful intelligence for identifying hotspots and unusual concentrations of activity. This indicates that GIS methods developed in fields such as epidemiology and regional analysis can be adapted effectively to cybersecurity (Amin et al., 2021).

Public-facing cyber maps and breach visualizations provide an additional bridge between GIS and cybersecurity because they translate complex attack data into spatial forms that support awareness, communication, and exploratory interpretation. Yahoo Tech framed this genre as a way to watch worldwide cyberattacks live and highlighted an important caution that such maps are usually vendor hosted and should not be mistaken for precise attribution or neutral measurement of global attack reality (Howley, 2015). Check Point's current threat intelligence materials extend this model by pairing a live threat map with AI enriched intelligence derived from hundreds of millions of sensors worldwide and billions of daily security decisions, showing how map based interfaces are now embedded within larger threat intelligence ecosystems rather than functioning only as standalone visuals (Check Point Software Technologies, 2026a, 2026b). Information is Beautiful offers a complementary non-live model through its long running visualization of the world's biggest data breaches and hacks, which emphasizes event magnitude, sector, and data sensitivity over time rather than real-time attack flow

(Information is Beautiful, 2024). Taken together, these examples reinforce the conclusion that one of the most mature links between GIS and cybersecurity lies in visualization for situational awareness and risk communication, while also underscoring the need for careful interpretation of what such public maps do and do not actually show.

However, the review also indicates that the value of threat visualization depends heavily on data quality and interpretation. Geographic representations can be misleading if users assume precision where data are uncertain, especially in the case of Internet Protocol (IP) geolocation, proxy routing, or spoofed location signals. Thus, current evidence suggests that GIS-based situational awareness is most defensible as a decision support capability rather than a substitute for attribution or deep forensic investigation (Shafique et al., 2021; Stanik & Kiedrowicz, 2022a).

Critical infrastructure and dependency analysis. Among the reviewed themes, one of the strongest practical justifications for GIS in cybersecurity appears in critical infrastructure protection. Infrastructure systems such as energy, water, communications, transportation, and healthcare are geographically distributed, operationally interdependent, and increasingly dependent on digital control systems. Because of these characteristics, cyber incidents cannot be evaluated only at the level of isolated devices or networks. They must also be understood in terms of spatial exposure, upstream and downstream dependency, and potential cascading consequences across connected systems (Arvidsson et al., 2021; Esri, 2015).

Research on critical infrastructure and risk governance highlights the importance of geospatial analysis for understanding interdependencies between sectors and for supporting multi-actor coordination in risk management. GIS-based approaches have been used to model hazard exposure, visualize infrastructure dependencies, and support communication between decision makers and technical operators. In the cybersecurity context, this becomes especially important when a digital weakness in one component can have indirect effects on geographically separate but operationally dependent systems (Arvidsson et al., 2021).

Lewis (2020) provides a strong systems-level justification for this position by arguing that many infrastructure failures are rooted not only in weak components but also in the topology of the system itself. Drawing on complexity theory, normal accident theory, and network science, he shows that hidden coupling, excessive connectivity, hub concentration, and self organizing criticality can increase fragility and make cascading failure more likely across critical sectors. He further argues that vulnerability is often built into infrastructure through the arrangement of links, hubs, and interdependencies rather than any single failed asset. This is especially relevant to GIS-enabled cybersecurity because geospatial methods can help reveal where dependencies are concentrated, which assets function as bottlenecks or blocking nodes, and how disruption in one location can propagate through a wider operational network. In this sense, GIS is valuable not only for mapping assets, but for identifying where the structure of a networked infrastructure system may amplify cyber and physical consequences (Lewis, 2020).

The most visible applied example in the reviewed materials is MITRE's Project Homeland, which uses spatial knowledge graphs to combine geographic entities such as substations, hospitals, treatment facilities, and communication nodes with non-spatial entities such as software platforms, operational dependencies, and vulnerabilities. The key result is not merely a richer map but a more complete understanding of hidden dependencies and composite risk. This case shows how a vulnerability in one software component can become a system-wide resilience issue when it affects infrastructure on which other critical services depend (Clarke et al., 2025).

To reduce dependence on one institutional example, the review also considered broader capability frameworks for critical infrastructure resilience. Malatji et al. (2022) argue that operators need integrated cybersecurity capability domains spanning governance, controls, IoT, cloud, and industrial systems. Their work is not GIS-centered, but it strengthens the conclusion that GIS should be linked to a broader resilience architecture rather than treated as a standalone visualization layer. Stanik and Kiedrowicz (2025) complement this position by showing that critical infrastructure security management in GIS benefits from explicit integration of national cybersecurity standards, risk assessment, and incident management procedures. The review suggests that the strongest current evidence supports GIS in critical infrastructure when it is used alongside sector standards, capability frameworks, and dependency analysis, not in isolation (Clarke et al., 2025; Malatji et al., 2022; Stanik & Kiedrowicz, 2025).

Smart cities and emerging technologies. The reviewed literature shows that smart cities represent a major application domain for GIS-enabled cybersecurity because they combine cyber-physical infrastructure, sensor networks, automated controls, and location-dependent services. Studies in this area describe environments in which IoT devices, transport systems, wireless networks, emergency systems, and utility controls are deeply interconnected. The main result across these studies is that cyber risk in smart cities is inherently spatial because attacks on one node can propagate across connected urban systems and because many of the affected services are tied to specific places, routes, facilities, and populations (Andrade et al., 2020; Islam et al., 2025; Kalinin et al., 2021).

The evidence base in this area is broader than in earlier GIS cybersecurity work but also more heterogeneous. Kalinin et al. (2021) provide a focused smart city risk assessment model using neural networks, while Tian et al. (2023) address spatial temporal anomaly detection in multivariate systems. Islam et al. (2025) emphasize blockchain-enabled trust, integrity, and AI-driven threat detection. Joshi et al. (2026) add a bibliometric perspective, showing that post 2020 smart city cybersecurity research has expanded rapidly around AI, blockchain, IoT security, governance, and resilience. Together, these studies suggest that the combination of GIS, AI, and time-sensitive monitoring can support more adaptive cyber defense. Yet they also show that the field still lacks consistent evaluation standards across sectors (Islam et al., 2025; Joshi et al., 2026; Kalinin et al., 2021; Tian et al., 2023).

One particularly important issue is the integrity of location itself. GPS spoofing studies show that location-aware systems can be manipulated in ways that undermine

autonomous vehicles, unmanned platforms, and other geospatially dependent services. Deep learning and machine learning methods have shown strong results in detecting such attacks, but these results are often obtained in controlled scenarios or specific technical environments. The current evidence therefore indicates strong technical promise, while broader operational validation remains necessary before general claims about readiness can be made (Shabbir et al., 2023; Shafique et al., 2021).

Overall, smart city cybersecurity appears to be one of the most active and interdisciplinary areas in the literature. It provides strong support for the argument that cyber risk in urban systems is tied to place, infrastructure, and service geography. At the same time, many of the most innovative solutions remain emerging rather than mature, especially where blockchain, ontology systems, and AI-enabled governance are concerned (Islam et al., 2025; Sobeslav et al., 2026).

Governance, software assurance, and operational limitations. A final theme in the review concerns governance, software assurance, and the limitations of GIS cybersecurity integration. One important contribution of the literature is the suggestion that established cybersecurity frameworks can be enriched through spatial context. The NIST Secure Software Development Framework is particularly useful in this respect because it organizes security activities into preparation, protection, production, and vulnerability response. The reviewed materials indicate that GIS can strengthen these practices by helping organizations map deployment footprints, identify geographic risk concentrations, locate affected assets, and prioritize remediation according to operational exposure (Esri, 2015; National Institute of Standards and Technology, 2022).

The literature also makes clear that GIS platforms themselves are cybersecurity assets that require protection. Stanik and Kiedrowicz (2022a) argue that attacks on GIS can lead to leakage of sensitive spatial data, corruption of decision support outputs, service interruption, and loss of availability. Kiedrowicz et al. (2025) extend this line of thinking by showing how DevSecOps can improve the continuity and resilience of GIS systems through earlier security integration in the software lifecycle. Their evidence suggests that secure GIS requires not only network protection but also process maturity, automation, and organizational adaptation. Dragos and Schmeelk (2021) reinforce this point from a digital forensics perspective by showing that location data quality and numeric precision can affect mobile investigations, wireless security analysis, and secure software development, meaning that secure GIS also depends on trustworthy coordinate handling, metadata preservation, and defensible interpretation in legal and investigative settings.

Two recent studies sharpen this governance dimension further. Besiekierska and Czaplicki (2022) show that legal obligations concerning cybersecurity of spatial information are often not fully implemented in public sector practice, with recurring weaknesses in information security management systems, auditing, backups, and staff preparedness. Kiedrowicz (2025) then moves from governance obligations to operational response, arguing that incident management in GIS requires integrated procedures for monitoring, detection, response, recovery, and reporting, and that

effective practice should be aligned with standards such as ISO 27001, ISO 19115, OGC guidance, NIS2, and GDPR. Stanik and Kiedrowicz (2025) deepen this standards perspective by explicitly examining the integration of national cybersecurity standards into GIS in the context of critical infrastructure security management, emphasizing risk assessment, incident management, and the need for close cooperation between cybersecurity professionals and GIS users. Kiedrowicz and Stanik (2024) add that contingency planning is a key life cycle artifact in GIS cybersecurity management and should be integrated throughout the system development and operations life cycle, including business impact analysis, preventive safeguards, recovery strategies, testing, training, and plan maintenance.

Lewis (2020) sharpens this governance dimension further by identifying several persistent implementation problems: public-private coordination gaps, information sharing barriers, unclear jurisdictional responsibilities, and chronic funding limitations. He argues that critical infrastructure protection often appears coherent at the policy level while remaining uneven in practice because authority, expertise, funding, and incentives are distributed unevenly across federal, state, local, tribal, and private sector actors. This is directly relevant to secure GIS implementation because geospatially enabled cybersecurity depends on coordinated access to infrastructure data, common operating pictures across sectors, and investment decisions that account for both local conditions and cross sector interdependence. These governance constraints help explain why GIS can be analytically powerful in cyber resilience work while still remaining difficult to operationalize consistently across organizations (Lewis, 2020).

A further certification oriented contribution comes from Stanik and Kiedrowicz (2022b), who argue that the Statement of Applicability is a central and mandatory artifact in ISO 27001 based GIS certification because it links risk assessment to implemented controls, documents justified control selection and exclusions, records implementation status, and supports monitoring and auditability. This suggests that secure GIS governance also depends on the quality of security documentation: standards alignment is not only a matter of policy intent, but also of how well safeguards, responsibilities, evidence, and monitoring methods are formalized and maintained across information processes.

Governance models for smart cities add another layer to this discussion. Sobeslav et al. (2026) show that ontology driven expert systems can improve consistency and formal rigor in modeling assets, threats, vulnerabilities, and countermeasures for smart city services and open data environments. This complements the dependency logic seen in MITRE's knowledge graph work, but it also highlights a different limitation: semantic governance systems can be analytically powerful while still requiring substantial maintenance, interoperability work, and institutional maturity.

Operational threat identification methods are also becoming more explicit in recent GIS literature. Górny (2025) compares approaches such as system log analysis, vulnerability scanning, penetration testing, intrusion detection/prevention system (IDS/IPS), AI and ML anomaly analysis, GIS data integrity monitoring, network traffic analysis, and security audits. His comparative discussion reinforces a central conclusion

of this review: no single detection method is sufficient for GIS environments. Instead, the strongest practical approach appears to be a layered combination of monitoring, anomaly detection, integrity checks, and procedural auditing. This confirms that secure GIS depends on both technical controls and organized incident management rather than any single tool category.

Several recurring limitations were identified across the reviewed materials. These include privacy concerns in tracking location based behavior, uncertainty in geolocation data, the difficulty of integrating physical and digital layers, and the need for specialized expertise that combines GIS and cybersecurity knowledge. These are not minor obstacles. They shape whether GIS-based cyber analysis can be adopted responsibly and used effectively in operational settings. The review suggests that the strongest current evidence supports GIS where organizations can combine spatial analytics with governance capability, software assurance, incident handling, certification documentation, and sector-specific resilience planning rather than relying on mapping alone (Górny, 2025; Malatji et al., 2022; Stanik & Kiedrowicz, 2022a; Stanik & Kiedrowicz, 2022b; Veerasamy et al., 2022).

Conclusions

This structured review shows that the integration of GIS with cybersecurity is conceptually justified and practically relevant, especially in environments where cyber risks affect geographically distributed assets, services, and infrastructures. The reviewed literature indicates that GIS contributes to cybersecurity by providing spatial context for threat visualization, vulnerability assessment, dependency analysis, and resilience oriented decision making. In this sense, GIS should be understood not only as a mapping interface but as an analytical environment that connects digital threats with physical systems, operational consequences, and place-based priorities (Arvidsson et al., 2021; Esri, 2015; Veerasamy et al., 2022). Lewis (2020) reinforces this conclusion by arguing that resilient infrastructure cannot be secured only through isolated asset hardening, because fragility often arises from the structure, interdependence, and operating logic of the system itself. From this perspective, GIS is especially useful where cyber risk must be interpreted in relation to connected infrastructure systems, cascading effects, topology aware vulnerabilities, and geographically distributed response priorities.

The review suggests that the strongest current evidence for this integration appears in critical infrastructure protection and smart city security. In critical infrastructure settings, GIS helps reveal dependencies among interconnected systems and supports understanding of how cyber incidents can trigger cascading effects across power, water, transportation, communications, and health services. In smart city environments, GIS supports the analysis of sensor-rich and location-dependent systems where cyber risk is tied to real-time operations, mobility, and urban services. The evidence is strongest when GIS is used together with broader capability frameworks, sector standards, and

resilience models rather than as a standalone tool (Arvidsson et al., 2021; Clarke et al., 2025; Kalinin et al., 2021; Malatji et al., 2022).

The review also indicates that GIS gains additional significance when combined with emerging technologies such as AI, machine learning, ontology systems, and knowledge graph methods. These combinations strengthen the capacity to detect anomalies, model hidden dependencies, and support faster interpretation of complex cyber-physical events. At the same time, many of these developments should still be treated as emerging capabilities rather than universally mature solutions because evidence remains sector-specific and evaluation standards are uneven (Islam et al., 2025; Sobeslav et al., 2026; Tian et al., 2023).

An equally important conclusion is that GIS platforms themselves must be treated as strategic digital assets that require cybersecurity protection. The reviewed literature points to recurring concerns related to data confidentiality, integrity, availability, geolocation uncertainty, plugin and API exposure, and the manipulation of geospatial outputs. Thus, the relationship between GIS and cybersecurity is bidirectional: GIS can improve cyber defense, but GIS environments must also be secured if they are to function as trustworthy decision support systems (Dragos & Schmeelk, 2021; Kiedrowicz et al., 2025; Stanik & Kiedrowicz, 2022a).

Recent studies also reinforce the importance of legal compliance, incident management, standards integration, cyber awareness, multi-layer threat detection, and contingency planning in operational GIS environments. Public cyber maps and breach visualizations from organizations such as Check Point and Information is Beautiful further suggest that one of the most operationally mature intersections between GIS and cybersecurity lies in threat communication and situational awareness, although these tools should be interpreted as awareness and exploratory analytics resources rather than definitive attribution systems (Check Point Software Technologies, 2026a, 2026b; Howley, 2015; Information is Beautiful, 2024). Public sector weaknesses in implementing cybersecurity obligations, combined with the need for integrated incident response procedures, national and international standards alignment, life-cycle-based contingency planning, and well-maintained certification artifacts such as the Statement of Applicability, suggest that resilient GIS depends as much on organizational capability and governance maturity as on analytics and visualization alone (Besiekierska & Czaplicki, 2022; Górny, 2025; Kiedrowicz, 2025; Kiedrowicz & Stanik, 2024; Miłek, 2025; Stanik & Kiedrowicz, 2025; Stanik & Kiedrowicz, 2022b).

Future research should focus on three priorities. First, review studies in this field should report search logic and screening procedures more reproducibly so that interdisciplinary synthesis becomes easier to compare. Second, more empirical work is needed to validate GIS cybersecurity applications across sectors, especially beyond single case demonstrations and controlled technical scenarios. Third, research should further develop GIS aware resilience and maturity frameworks that integrate dependency analysis, secure software practices, AI-enabled monitoring, incident management standards, certification artifacts, and governance requirements in a form that organizations can operationalize.

Overall, the reviewed evidence does not support the claim that every cybersecurity problem is spatial. However, it clearly shows that many high consequence cyber risks have strong geographic, infrastructural, and operational dimensions that are difficult to understand without spatial analysis. For this reason, GIS should be viewed as a valuable component of contemporary cyber risk and resilience practice, and as an increasingly important area for further interdisciplinary research.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declaration of Competing Interests

The author declares that there are no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No new data were created or analyzed in this study. This article is based on published literature and technical materials cited in the reference list.

Use of Generative AI and AI-Assisted Technologies

Generative AI (ChatGPT 5.4) assisted in language refinement during the preparation of this manuscript.

Acknowledgements (optional)

The author thanks Dr. William Mike Smith (Webster University) for his insightful comments and constructive feedback on earlier versions of this manuscript.

References

Aldabbagh A. M., Ilyas M. (2021). Smart city GIS mapping and analysis of intrusion detection. In: 2021 IEEE International Conference on Electronics, Computing and Communication Technologies. https://doi.org/10.1109/ICECCT52121.2021.9616943.

Amin R.W., Sevil H.E., Kocak S., Francia G. III, Hoover P. (2021). The spatial analysis of the malicious uniform resource locators (URLs): 2016 dataset case study. Information, vol. 12, no. 1, art. 2. https://doi.org/10.3390/info12010002.

Andrade R.O., Yoo S.G., Tello-Oquendo L., Ortiz-Garces I. (2020). A comprehensive study of the IoT cybersecurity in smart cities. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3046442.

Arvidsson B., Johansson J., Guldåker N. (2021). Critical infrastructure, geographical information science and risk governance: A systematic cross-field review. Reliability

Engineering and System Safety, vol. 213, art. 107741. https://doi.org/10.1016/j.ress.2021.107741.

Besiekierska A., Czaplicki K. (2022). Cybersecurity of spatial information. GIS Odyssey Journal, vol. 2, no. 2, pp. 23–30. https://doi.org/10.57599/gisoj.2022.2.2.23.

Check Point Software Technologies (2026a). Threat intelligence & research. https://www.checkpoint.com/solutions/threat-intelligence-research/ [access: 10.04.2026].

Check Point Software Technologies (2026b). Live cyber threat map. https://threatmap.checkpoint.com/ [access: 10.04.2026].

Clarke A., Martin A., Reichmann N. (2025). MITRE uses ArcGIS Knowledge to analyze critical infrastructure dependencies. ArcGIS Blog. https://www.esri.com/arcgis-blog/ [access: 10.04.2026].

Dragos D., Schmeelk S. (2021). Locating the perpetrator: Industry perspectives of Cellebrite education and roles of GIS data in cybersecurity and digital forensics. In: K. Arai (ed.), Intelligent Computing. Lecture Notes in Networks and Systems, vol. 285, pp. 1041–1050. Springer, Cham. https://doi.org/10.1007/978-3-030-80129-8_68.

Esri (2015). The geospatial approach to cybersecurity: Implementing a platform to secure cyber infrastructure and operations. White paper. Environmental Systems Research Institute. https://www.esri.com/content/dam/esrisites/sitecore-archive/Files/Pdfs/library/whitepapers/pdfs/geospatial-approach-to-cybersecurity.pdf [access: 10.04.2026].

Górny P. (2025). Methods for identifying cyber threats in GIS systems. Comparative analysis. GIS Odyssey Journal, vol. 5, no. 2, pp. 121–134. https://doi.org/10.57599/gisoj.2025.5.2.121.

Howley D. (2015). How to watch worldwide cyberattacks – live! Yahoo Tech. https://tech.yahoo.com/general/article/how-to-watch-worldwide-cyberattacks-live-124594707994.html [access: 10.04.2026].

Hui Z., Baynard C.W., Hu H., Fazio M. (2015). GIS mapping and spatial analysis of cybersecurity attacks on a Florida university. In: 2015 IEEE International Conference on GeoInformatics. https://doi.org/10.1109/GEOINFORMATICS.2015.7378714.

Information is Beautiful (2024). Updated: World's biggest data breaches – 450+ hacks in one visualisation. https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ [access: 10.04.2026].

Islam R., Bose R., Roy S., Khan A.A., Sutradhar S., Das S., Ali F., AlZubi A.A. (2025). Decentralized trust framework for smart cities: A blockchain-enabled cybersecurity and data integrity model. Scientific Reports, vol. 15, art. 23454. https://doi.org/10.1038/s41598-025-06405-y.

Jiang D., Gao C., Guo Q., Chen S., Hao M. (2023). Geographical properties and thinking of cyberspace. Journal of Geo-information Science, vol. 25, no. 10, pp. 1923–1932. https://doi.org/10.12082/dqxxkx.2023.220169.

Joshi S., Baviskar A., Rajmane S. (2026). A review of cybersecurity in smart cities and intelligent transport systems. Discover Internet of Things, vol. 6, art. 41. https://doi.org/10.1007/s43926-026-00312-y.

Kalinin M., Krundyshev V., Zegzhda P. (2021). Cybersecurity risk assessment in smart city infrastructures. Machines, vol. 9, no. 4, art. 78. https://doi.org/10.3390/machines9040078.

Kiedrowicz M. (2025). GIS security incident management: Practical approaches and standards. GIS Odyssey Journal, vol. 5, no. 1, pp. 59–67. https://doi.org/10.57599/gisoj.2025.5.1.59.

Kiedrowicz M., Stanik J. (2024). GIS information system contingency plan as a key artifact in the cybersecurity management lifecycle. GIS Odyssey Journal, vol. 4, no. 1, pp. 39–53. https://doi.org/10.57599/gisoj.2024.4.1.39.

Kiedrowicz M., Stanik J., Worwa K. (2025). The role of DevSecOps in ensuring business continuity and resiliency of GIS systems. Communications of International Proceedings, vol. 2025, no. 37, art. 4630325. https://doi.org/10.5171/2025.4630325.

Lewis T.G. (2020). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation (3rd ed.). John Wiley & Sons.

Malatji M., Marnewick A.L., Von Solms S. (2022). Cybersecurity capabilities for critical infrastructure resilience. Information and Computer Security, vol. 30, no. 2, pp. 255–279. https://doi.org/10.1108/ICS-06-2021-0091.

Miłek M. (2025). Use of the capabilities of GIS systems in the area of cybersecurity. GIS Odyssey Journal, vol. 5, no. 2, pp. 73–91. https://doi.org/10.57599/gisoj.2025.5.2.73.

National Institute of Standards and Technology (2022). Secure Software Development Framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities. NIST Special Publication 800-218. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-218.

Shabbir M., Kamal M., Ullah Z., Khan M.M. (2023). Securing autonomous vehicles against GPS spoofing attacks: A deep learning approach. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3319514.

Shafique A., Mehmood A., Elhadef M. (2021). Detecting signal spoofing attack in UAVs using machine learning models. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3089847.

Sobeslav V., Cech P., Horalek J., Ponce D., Urbanik P. (2026). An ontology-driven knowledge-based system for modeling cybersecurity architectures in smart cities and open data environments. Journal of Cases on Information Technology, vol. 28, no. 1. https://doi.org/10.4018/JCIT.399500.

Stanik J., Kiedrowicz M. (2022a). Risk in GIS systems. GIS Odyssey Journal, vol. 2, no. 1, pp. 39–63. https://doi.org/10.57599/gisoj.2022.2.1.39.

Stanik J., Kiedrowicz M. (2022b). Statement of applicability as a key element of the GIS certification process in the light of cybersecurity standards. GIS Odyssey Journal, vol. 2, no. 2, pp. 79–92. https://doi.org/10.57599/gisoj.2022.2.2.79.

Stanik J., Kiedrowicz M. (2025). Integration of national cybersecurity standards into the geographic information systems in the context of critical infrastructure security management. GIS Odyssey Journal, vol. 5, no. 1, pp. 111–121. https://doi.org/10.57599/gisoj.2025.5.1.111.

Tian Z., Zhuo M., Liu L., Chen J., Zhou S. (2023). Anomaly detection using spatial and temporal information in multivariate time series. Scientific Reports, vol. 13, art. 4400. https://doi.org/10.1038/s41598-023-31193-8.

Vasdev K. (2020). GIS in cybersecurity: Mapping threats and vulnerabilities with geospatial analytics. International Journal of Core Engineering and Management, vol. 6, no. 8, pp. 190–195. https://www.ijcem.org [access: 10.04.2026].

Veerasamy N., Moolla Y., Dawood Z. (2022). Application of geospatial data in cyber security. In: Proceedings of the 21st European Conference on Cyber Warfare and Security, pp. 305–313. https://doi.org/10.34190/eccws.21.1.447.