GIS Odyssey Journal

2025 • Volume 5 • Number 2

https://doi.org/10.57599/gisoj.2025.5.2.73

Marzenna Miłek[1]

USE OF THE CAPABILITIES OF GIS SYSTEMS IN THE AREA OF CYBERSECURITY

Abstract: We are currently dealing with a very dynamic development of digital technologies and, consequently, we are also dealing with an increasing number of cyber threats. This state of affairs makes ensuring the security of the information processed in an organisation and the security of the IT systems in operation a key element of the security strategy of any IT solution in which data is processed. One class of such systems, processing collections of key information, are Geographic Information Systems (GIS). Information security and proper protection of data, especially strategic data, is becoming an increasing challenge. This paper outlines how geo-location tools can be used to support cyber-security and cyber-resilience building activities. It discusses how GIS systems can be used to develop a roadmap of operations for defence and intelligence systems and help analyse, share information and create situational awareness. A literature review and case studies of attacks on GIS systems and data leaks identify the main challenges and requirements related to the possibilities of using GIS-class systems in the area of cyber security. The results of the research present directions for building cyber resilience and cyber responsibility for the data held by the organisation. The article concludes with practical conclusions and suggestions for future research directions in the area of using GIS class systems in the field of cyber awareness and cyber security. Although geospatial analysis has been extensively applied in physical security and logistics, its application in digital threat environments is a relatively unexplored area of research.

Keywords: cybersecurity, Geographic Information Systems (GIS), security management, systems integration

Received: 18 June 2025; accepted: 13 July 2025

[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0009-0002-9806-6755, email: marzenna.milek@wat.edu.pl

Introduction

In the era of modern cyber warfare, any information system can become a target of cybercriminal attacks. In response to increasing threats, numerous cybersecurity tools and systems have been developed, however, GIS (Geographic Information Systems) are rarely included among these protective solutions. This article attempts to analyze how GIS-class systems can support strengthening cyber resilience against various types of cyber threats.

Contemporary cyber threats are characterized by rapid development and growing complexity, necessitating the creation of effective protection strategies. Geolocation and mapping tools enable tracking, identification, and analysis of attack-related data, as well as visualization of such information on maps. This allows not only for locating objects, people, or events but also for analyzing movement patterns, the extent of incidents, and monitoring changes in geographical space. These capabilities prove especially valuable in the field of cybersecurity.

Geospatial data plays a crucial role in prioritizing threats and identifying critical areas of interest. Although GIS systems are widely used in urban planning, environmental management, and business processes, their application in cyberattack analysis remains a relatively underexplored area. The literature lacks comprehensive studies presenting the use of GIS data analysis in the context of digital threats.

As cybercrime evolves in scale and complexity, traditional cybersecurity approaches become insufficient. The dynamic nature of threats calls for interdisciplinary solutions that leverage underutilized data sources. GIS systems, primarily known for spatial planning applications, are gaining importance in cyber threat analysis due to their ability to visualize spatial patterns and support decision-making processes (Saadat Barikani, 2024).

This paper aims to investigate the potential of integrating geospatial data into cybersecurity systems to enhance situational awareness, threat prioritization, and response strategies. Furthermore, it addresses the challenges, requirements, and best practices associated with building cyber resilience in GIS systems, thereby filling a research gap related to the specific nature of data processed in these systems.

Despite the growing number of analyses on cyberattacks and data breaches, there is a lack of detailed research on cybercriminals' motivations for targeting GIS data and how such data is subsequently used. GIS systems employed in infrastructure and telecommunications often serve as platforms integrating business data, asset management, and reporting processes. Consequently, the data processed is often strategic, underscoring the need for its protection and responsible management in the cybersecurity context.

In the era of increasing cyber threats and increasingly sophisticated attacks on information systems, understanding the role of geospatial data in the context of digital security becomes crucial. The main problem of this article is the identification and analysis of the business and strategic potential of data stored and processed in GIS-class systems, with particular emphasis on their significance for cybersecurity. This issue includes assessing the value of such data, their importance for the functioning of entities and organizations within their environment, as well as the potential use of the collected information to conduct targeted attacks, especially on critical infrastructure and other key assets.

The article is divided into the following parts:

- Introduction – presentation of the background and importance of the topic in the era of cyberwar, as well as the goals and conclusions resulting from the topics discussed in the article.
- The literature review presents the importance of cyber protection using examples of data leaks and their consequences.
- Research problem – this part articulates the central research questions, focusing on the potential applications of Geographic Information Systems (GIS) in cybersecurity and cyberattack scenarios. It further investigates approaches to developing cyber resilience through the integration of GIS technologies.
- Methodology is a description of the research methods and the tools and methods used to obtain an answer to the research problem.
- Discussion – a presentation of the obtained results in the context of the analysis of the literature and conclusions resulting from practice.
- At the end there is a summary of the main goals, a discussion of the final conclusions and recommendations for the potential of future research.

Literature review

In the literature concerning the use of data processed in GIS-class systems, several main research approaches can be distinguished. The first approach involves the perspective of GIS system manufacturers, who in their reports and comparative analyses focus on evaluating the cybersecurity of the solutions offered and present case studies of implementations, provided that access to such information has been granted by clients. The second approach includes studies and reports documenting data breach incidents and analyzing the consequences of these events, including the potential use of disclosed information for attacks other than direct cyberattacks.

Among the key literature contributions is the publication The Geospatial Approach to Cybersecurity released by Esri (2015), which provides a detailed description of the implementation of the ArcGIS system to support cybersecurity efforts. Additionally, the literature contains numerous works addressing the applications of geolocation data as well as reports describing cases of theft or leakage of data from geospatial databases. However, despite growing interest in the topic, there is a lack of comprehensive studies integrating the use of geospatial data with cybersecurity systems.

Within the scope of this study, a literature analysis was conducted that, on the one hand, demonstrates the potential of GIS-class tools in the context of data analysis and visualization, and on the other hand, documents cases of cybercrime related to systems storing geospatial data (Esri, 2014). The aim of this analysis was to demonstrate the feasibility of assessing the usefulness of geospatial data and mapping such data in connection with IT incident data, which may serve as a foundation for developing new methods to support cybersecurity.

Research problem

Accordingly, the article focuses on answering the following research questions:

1. How can GIS-class systems be effectively utilized in the field of cybersecurity?
2. What opportunities does the use of geolocation data provide for enhancing organizational cyber resilience?
3. What are the most effective methods for acquiring cyber resilience in the context of a dynamically changing external environment?
4. What conclusions can be drawn from case studies of cyberattacks, and how can they be applied in practice using GIS-class systems?

The analysis of these issues aims not only to deepen theoretical knowledge but also to identify practical solutions that can contribute to improving digital security through the integration of geospatial technologies.

GIS Systems and Cybersecurity. In the context of escalating cyber threats, Geographic Information Systems (GIS) are assuming an increasingly significant role in enhancing cybersecurity frameworks. GIS technologies provide cybersecurity professionals with advanced tools to identify and analyze trends and patterns that may remain obscured in conventional reporting formats. By enabling the visualization and examination of data from diverse perspectives—such as spatial mapping of network infrastructures, data centers, and other critical assets—GIS facilitates more informed decision-making regarding the implementation of appropriate security measures, encompassing both physical protections and technological safeguards (Esri, 2015; Esri, 2023). This multidimensional approach contributes to a comprehensive understanding of vulnerabilities and supports the development of targeted strategies to mitigate cyber risks.

Definition of Geospatial Data. Geospatial data is defined as a combination of locational information—typically coordinates on the Earth's surface—and associated attributes that describe key characteristics of objects, events, or phenomena, along with temporal information indicating the time or period during which these locations and attributes exist (IBM, 2022). When geospatial analytics are applied to such data, the integration of spatial and temporal dimensions with conventional data types enables the creation of diverse visualizations tailored to specific analytical needs. This mode of data representation—through maps, cartograms, charts, and other graphical formats – provides a comprehensive perspective that mitigates the risk of overlooking critical information. In the context of increasingly frequent cyberattacks, leveraging geospatial data analysis facilitates more rapid and informed decision-making.

According to IBM (2022), major types of geospatial data include:

1. Vector Data: Represents geographic features as discrete points, lines, and polygons. This data type encodes spatial relationships through coordinates and topological connections between features.

2. Raster Data: Depicts geographic phenomena as a grid of cells or pixels, where each pixel value corresponds to a specific attribute of the feature at that location, such as elevation or temperature.
3. Satellite Imagery: A subset of raster data obtained via remote sensing technologies like satellites or drones. It is widely used for applications including land use mapping and environmental monitoring.
4. LiDAR Data: Light Detection and Ranging (LiDAR) data is a remote sensing method that employs laser pulses to generate highly detailed three-dimensional maps of terrain and vegetation.
5. GPS Data: Captures the precise location and movement of objects or individuals using the Global Positioning System, commonly applied in navigation, tracking, and mapping.
6. Census Data: Provides demographic and socioeconomic information about populations, supporting urban planning, marketing strategies, and social science research.
7. Weather and Climate Data: Represents atmospheric conditions and climate patterns, essential for weather forecasting, climate modeling, and environmental assessments.
8. Drawn Images: Computer-Aided Design (CAD) images containing architectural and geographic representations of buildings or infrastructure.
9. Social Media Data: Geotagged social media posts and activity, enabling trend analysis and behavioral insights by region.

The integration and analysis of these diverse geospatial data types offer powerful tools for enhancing situational awareness and strategic decision-making in various domains, including cybersecurity.

Ways of using geospatial data in the context of cyber threats. Given that GIS systems collect valuable data, there are risks of cyber threats seeking to exploit that data. Given the data that is available from GIS systems, there are two ways to leverage this data. The first is to directly leverage the data to monetize the information by using it for profit. There is a great deal of theft of data from GIS-class systems worldwide. For example, the leak of personal data in Poland in 2021, where the personal data of more than 20,000 police officers, employees of border guards, fire brigades, tax offices, municipal guards or state security services was probably made available by mistake in the GIS service of the Government Security Centre. The data file was made publicly available in the cloud service ArcGIS Online, where, in addition to name and surname, the file contained data such as PESEL, telephone number and workplace address. This resulted in a potential threat to identify the whereabouts of a specific functionary during working hours, which in turn could be the reason for a potential attack on a public figure (Geoforum, 2021).

Utilization of Geospatial Data in the Context of Cyber Threats: Enhancing Cybersecurity Awareness through GIS Systems. Geographic Information Systems (GIS) inherently collect and process valuable spatial and attribute data, which, while offering significant analytical advantages, also present considerable risks in the context of cyber threats. The sensitive nature of geospatial data stored within GIS platforms makes these systems potential targets for cybercriminal activities aimed at exploiting such information. Understanding these risks is critical for developing effective cybersecurity awareness and resilience strategies.

The exploitation of GIS data can be broadly categorized into two primary pathways. The first involves the direct misuse of geospatial information for financial gain, where stolen data is monetized or leveraged for illicit purposes. Globally, numerous incidents of data breaches involving GIS-class systems have been reported, underscoring the vulnerability of these platforms. A notable example occurred in Poland in 2021, when personal data of over 20,000 individuals – including police officers, border guards, firefighters, tax office employees, municipal guards, and state security personnel – was inadvertently exposed through the Government Security Centre's GIS service. The compromised dataset, hosted on the ArcGIS Online cloud platform, contained sensitive identifiers such as full names, PESEL numbers (national identification numbers), telephone contacts, and workplace addresses (Geoforum, 2021).

This breach not only violated data privacy but also introduced significant security concerns by potentially enabling adversaries to track the real-time locations and movements of key public officials during working hours. Such exposure heightens the risk of targeted attacks against public figures and critical personnel, thereby amplifying the importance of integrating cybersecurity considerations into GIS data management.

From the perspective of cybersecurity awareness, GIS systems offer a dual opportunity. On one hand, they must be safeguarded against unauthorized access and data leakage. On the other hand, the spatial and temporal visualization capabilities of GIS can be harnessed to enhance situational awareness regarding cyber threats. By mapping cyber incidents, identifying vulnerable infrastructure locations, and analyzing attack patterns spatially, GIS tools empower cybersecurity professionals to anticipate, detect, and respond to threats more effectively.

Therefore, leveraging GIS not only as a repository of sensitive data but also as an active analytical platform can significantly contribute to building organizational and societal awareness of cyber risks. This approach facilitates informed decision-making, targeted resource allocation, and the development of proactive defense mechanisms tailored to the spatial dynamics of cyber threats.

Utilization of GIS Systems for Geospatial Data Analysis in the Context of Cyber Threats. A second significant application of GIS systems is the analysis of geospatial data to examine information related to cyberattacks, enabling the identification of the location, manner, timing, and scope of such incidents. This type of analysis facilitates a deeper understanding of the characteristics of cybercriminal activities, thereby supporting more effective threat mitigation.

In practice, the construction of reports visualizing cyber threats relies on addressing key questions such as:

1. Where are cyberattacks occurring?
2. What are the most common targets?
3. Where do the sources of attacks originate?
4. What is the location of the infrastructure used to conduct cyberattacks, such as proxy servers, command and control servers, email servers, or other tools?

5. What types of cyberattacks can be classified?
6. What attack methods have been employed?

GIS platforms, such as ArcGIS, provide advanced tools for monitoring known target locations, analyzing adversary behavior signatures, and identifying emerging threats (Esri, 2023). By integrating geospatial data with cyber threat intelligence, it is possible to create dynamic threat maps that consider both attack sources and their targets, as well as methods of operation (Microsoft, 2023).

Threat analysis platforms leverage artificial intelligence and machine learning techniques to filter data, automatically prioritize risks, and generate alerts, enabling security teams to respond rapidly to incidents (Microsoft, 2023). Combined with GIS spatial visualization capabilities, this approach enhances understanding of the distribution and dynamics of cyber threats, thereby supporting informed decision-making regarding the protection of critical infrastructure and organizational assets.

In summary, the integration of GIS systems with cyber threat analysis constitutes a modern tool that supports building resilience against attacks and enhances situational awareness in the field of cybersecurity.

And if we already have some history or comparisons can we further analyze if and how the pattern of cyber-attacks has changed over time?

In this case, the combination of geospatial data and cyber threat analytics will not only allow us to visualize the results, but it will also be possible to present the types and methods of attacks, which targets were targeted, along with the identification of the location, duration of the attack or frequency. With such analysis, we can simulate potential future events.

Analytics. When historical data or comparative datasets are available, it becomes feasible to conduct longitudinal analyses to determine if and how patterns of cyberattacks have evolved over time. The integration of geospatial data with cyber threat analytics not only facilitates the visualization of such temporal trends but also enables a comprehensive characterization of attack types, methodologies, targeted assets, and associated spatial-temporal parameters such as location, duration, and frequency of incidents.

This multidimensional analysis supports the identification of shifts in attacker behavior and emerging threat vectors, thereby enhancing the understanding of the dynamic nature of cyber threats. Moreover, by leveraging these insights, it is possible to develop predictive models and simulate potential future cyberattack scenarios, which can inform proactive defense strategies and resource allocation.

Such an approach underscores the value of combining spatial and temporal dimensions in cybersecurity research, providing a robust framework for monitoring, analyzing, and anticipating cyber threats in an increasingly complex digital landscape.

Advances in Geospatial Data Accessibility and the Role of IoT Technologies in Cybersecurity. Recent technological advancements have significantly simplified the acquisition and utilization of geospatial data and analytics, eliminating the necessity for specialized and complex software traditionally required for such tasks. The proliferation of Internet of Things (IoT) technologies has further expanded the capacity to collect spatial and locational data across diverse contexts, ranging from large organizational infrastructures to everyday consumer applications, such as autonomous vacuum cleaners and robotic lawn mowers (Safe, 2022).

Historically, spatial information was conveyed through rudimentary means such as maps, compasses, or smoke signals to denote geographic locations. In contrast, contemporary IoT devices are inherently equipped with geolocation capabilities, facilitating continuous and automated data collection. This evolution profoundly impacts population tracking, environmental monitoring, and the generation of predictive models and strategic action plans. In the context of cybersecurity, the widespread availability of geospatial data through IoT devices introduces both opportunities and challenges. On one hand, the integration of geospatial analytics enhances situational awareness by enabling real-time monitoring of critical infrastructure, identification of attack vectors, and mapping of cyber threat origins and propagation paths. This spatial intelligence supports more effective threat detection, incident response, and resource allocation.

On the other hand, the vast amount of location-based data generated by IoT devices increases the attack surface, exposing sensitive information to potential exploitation by malicious actors. Unauthorized access to geospatial data can lead to privacy breaches, facilitate targeted cyberattacks, and compromise the security of critical assets. Therefore, ensuring the confidentiality, integrity, and availability of geospatial information within IoT ecosystems is paramount for maintaining robust cybersecurity postures.

The democratization of geospatial data collection through IoT not only enhances the granularity and timeliness of spatial information but also necessitates the development of advanced security frameworks that address the unique vulnerabilities associated with location-based data. By leveraging geospatial analytics within secure environments, organizations can significantly improve their cyber resilience and proactive defense capabilities.

Thanks to the use of GIS systems, it is possible to more effectively detect and analyze various cyber threats, especially those with a spatial dimension or related to geographically distributed infrastructure. Below are specific examples of threats that can be better monitored and countered through GIS:

- Attacks on critical infrastructure – GIS allows for the localization and visualization of critical infrastructure elements such as energy grids, telecommunications, or transportation networks, enabling rapid detection and analysis of attacks targeting these assets and assessment of potential damage scope.
- Propagation of malware and DDoS attacks – spatial analysis enables mapping of attack sources and their propagation routes within networks, supporting identification of key vulnerable points and optimization of defensive measures.
- Phishing and social engineering attacks – GIS facilitates geographic analysis of phishing campaigns or fake websites, helping identify high-risk regions and plan educational and preventive actions.
- Attacks on IoT devices – locating and monitoring IoT devices via GIS allows detection of anomalies in device behavior within specific areas, which is crucial for preventing attacks exploiting vulnerabilities in these devices.

- Incident management and crisis response – GIS supports coordination of emergency services during crises such as terrorist attacks or IT system failures by visualizing threats, evacuation routes, and locations of rescue resources.
- Trend analysis and threat forecasting – by integrating historical and current data, GIS enables analysis of changes in the nature and distribution of cyberattacks over time, allowing modeling of potential future threats and preparation of appropriate defense strategies.
- Detection and monitoring of AI- and ML-related threats – GIS can support spatial analysis of incidents involving advanced artificial intelligence techniques, enabling identification of areas with increased activity of AI-based attacks and assisting adaptive defense mechanisms.

In summary, GIS systems, due to their ability to integrate and visualize spatial data, constitute a key tool in detecting, analyzing, and countering diverse cyber threats, especially those with a geographic dimension or related to distributed infrastructure. The use of GIS enhances the efficiency of preventive measures, monitoring, and incident response, thereby improving the level of digital security and protection of critical state and organizational assets.

The Use of Geospatial Data in Monitoring Cybersecurity Threats and Crime Analysis: The Case of Poznań. Contemporary applications of geospatial data in cybersecurity focus on monitoring hacker group activities and analyzing their behaviors, with particular attention to the repeatability of event sequences. This approach enables the creation of maps and identification of trends related to potential future attacks. Additionally, integrating social media analysis allows for a more comprehensive understanding of possible cybercriminal actions. The collected data serve as a basis for developing attack scenarios, their visualization, determining the area of impact, and assessing the consequences of incidents. Beyond criminal aspects, geolocation data integrated with other databases can also support defensive measures, cyber intelligence development, and operations of local public services, including the police. A practical example of the application of Geographic Information Systems (GIS) in crime prevention and combating crime can be observed in the city of Poznań. GIS serves as a vital tool supporting institutions responsible for public safety by enabling spatial analysis of criminogenic phenomena. One key method is hotspot analysis, which considers crime concentration alongside additional thematic layers such as demographics and land use. Such analyses are essential for understanding the causes of crime and formulating effective strategies to mitigate it.

In Poznań, hotspot analysis revealed that the highest concentration of car thefts is closely linked to the characteristics of the Rataje district. The specificity of this area, including large housing estates and particular social conditions (e.g. lack of strong social ties, high population density, numerous parking lots, and quick access to the A2 motorway), creates favorable conditions for criminal activity. Conversely, factors such as the availability of alcohol outlets or proximity to green areas do not show a significant influence on the occurrence of car thefts. The spatial distribution of these incidents, illustrated against the urban built-up background, was developed based on data from the

Poznań City Police Headquarters and the Topographic Objects Database (BDOT) (Arkanagis, 2019).

In summary, integrating geospatial data with threat analysis – both in cyberspace and the physical urban environment – constitutes an effective tool supporting decision-making processes in the field of security. The use of GIS allows for a better understanding of the spatial determinants of threats and facilitates the planning of preventive and intervention measures, thereby enhancing the efficiency of agencies responsible for maintaining public order and cybersecurity.

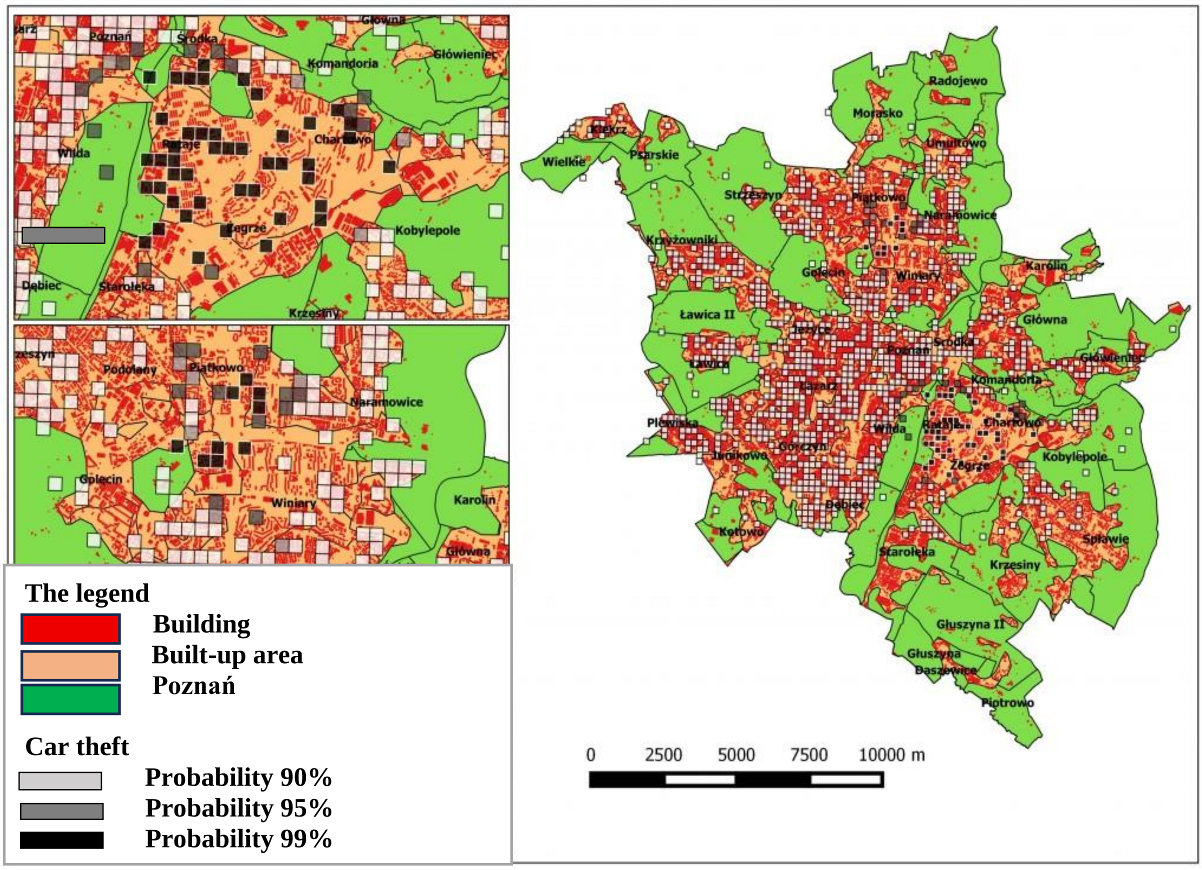

Fig. 1. Spatial distribution of car thefts with various probabilities against the background of built-up areas in Poznań
Source: Arkanagis, 2019; based on data from the Poznań City Police Headquarters and BDOT

The Role of Geospatial Data in Enhancing Cybersecurity and Building Cyber Resilience. To improve security and develop effective defense mechanisms, numerous cybersecurity experts increasingly utilize geospatial data to predict potential cyberattacks and analyze their progression. Despite the ongoing digital transformation across many organizations, functional requirements for new systems often overlook the capabilities offered by geospatial data. This is notable given the substantial evidence demonstrating that the integration of Geographic Information Systems (GIS) into cybersecurity frameworks can significantly enhance cyber resilience against emerging threats.

The scientific literature contains several key studies that highlight the critical relationship between geolocation data mapping and cyber threat analysis. For instance, researchers from the University of Florida conducted a pioneering study mapping cyberattacks onto geospatial datasets (Hu et al., 2015). Their geospatial analysis revealed spatial patterns of cyberattacks and identified countries with heightened vulnerability, as well as specific hotspots within the United States.

Similarly, Xui & Li (2014) performed an analysis correlating IP address data with spatial databases to geolocate cybercrime activities. Bhargava et al. (2015) developed a framework to classify various types of cybercrimes in accordance with Indian legislation and analyzed their spatial distribution across India. In the defense sector, German cybersecurity professionals have integrated GIS with cybersecurity tools to uncover patterns of cyberattacks (Conklin, 2022). Furthermore, commercial cybersecurity firms such as Kaspersky (2021), Bitdefender (2022), and Fortinet (2022) provide geospatial threat maps visualizing cyber threats detected by their software solutions.

These examples illustrate how proficient use of GIS-class data can contribute not only to preventing potential cyberattacks but also to establishing foundational elements for cyber resilience and responsible cybersecurity practices. This analysis of geospatial data utilization and its associated benefits – beyond the conventional domains of spatial data processing – demonstrates the potential to influence cybersecurity levels and strengthen cyber defense mechanisms. The diverse datasets processed and stored within GIS platforms enrich the visualization and understanding of various phenomena, including current cyber threats, thereby supporting more informed decision-making.

Methodology

This study employs a multi-method approach to investigate the utilization of geolocation data in enhancing cyber resilience. Adopting a conceptual research framework, the study synthesizes insights from cybersecurity, data science, and geoinformatics literature to develop a comprehensive model. The methodological process comprises the following sequential stages:

1. Literature Review: A systematic examination of existing scholarly work on the application of Geographic Information Systems (GIS) within cybersecurity and related fields was conducted to identify prevailing knowledge gaps. The review encompassed peer-reviewed journal articles, academic books, conference proceedings, and authoritative research reports.
2. Analytical Mapping: Key geospatial variables relevant to cyber threat analysis were identified and categorized. These include attributes such as the origin of attacks, frequency, temporal patterns, attack typologies, and severity levels. This step facilitated the delineation of critical data points for subsequent modeling.
3. Framework Development: Based on the findings from the literature and analytical mapping, a conceptual framework was constructed. This model delineates the stages

and components necessary for effective integration of GIS technologies into cybersecurity infrastructures, emphasizing data flows, analytical processes, and decision-support mechanisms.

4. Use Case Scoping: Potential applications of the proposed framework were explored across diverse scenarios, including protection of critical infrastructure, vulnerability mapping of network assets, and global cyber threat monitoring. This phase aimed to contextualize the framework's utility and adaptability.
5. Expert Consultation: Semi-structured interviews and workshops were conducted with cybersecurity professionals to gather qualitative insights regarding the practical deployment of GIS in cyber defense strategies. Additionally, case studies of data breaches in Poland and internationally were analyzed to extract lessons and validate the framework's relevance.

Through this rigorous methodological approach, the study advances a nuanced understanding of how geospatial data can be leveraged to bolster cyber defense capabilities and informs future research and practice in this interdisciplinary domain.

Results and discussion

Currently, the use of geospatial data is no longer limited solely to national security institutions. An increasing number of entities recognize the potential of these data, leveraging their unique properties and analytical capabilities. There is a growing awareness that integrating geospatial data can effectively strengthen cyber defense mechanisms and enhance organizational security.

Spatial data have long been a critical resource for defense institutions, armed forces, intelligence services, emergency units, and teams responsible for protecting critical infrastructure. As a result of a case study on the application of geolocation data, several areas have been identified where geospatial data can be effectively utilized to build the foundations of an organization's cyber resilience. The presented list of characteristics aims to demonstrate the added value that geospatial data bring to enhancing cyber defense capabilities and increasing accountability in cybersecurity management.

Main areas of application of geolocation data in relation to cybersecurity:

1. Threat Tracking. A critical application of geospatial data within cybersecurity is the precise tracking of threats. By integrating defense mechanisms that associate digital activities with traceable physical locations, cybersecurity professionals can enhance monitoring and response efficacy (Brode, 2021). Geofencing techniques enable the establishment of designated safe zones, restricting access exclusively to predefined spatial boundaries. Access attempts originating from unauthorized or blacklisted regions can be automatically blocked and flagged for subsequent investigation. Furthermore, detection of malicious activities localized to specific geographic areas facilitates the tracing of threat actors' behaviors, enabling the identification of recurrent attack patterns and frequently targeted assets. This geospatial intelligence supports proactive interventions prior to the materialization of cyberattacks. Additionally, certain geographic regions may emerge as hotspots for specific cyber threat categories,

warranting intensified surveillance and allocation of cybersecurity resources to mitigate vulnerabilities.

2. Data Analysis. Geospatial technologies facilitate the integration and synthesis of heterogeneous datasets originating from diverse sources and communication channels, thereby improving the identification of relationships between entities and events. This multi-source data fusion enhances analytical clarity and enables extraction of actionable insights. For example, cyberattack data initially presented in tabular form – enumerating affected locations – can be transformed into spatial representations such as thematic maps or regional aggregations, revealing geographic distributions and concentrations of attack types. Through spatial analysis, disparate data points coalesce into meaningful intelligence that underpins both knowledge generation and effective information dissemination.

3. Visualizations. The interpretation of voluminous numerical datasets often poses significant challenges, particularly when discerning latent trends or irregularities (Datumize, 2020). Geospatial visualization techniques provide structured, intuitive representations of complex data, thereby facilitating enhanced comprehension and analytical interpretation. By converting raw data into visual formats – such as maps, heatmaps, or charts – users can more readily detect spatial patterns, correlations, and anomalies. Visual clarity supports informed decision-making and enables multi-perspective data analysis. Moreover, graphical presentations accentuate anomalies; for instance, an improbable concentration of cyberattacks in a small population center may indicate data errors, which might be overlooked in purely textual or tabular formats. Consequently, geospatial visualization is a vital tool in cybersecurity, mitigating cognitive overload and accelerating the identification of inconsistencies or emerging threats within complex datasets.

4. Cyber Intelligence The transformation of raw geospatial data into actionable intelligence constitutes a foundational process in cybersecurity operations. Geographic Information Systems (GIS) enable the integration of geospatial information with auxiliary datasets for advanced analytical purposes. Effective visualizations derived from GIS facilitate decision-makers in identifying frequently targeted locations and attack vectors. This intelligence informs strategic allocation of resources, implementation of tailored security measures, and localization of awareness campaigns aimed at mitigating emerging cyber threats.

5. Cyber Threat Prioritization. Geospatial analytics enhances the prioritization of cyber threats by providing contextual insights into spatial and temporal patterns of attack intensity. Geographic tracking of threat surges allows cybersecurity experts to identify the most affected regions, thereby enabling risk assessment based on severity and frequency metrics. Longitudinal monitoring of geospatial trends assists in discerning whether specific threats are escalating or abating, which supports the differentiation between critical risks and those of lower urgency, optimizing resource deployment.

6. Protection of Cyber Infrastructure. Geospatial data supplies essential intelligence for the protection of digital infrastructure by elucidating attack patterns and pinpointing high-risk assets. This information underpins strategic planning and the implementation

of preventive measures, particularly when correlated with temporal trends. For example, chronological analyses may reveal attack spikes associated with known system vulnerabilities or significant events, guiding targeted investigations and mitigation strategies to bolster infrastructure resilience.

7. Collaboration and Coordination. Geospatial pattern recognition facilitates the identification of recurrent targets, such as specific hardware components or service providers. Leveraging these insights, cybersecurity professionals can foster collaboration with affected stakeholders to monitor and neutralize ongoing threats. At a macro level, the sharing of geospatial intelligence enables global cooperation among security agencies, intelligence services, and cybersecurity teams. This collaborative framework supports coordinated responses, vulnerability assessments, and the development of comprehensive operational plans to contain and mitigate the propagation of cyber threats.

8. Enhanced Response Capabilities. A principal advantage of geospatial visualization lies in its capacity to reveal emerging cyber threat trends in an accessible and interpretable format. The identification of spatial patterns allows for rapid correlation of threat behaviors with contextual parameters, facilitating expedited and effective response measures. This clarity enhances situational responsiveness and contributes to minimizing the impact of escalating cyber incidents.

9. Informed Decision-Making. The insights derived from geospatial data analysis significantly augment the cybersecurity decision-making process. Moving beyond reliance on intuition or generalized assumptions, stakeholders can formulate strategies grounded in empirical evidence. Geospatial visualizations improve situational awareness by providing a comprehensive understanding of the spatial dynamics of cybersecurity challenges, thereby enabling precise, evidence-based decisions that optimize defense postures and resource allocation.

To analyze the impact of geolocation data on cybersecurity, the following scientific methods can be applied, particularly statistical and analytical approaches:

- Anomaly Detection – identifying unusual or outlying patterns in geolocation and cyber data that may indicate suspicious activities or attacks.
- Time Series Analysis – modeling and forecasting trends of cyber threats in relation to geographic location, using methods such as ARIMA or LSTM, which allows detection of spatiotemporal attack patterns.
- Attack Signature Analysis – detecting known attack patterns in data that can be linked to specific geographic locations, enabling threat tracking and classification.
- Threat Modeling – identifying and classifying potential threats with consideration of geolocation data, supported by statistical analysis of historical and current data.
- Risk Analysis and Cybersecurity Risk Quantification – assessing the likelihood and impact of threats in a geographic context, facilitating prioritization of protective measures and resource allocation.
- Control Effectiveness Analysis – evaluating the effectiveness of existing security controls in specific locations based on incident data and their geolocation.

- Data Fusion – integrating geolocation data with other cyber and contextual data sources to obtain a more comprehensive picture of threats and their spatial distribution.
- Geospatial Visualization – creating maps and visual models that facilitate the identification of spatial threat patterns and anomalies, supporting decision-making processes.
- Trend Analysis and Forecasting – using statistical techniques to monitor and predict changes in threat activity within specific geographic regions.
- Attacker Behavior Modeling – analyzing and forecasting attacker tactics, techniques, and procedures (TTPs) with consideration of geolocation aspects, enabling improved defensive preparedness.

All of these methods require continuous adaptation and updating to effectively respond to the dynamically evolving cyber threat landscape and to fully leverage the potential of geolocation data in protecting information systems.

The scientific foundations for integrating GIS systems into cybersecurity strategies are based on several key principles and methods that arise from the interdisciplinary nature of these systems and their applications in security management:

- Optimization of resource and force management – GIS enables the creation of an integrated, shared operational picture, allowing for efficient planning and allocation of resources in the protection of cyberspace and critical infrastructure.
- Spatial and multidimensional analyses – GIS provides tools for advanced spatial analysis, enabling the identification of vulnerable areas, attack patterns, and correlations between incidents across geographic and temporal dimensions.
- Decision support in crisis situations – GIS facilitates data-driven decision-making based on reliable spatial data analysis, enhancing the effectiveness of responses to cyber incidents compared to intuition-based decisions.
- Threat modeling and simulations – the use of methods such as threat attribute matrices and game theory allows forecasting of potential attack locations and intensities, which is crucial for prevention and strategic planning.
- Data integration and interoperability – GIS serves as a platform that integrates diverse geospatial and cyber data, enabling comprehensive threat analysis and coordination of actions among various entities and systems.
- Situational awareness building and inter-organizational cooperation – through visualization and analysis of spatial data, GIS supports the creation of shared situational awareness and coordination within cybersecurity protection strategies.
- Theoretical and conceptual foundations – the development of GIS is grounded in solid theoretical bases from spatial analysis, statistics, computer science, and security engineering, ensuring scientific rigor of the applied methods and tools.

In summary, the integration of GIS systems into cybersecurity strategies is founded on scientifically justified methods of spatial analysis, threat modeling, and decision support, which enable effective risk and resource management in the dynamic cyber environment.

The growing frequency and sophistication of cyberattacks necessitate innovative approaches in cybersecurity. This paper explores the emerging integration of Geographic Information Systems (GIS) as a complementary tool in cybersecurity strategy. Geospatial data offers significant analytical value, allowing for the visualization, correlation, and interpretation of cyber threat information across spatial and temporal dimensions. Despite its potential, academic literature on GIS applications within cybersecurity remains limited. This study proposes a conceptual, multi-dimensional framework for incorporating geospatial data into cybersecurity operations. The framework is intended to provide a foundation for future applied research and practical implementation across various threat scenarios.

Explanation of Framework Components:

1. Raw Cyber Data Sources – initial datasets include logs of attacks, timestamps, origin IP addresses, and related metadata.
2. Data Collection & Preprocessing – data is cleaned, standardized, and prepared for geospatial tagging.
3. Geospatial Mapping & Data Layering – attack data is linked with geographic coordinates, and enriched with demographic, infrastructural, or political context.
4. Visualisation & Spatial Analytics – techniques such as heatmaps, temporal overlays, and cluster mapping are used to identify meaningful patterns.
5. Threat Detection & Prioritisation – geospatial trends support prioritisation based on frequency, proximity to critical assets, or known vulnerabilities. (Vasdev, 2020).
6. Intelligence Generation & Reporting – analytical findings are communicated through dashboards and intelligence reports for key stakeholders.
7. Strategic Response & Collaboration – based on insights, actions are coordinated across sectors and jurisdictions to implement targeted defenses.

The increasing frequency and complexity of cyberattacks necessitate the development of innovative methods and tools in the field of cybersecurity. This article analyzes the emerging integration of Geographic Information Systems (GIS) as a complementary instrument supporting cybersecurity strategies. Geospatial data demonstrate high analytical value, enabling the visualization, correlation, and interpretation of information related to cyber threats across spatial and temporal dimensions. Despite growing interest, the scientific literature on GIS applications in the context of cybersecurity remains limited. This study proposes a conceptual, multidimensional theoretical framework for integrating geospatial data with cybersecurity operations, intended to serve as a foundation for further empirical research and practical implementations across diverse threat scenarios.

How the Integration of GIS with Cybersecurity Tools Can Contribute to the Development of New Research Methods. The integration of Geographic Information Systems (GIS) with cybersecurity tools can significantly advance the development of novel research methodologies through the following mechanisms:

1. Enhanced Precision in Spatial Threat Analysis – GIS enables precise mapping of attack origins, threat propagation, and critical infrastructure locations, facilitating the creation of more detailed and dynamic models of cyber threats.

2. Combining Macro and Micro-Level Data – Similar to GIS integration with Building Information Modeling (BIM), merging geospatial data with operational and technical cybersecurity data allows for multidimensional analyses that combine broad spatial context with granular network and device information.
3. Support for Decision-Making and Defensive Planning – Visualizing threats within a geographic context improves understanding of attack dynamics, aiding the development of preventive strategies and incident response plans.
4. Development of Advanced Analytical and Simulation Tools – The integration fosters the creation of sophisticated platforms capable of simulating attack scenarios, analyzing spatiotemporal trends, and automatically detecting anomalies in threat distributions.
5. Improved Interoperability and Data Sharing – Utilizing GIS standards and integrating with infrastructure management and crisis response systems enhances data consistency and accessibility, which is crucial for interdisciplinary research and cross-sector collaboration.
6. Promotion of Interdisciplinary Research – Combining geoinformatics with cybersecurity opens new research avenues by linking spatial analysis methods with techniques for detecting and mitigating digital threats.

In summary, the integration of GIS with cybersecurity tools lays the foundation for innovative research methods that merge spatial analysis with advanced threat analytics, thereby increasing the effectiveness of critical infrastructure protection and enhancing overall digital security.

Conclusion

Geospatial data applied in the field of cybersecurity provide additional, multidimensional analytical perspectives. Visualization of data such as the geographic sources of attacks, the number of incidents in specific regions, and the classification of threat types enables analysts to more precisely detect spatial correlations and temporal patterns. For example, a heatmap of intrusion attempts may reveal a concentration of attacker activity in urban areas or correlate spikes in incident numbers with specific geopolitical events. Moreover, geospatial visualizations offer a more intuitive and effective understanding of data compared to raw numerical values. Anomalies, such as the reporting of an unrealistically high number of attacks in a small locality, can be immediately identified within a spatial interface, whereas such irregularities might remain unnoticed in traditional tabular formats. The proposed framework model facilitates the classification and prioritization of cyber threats based on spatial intelligence. Additionally, it promotes inter-organizational cooperation by enabling shared situational awareness and coordination of strategic actions responding to regional threat patterns.

This study presents the potential benefits arising from the integration of geospatial data into cybersecurity practices through the proposed conceptual framework. GIS technologies offer advanced capabilities in data visualization, threat detection, and strategic planning. Given the limited number of scientific studies in this area, future research should focus on empirical validation of the proposed model in real-world scenarios, evaluation of its effectiveness, and addressing key challenges such as data privacy protection and ensuring system interoperability.

Acknowledgements

This work was financed/co-financed by Military University of Technology under research project UGB 531-000023-W500-22.

References

Arkanagis (2019). https://www.arcanagis.pl/zlapani-na-goracym-uczynku-czyli-gis-owe-hotspoty-przestepczosci-miasta-poznania/? [access: 10.04.2025].

Bhargava N., Bhargava R., Tanwar, P.S. (2015). Analysing and Implementing Spatial Distribution of Cyber Crime Trends in India. International Journal of Advanced Research in Computer Science, 6(4).

Bitdefender (2022). Cyberthreat Real-time Map. https://threatmap.bitdefender.com/ [access: 26.04.2025].

Brode D. (2021). Geospatial intelligence and cyber defense: Mapping the invisible battlefield. Journal of Cybersecurity Research, 13(2), 45–58.

Conklin B. (2022) Cybersecurity: The Geospatial Edge. https://www.esri.com/about/newsroom/blog/german-cybersecurity-experts-use-gis/ Cybersecurity: The Geospatial Edge [access: 25.04 2025].

Datumize (2020). Why data visualization is important. https://datumize.com [access: 19.03.2025].

Esri (2014). The Geospatial Approach to Cybersecurity: An Executive Overview. Esri White Paper. https://www.esri.com/~/media/files/pdfs/library/whitepapers/pdfs/geospatial-approach-cybersecurity.pdf [access: 04.03.2025].

Esri (2015). The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations. https://www.esri.com/content/dam/esrisites/sitecore-archive/Files/Pdfs/library/whitepapers/pdfs/geospatial-approach-to-cybersecurity.pdf [access: 05.04.2025].

Esri (2023). Physical Security Management| System Integration with GIS. https://www.esri.com/en-us/industries/securityoperations/strategies/physical-security [access: 12.03.2025].

Fortinet (2022). Fortiguard Map. https://threatmap.fortiguard.com/ [access: 22.05.2025].

Geoforum (2021). https://geoforum.pl/news/30713/powazny-wyciek-danych-osobowych-w-rzadowej-usludze-gis [access: 05.04.2025].

Hu Z., Baynard Ch.W., Hu H.; Fazio M. (2015). GIS mapping and spatial analysis of cybersecurity attacks on a Florida university. https://ieeexplore.ieee.org/abstract/document/7378714 [access: 26.04.2025].

IBM (2022). What is geospatial data? https://www.ibm.com/topics/geospatial-data [access: 21.03 2025].

Kaspersky Labs (2021). Cyberthreat Real-time Map. https://cybermap.kaspersky.com [access: 16.05.2025].

Microsoft (2023). What is cybersecurity analysis? https://www.microsoft.com/pl-pl/security/business/security-101/what-is-cybersecurity-analytics [access: 21.03.2025].

Saadat Barikani S.A. (2024). Mapping Out Disaster Preparedness: The Role of GIS Applications in Effective Disaster Management. Precision Eco-landscaping. https://pelglobal.com/2024/02/23/mapping-out-disaster-preparedness-the-role-of-gis-applications-in-effective-disaster-management/ [access: 21.03 2025].

Safe (2022). What is spatial data? https://www.safe.com/what-is/spatial-data/ [access: 21.03.2025].

Vasdev K. (2020). GIS in Cybersecurity: Mapping Threats and Vulnerabilities with Geospatial Analytics. International Journal of Core Engineering & Management, vol. 6, no. 8, pp. 234–251.

Xiu W, Li X. (2014).The design of cybercrime spatial analysis system. In Information Science and Technology (ICIST), 4th IEEE International Conference on 2014 Apr 26, pp. 132–135.