GIS Odyssey Journal

2025 • Volume 5 • Number 1

https://doi.org/10.57599/gisoj.2025.5.1.111

Jerzy Stanik[1], Maciej Kiedrowicz[2]

INTEGRATION OF NATIONAL CYBERSECURITY STANDARDS INTO THE GEOGRAPHIC INFORMATION SYSTEMS IN THE CONTEXT OF CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT

Abstract: In the era of increasing digitization and dependence on information technologies, cybersecurity is becoming a key element of critical infrastructure management. Geographic Information Systems (GIS) play a vital role in monitoring, analyzing, and managing infrastructure assets. This paper explores the integration of national cybersecurity standards with GIS systems, focusing on critical infrastructure security management. A literature review and case studies of cybersecurity standards implementation in GIS systems allow for the identification of the main challenges and requirements. The article also presents methods of risk assessment and incident management in the context of GIS. The results of the research indicate the need for close cooperation between cybersecurity professionals and GIS users to ensure comprehensive protection of critical infrastructure. The article concludes with practical conclusions and proposals for future research directions in the area of integration of cybersecurity standards with GIS systems.

Keywords: Cybersecurity, Geographic Information Systems (GIS), Critical infrastructure, Compliance standards, Security management, Risk assessment, Systems integration

Received: 2 March 2025; accepted: 23 March 2025

[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-0162-2579, email: jerzy.stanik@wat.edu.pl

[2] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-4389-0774; email: maciej.kiedrowicz@wat.edu.pl

Introduction

M0odern society is increasingly relying on information and communication technology, making cybersecurity a key component of protecting critical infrastructure. Geographic Information Systems (GIS) play a vital role in the management of infrastructure resources, enabling the monitoring, analysis, and visualization of spatial data. In the context of critical infrastructure, such as energy, transportation, water and telecommunications, GIS systems are invaluable in ensuring business continuity and rapid response to incidents.

However, the complexity and importance of GIS systems also make them vulnerable to a variety of cyber threats. Hacking attacks, malware, data theft or sabotage can have serious consequences for the functioning of critical infrastructure. Therefore, the integration of national cybersecurity standards with GIS systems becomes essential to minimize risks and ensure the protection of data and systems.

National cybersecurity standards, such as ISO/IEC 27001, the NIST Cybersecurity Framework, and national regulations on critical infrastructure protection, provide guidelines and best practices for information security management. Implementing these standards in GIS systems allows you to create a consistent and effective approach to protection against cyber threats.

The literature emphasizes the importance of integrating cybersecurity standards with GIS systems, but there is a limited number of empirical studies in this area. Most of the available research focuses on general aspects of cybersecurity or on specific sectors of critical infrastructure, leaving aside the unique challenges and requirements associated with GIS. This article aims to fill this research gap by analyzing the challenges, requirements, and best practices related to the integration of cybersecurity standards into GIS systems.

Despite the growing importance of cybersecurity in the management of critical infrastructure, there is a limited number of studies on the integration of national cybersecurity standards with Geographic Information Systems (GIS). Most of the available research focuses on general aspects of cybersecurity or on specific critical infrastructure sectors such as energy or transportation, overlooking the unique challenges and requirements associated with GIS. There is also a lack of comprehensive case studies of the implementation of cybersecurity standards in GIS systems and the assessment of their effectiveness in the protection of critical infrastructure.

The main research problem is the identification and analysis of challenges and requirements related to the integration of national cybersecurity standards with GIS systems in the context of critical infrastructure security management. This includes assessing the effectiveness of these standards in minimizing the risk of cyber threats and ensuring the continuity of operations of key infrastructure services.

Therefore, the main research questions that will be analyzed in the article are:

- What are the main challenges and requirements of integrating national cybersecurity standards into GIS?

- How can cybersecurity standards be effectively implemented in GIS systems to protect critical infrastructure?
- What are the best practices and procedures for managing security in GIS?
- What are the most effective risk assessment and incident management methods for GIS?
- What are the results and conclusions of the case study of cybersecurity standards in GIS systems?

The article is divided into the following parts: Introduction – presentation of the background and meaning of the topic, the objectives of the article and its structure; Literature review – the importance of compliance standards such as ISO/IEC 27001, the NIST Cybersecurity Framework or national regulations on the protection of critical infrastructure is emphasized; Research problem – What are the efficacies and challenges of integrating national cybersecurity standards with GIS systems to protect and manage the security of critical infrastructure?; Methodology – a description of research methods and data collection tools and techniques to obtain a comprehensive picture of the integration of national cybersecurity standards with GIS systems; Discussion – Discussion of the results in the context of the literature, conclusions and practical implications, limitations of the research and proposals for further research; Conclusions – summary of the main findings, relevance of the results for theory and practice, and recommendations for future research.

Literature review

In the literature on the integration of cybersecurity standards with Geographic Information Systems (GIS), several key research areas can be distinguished. Books, scientific articles, domain journals and research reports provide valuable information on challenges and best practices in the field. One of the foundational sources is the book "The Geospatial Approach to Cybersecurity" published by Esri, which describes the implementation of the ArcGIS platform to ensure the cybersecurity of infrastructure and operations (Esri, 2015). This book emphasizes the importance of the geographical layer in the context of cyber operations and presents a geospatial model for perimeter defense. In "Applications of GIS to Cybersecurity," authors Brian Biesecker and Ken Mitchell examine how GIS can help address fundamental cybersecurity issues, such as the impact of cyberattacks on critical systems and infrastructure (Biesecker, 2018). This article also provides examples of how cybersecurity tools are integrated with the ArcGIS platform. Domain journals such as GIS Applications to Cybersecurity and Critical Infrastructure Protection provide detailed analysis on how to protect critical infrastructure with GIS technology. In this article, the authors discuss how integrating GIS systems with cybersecurity tools can improve situational awareness and support risk management (European Parliament and Council, 2024). Research reports, such as "The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations" by Esri, provide actionable guidance on how to implement cybersecurity standards in GIS. This report emphasizes the importance of prioritizing cybersecurity

activities in the context of strategic business activities and presents a geospatial model for assessing the impact of missions (Esri, 2015). In addition, in the article "Physical Security Management | System Integration with GIS" project describes how spatial analysis can increase physical security by identifying high-risk and vulnerable areas (Esri, 2023). Conferences such as the Network Security Congress (KBS) also provide valuable insights into modern cybersecurity challenges and the integration of GIS systems with cybersecurity tools.

Research problem

Definition and classification of GIS systems. Geographic Information Systems (GIS) are complex tools used to collect, store, analyze, and visualize spatial data. GIS enables the integration of geographic data with other types of information, allowing for a better understanding and management of natural resources, infrastructure, and social and economic processes. GIS systems can be classified in different ways, depending on their functions and applications. The most common GIS are desktop, server, mobile and web. Each of these types of GIS systems has its own specific features and applications that affect the way they are implemented and managed in security (Esri, 2015).

Cybersecurity standards: an overview. Cybersecurity standards are a set of guidelines and best practices to protect information systems from cyber threats. In the context of GIS systems, standards such as ISO/IEC 27001, the NIST Cybersecurity Framework, and national regulations for the protection of critical infrastructure are of key importance. ISO/IEC 27001 is an international standard for information security management that specifies requirements for the establishment, implementation, maintenance, and continuous improvement of an information security management system (ISMS) (Biesecker, et al., 2018). The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology, provides guidelines for identifying, protecting, detecting, responding, and recovering from cyber threats (Esri, 2014). National regulations, such as the Critical Infrastructure Protection Acts, set out the obligations and requirements for securing key assets and systems (Biesecker et al., 2018).

Principles of critical infrastructure security management. Critical infrastructure security management includes a range of activities to protect critical assets and systems from threats, both physical and cyber. The basic principles of critical infrastructure security management include risk identification and assessment, implementation of appropriate protection measures, threat monitoring and detection, incident response, and disaster recovery. In the context of GIS systems, managing the security of critical infrastructure requires special attention due to the complexity and importance of these systems. It is crucial to ensure the integrity, confidentiality and availability of spatial data and the continuity of GIS systems. The implementation of cybersecurity standards in GIS systems allows for effective risk management and minimization of potential threats.

Integration of cybersecurity standards with GIS Systems. Integrating cybersecurity standards into GIS systems presents a number of requirements and challenges. Key requirements include ensuring the integrity, confidentiality, and

availability of spatial data, which is essential for the effective management of critical infrastructure. This requires the implementation of appropriate technical and organizational measures, such as data encryption, access control, and threat monitoring and detection (Esri, 2014). One of the main challenges is the complexity of GIS systems, which integrate a variety of data sources and technologies. The implementation of cybersecurity standards in such systems requires close cooperation between cybersecurity specialists and GIS users (Biesecker et al., 2018). An additional challenge is the dynamically changing environment of cyber threats, which requires continuous improvement and updating of the applied protection measures (Admin, 2024; Vasdev, 2020).

Examples of cybersecurity standards implementation in GIS systems can be found in various sectors of critical infrastructure. For example, in the energy sector, GIS systems are used to monitor and manage power grids. The implementation of cybersecurity standards, such as the NIST Cybersecurity Framework, allows these systems to be protected from cyberattacks while ensuring continuity of energy supply. In the transportation sector, GIS systems are used to manage road and rail infrastructure. Implementing ISO/IEC 27001 standards in these systems makes it possible to secure traffic and infrastructure data, which is crucial to ensure the safety and efficiency of transport operations.

A case study of cybersecurity standards in GIS provides valuable information on best practices and challenges related to this process. An example is the case study of the implementation of cybersecurity standards in a GIS system managing a water supply network in a large city. As part of this project, data encryption, access control and threat monitoring were used, which allowed for effective protection of the system against cyber attacks (Esri, 2014). Another example is the case study of the implementation of cybersecurity standards in the GIS system used to manage telecommunications infrastructure. In this case, it was crucial to ensure the continuity of the system's operation and to protect data from unauthorized access. The implementation of the NIST Cybersecurity Framework standards has made it possible to achieve these goals by minimizing the risk associated with cyber threats (Biesecker et al., 2018; Vasdev, 2020).

Critical Infrastructure Security Management. Geographic Information Systems (GIS) play a key role in the management of critical infrastructure, enabling the monitoring, analysis, and visualization of spatial data. GIS allows for the integration of various data sources, which enables better understanding and management of infrastructure resources (Singh, 2024; U.S. Government Accountability Office, 2023). In the context of critical infrastructure management, GIS is used to map risk areas, assess the vulnerability of infrastructure, and plan preventive actions and incident response (Admin, 2024). With the power of spatial analysis, GIS systems support decision-making and coordination of actions in crisis situations (Saadat Barikani, 2024).

Implementing effective security practices and procedures is crucial to protecting critical infrastructure from cyber threats. Core practices include identifying and inventorying key IT and OT assets, developing a security culture, managing supply chain risk, designing resilient networks, and effectively managing access (U.S. Department of

Homeland Security, 2020). Security procedures should include regular updates and vulnerability management, implementation of physical protection measures, and preparedness for emergencies (Office of the Director of National Intelligence, 2023), (Dawson et al., 2021). In the context of GIS systems, special attention should be paid to the protection of spatial data and ensuring the continuity of system operations (Office of the Auditor General, 2023).

Risk assessment and incident management are key components of critical infrastructure security management. The risk assessment process includes threat identification, vulnerability analysis, and assessment of the potential consequences of incidents (Barrett, 2018). In the context of GIS systems, risk assessment should take into account the specific risks associated with spatial data and critical infrastructure. Incident management includes threat monitoring and detection, incident response, and disaster recovery processes. Effective incident management requires collaboration between different actors and the implementation of appropriate procedures and tools to respond quickly to threats.

Methodology

This study uses a variety of data collection methods to get a comprehensive picture of the integration of national cybersecurity standards into GIS systems. First of all, a literature review was conducted, including books, scientific articles, domain journals and research reports. In addition, empirical data was collected through interviews with cybersecurity experts and GIS users. These interviews were aimed at identifying the main challenges and best practices related to the implementation of cybersecurity standards. In addition, a thematic method was used to analyse specific examples of the integration of cybersecurity standards in different sectors of critical infrastructure.

The analysis of the data collected in the study included both qualitative and quantitative analysis. Qualitative analysis consisted of categorisation of data obtained from interviews and literature review, which allowed the identification of main themes and patterns. As part of the quantitative analysis, a statistical analysis of the data collected in the case studies was carried out to assess the effectiveness of the implementation of cybersecurity standards in GIS systems. This analysis also included risk assessment and incident management in the context of GIS systems. The study used a variety of research tools to support the process of data collection and analysis. Semi-structured questionnaires were used to conduct the interviews, which made it possible to obtain detailed information about the respondents' experiences and opinions.

Results and discussion

Research results. The results of the research indicate the effectiveness of integrating national cybersecurity standards with GIS systems in the protection of critical infrastructure. The case studies showed that the implementation of standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework contributed to a significant reduction in the risk of cyber threats and improved business continuity of GIS systems.

In the energy sector, the implementation of cybersecurity standards in GIS systems has enabled better monitoring and management of power grids. For example, the use of data encryption and advanced access control mechanisms allowed critical information to be protected from unauthorized access. As a result, GIS systems have become more resilient to cyberattacks, which has contributed to increased reliability of energy supply.

In the transportation sector, the implementation of ISO/IEC 27001 standards in GIS systems used to manage road and rail infrastructure has made it possible to secure traffic and infrastructure data. This enabled more effective traffic management and rapid incident response, which contributed to improved safety and efficiency of transport operations.

Interviews with cybersecurity experts and GIS users confirmed that the implementation of standards such as the NIST Cybersecurity Framework allows for better management of spatial data security and faster response to incidents. Experts emphasized the importance of regular training and education of GIS users in the field of cybersecurity, which allows to increase awareness of threats and more effective implementation of protection measures.

The results of the research indicate that risk assessment and incident management are key elements of effective integration of cybersecurity standards with GIS systems. The risk analyses carried out allowed for the identification of the main threats and vulnerabilities of GIS systems, which enabled the implementation of appropriate protection measures. As part of incident management, the use of advanced monitoring and threat detection tools allowed for quick response to incidents and minimization of their effects.

Taken together, the results of the study confirm that the integration of national cybersecurity standards with GIS systems contributes to a significant increase in the level of security of critical infrastructure. The implementation of standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework allows for effective risk management and ensuring the continuity of GIS systems. Cybersecurity education and training of GIS users is also crucial to increase awareness of threats and implement protection measures more effectively.

Discussion of the results. The discussion on the results of the research indicates several key aspects that are important for the integration of national cybersecurity standards with GIS systems.

First, the research highlights the importance of close collaboration between cybersecurity professionals and GIS users. Implementing effective technical and organizational protection measures requires an understanding of the specifics of GIS systems and the risks to which they are exposed. This cooperation allows for better adaptation of cybersecurity standards to the unique requirements of GIS systems, which increases the effectiveness of the implemented protection measures.

Secondly, the dynamically changing environment of cyber threats requires continuous improvement and updating of the protection measures used. Research results indicate that standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework are effective in minimizing risk, but their implementation must be regularly updated in

response to new threats. As a result, organizations must invest in the continuous improvement of their security systems and monitoring the latest trends and threats in the area of cybersecurity.

The results also highlight the importance of education and training for GIS users in cybersecurity. Increasing awareness of threats and knowledge of best practices in the field of spatial data protection is crucial for the effective implementation of cybersecurity standards. Training should cover both technical and organizational aspects so that GIS users are fully prepared to respond to incidents and minimize risk.

The discussion on the results of the research points to practical implications for organizations managing critical infrastructure. The implementation of cybersecurity standards in GIS systems allows for better risk management and ensuring the continuity of key services. Organizations should strive to integrate standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework into existing GIS systems to create a consistent and effective approach to cyber threat protection.

It is also worth noting the limitations of the research. The conducted case studies and interviews provide valuable information on the integration of cybersecurity standards with GIS systems, however, these studies are limited to selected sectors of critical infrastructure. Further empirical research is needed to better understand the challenges and best practices in different contexts and sectors.

Overall, the discussion of the research findings highlights the critical importance of collaboration between cybersecurity professionals and GIS users, continuous improvement of security measures, education and training, and practical implications for organizations managing critical infrastructure. The results of the research confirm the effectiveness of integrating cybersecurity standards with GIS systems, but further research is needed to fully understand this process.

Comparison with literature. A comparison of the results of the research with the literature indicates consistency with previous research on the integration of cybersecurity standards with GIS systems. The literature emphasizes the importance of standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework in the protection of critical infrastructure.

The Geospatial Approach to Cybersecurity, published by Esri, describes the implementation of ArcGIS to ensure the cybersecurity of infrastructure and operations. The authors emphasize the importance of the geographical layer in the context of cyber operations and present a geospatial model for perimeter defense (Esri, 2015). The results of the research confirm that the integration of cybersecurity standards with GIS systems, as described in this book, contributes to increasing the level of security of spatial data and the continuity of system operations.

In the article "Applications of GIS to Cybersecurity", authors Brian Biesecker and Ken Mitchell examine how GIS systems can help solve fundamental cybersecurity problems, such as the impact of cyberattacks on critical systems and infrastructure (Biesecker et al., 2018; Biesecker & Mitchell, 2018). This article also provides examples of how cybersecurity tools are integrated with the ArcGIS platform. The results of the research confirm that the implementation of cybersecurity standards in GIS systems allows for

better risk management and faster response to incidents, which is in line with the conclusions of the authors of the article.

The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations, published by Esri, provides practical guidance on how to implement cybersecurity standards in GIS (Esri, 2014). This report emphasizes the importance of prioritizing cybersecurity activities in the context of strategic business activities and presents a geospatial model for assessing the impact of missions. The results confirm that the implementation of standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework in GIS systems contributes to effective risk management and ensuring the continuity of system operations, which is consistent with the findings of the report.

Overall, a comparison of the research results with the literature indicates consistency with previous research on the integration of cybersecurity standards into GIS systems. The results of the research confirm that the implementation of standards such as ISO/IEC 27001 and NIST Cybersecurity Framework in GIS systems contributes to the improvement of spatial data security and business continuity of systems. The literature review also points to the need for further empirical research to better understand the challenges and best practices associated with integrating cybersecurity standards into GIS systems.

Conclusion

The research conducted as part of this article confirms the effectiveness of integrating national cybersecurity standards with GIS systems in the protection of critical infrastructure. Case studies and interviews with cybersecurity experts and GIS users have shown that the implementation of standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework contributes to significantly reducing the risk of cyber threats and improving the business continuity of GIS systems. The results also highlight the importance of education and training for GIS users in cybersecurity. Based on the research carried out, several practical conclusions can be drawn: Effective integration of cybersecurity standards into GIS systems requires close cooperation between cybersecurity professionals and GIS users. This cooperation allows for better adaptation of standards to the specific requirements of GIS systems. The dynamically changing environment of cyber threats requires regular updating and improvement of the applied protection measures. Organizations should invest in monitoring the latest trends and threats and in continuously improving their security systems. Increasing awareness of threats and knowledge of best practices in the field of spatial data protection is crucial for the effective implementation of cybersecurity standards. Training should cover both technical and organizational aspects. Effective risk assessment and incident management are key elements of critical infrastructure protection. Organizations should implement advanced threat monitoring and detection tools and rapid incident response procedures. The results of the research point to several areas that require further research: Further empirical research is needed to better understand the challenges and best practices

associated with the integration of cybersecurity standards into GIS systems in various critical infrastructure sectors. Research should focus on analysing emerging cyber threats and developing effective measures to protect against them. Further research should include the development of new tools and technologies to support the integration of cybersecurity standards into GIS systems, including advanced monitoring and threat detection tools. Research should also focus on developing effective education and training programs for GIS users in cybersecurity.

Acknowledgements

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

References

Admin (2024). The Role of GIS in Modern Infrastructure and Defense Planning. Planning Tank. https://planningtank.com/geographic-information-system/role-gis-modern-infrastructure-and-defense-planning [access: 01.03.2025].

Barrett M. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. NIST Cybersecurity Framework. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [access: 01.03.2025].

Biesecker B., Geraci P., Cherry S. (2018). GIS Applications to Cybersecurity and Critical Infrastructure Protection. Esri. https://proceedings.esri.com/library/userconf/fed18/papers/fed-095.pdf [access: 01.03.2025].

Biesecker B., Mitchell K. (2018). Applications of GIS to Cybersecurity. Esri. https://proceedings.esri.com/library/userconf/fed18/papers/fed-011.pdf [access: 01.03.2025].

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: 01.03.2025].

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 [accessed: 01.03.2025].

Esri (2023). Physical Security Management. System Integration with GIS. https://www.esri.com/en-us/industries/security-operations/strategies/physical-security [access: 01.03.2025].

European Parliament and Council (2024). Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng [access: 01.03.2025].

International Chamber of Commerce (2024). Protecting the Cybersecurity of Critical Infrastructures and Their Supply Chains. https://iccwbo.org/wp-content/uploads/sites/3/2024/07/ICC-2024_Protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains.pdf [access: 07.02.2025].

Office of the Auditor General (2023). Security Basics for Protecting Critical Infrastructure from Cyber Threats. https://audit.wa.gov.au/reports-and-publications/reports/security-basics-for-protecting-critical-infrastructure-from-cyber-threats/ [access: 01.03.2025].

Office of the Director of National Intelligence (2023). Safeguarding Our Critical Infrastructure. https://www.dni.gov/index.php/ncsc-features/2762-safeguarding-our-future [access: 01.03.2025].

Dawson M., Bacius R., Gouveia L.B., Vassilakos A. (2021). Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors. https://www.researchgate.net/publication/349969874_Understanding_the_Challenge_of_Cybersecurity_in_Critical_Infrastructure_Sectors/fulltext/604a196f299bf1f5d83dbd26/Understanding-the-Challenge-of-Cybersecurity-in-Critical-Infrastructure-Sectors.pdf.

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/.

Singh R. (2024). The role of geographic information systems (GIS) in disaster management and planning. International Journal of Geography, Geology and Environment, vol. 6, no. 2, pp. 195–205.

U.S. Department of Homeland Security. (2020). Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach. CISA. https://www.cisa.gov/resources-tools/resources/executing-critical-infrastructure-risk-management-approach . [access: 05.02.2025].

U.S. Government Accountability Office. (2023). Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods. https://www.gao.gov/products/gao-23-105468. [access: 22.02.2025].

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.