

SMART CITY MANAGEMENT AND CYBERSECURITY – CHALLENGES AND DIRECTIONS FOR DEVELOPMENT

Anna PADLOWSKA

Czestochowa University of Technology, Faculty of Management; anna.padlowska@pcz.pl,
ORCID: 0000-0002-2631-1371

Purpose: This article addresses the key issue of smart city development in Polish cities. The aim of the article is to identify the main challenges related to digital security in the context of smart city management and to identify directions for further development in this area. The analysis was conducted under the assumption that the development of smart cities is based on the intensive use of digital technologies, the functioning of which depends on an adequate level of digital security. It was also assumed that cybersecurity is one of the key factors determining the efficiency, reliability, and sustainable development of smart cities, and that ensuring it requires a comprehensive approach encompassing technological, organizational, legal, and social aspects. The growing dependence on digital infrastructure generates new threats to urban security.

Design/methodology/approach: The aim of this work was achieved through theoretical and practical analysis. The article identifies challenges and directions for development in the field of digital security in smart city management. The results presented in the paper demonstrate the threats present in Polish smart cities.

Findings: The research results enabled the identification of key directions of technological development and the level of digital security in cities. Improving the quality of life of their residents depends on modern technological and IT solutions that support urban systems. Theoretical and research analysis identified challenges and directions of development in the field of digital security in smart cities.

Research limitations/implications: The topic of this article is an important and timely research issue. The topic is particularly relevant given the increase in cyberattacks in Poland in recent years. Further research and expansion of its scope are recommended. The author plans to continue her research on this topic.

Practical implications: This article presents options for implementing digital security measures that businesses and consumers consider important. The identified solutions can help determine the direction of business security development.

Social implications: The presented research and development directions allow us to understand the importance of digital security in cities. This topic influences public awareness of security in smart cities. At the same time, city residents will learn about the benefits of implementing technological solutions that will improve their lives and functioning in cities.

Originality/value: The added value of this article is the opportunity to explore digital security solutions within the smart city concept. The topic presented is timely and particularly relevant for city dwellers.

Keywords: smart city, cybersecurity, smart city management.

Category of the paper: Research paper.

1. Introduction

The growing urban, environmental, and socio - economic challenges faced by modern cities are driving the dynamic development of the smart city concept. This concept encompasses a wide range of strategies primarily aimed at improving the quality of life in the city through the integration of information and communication technologies (ICT), while also promoting citizen participation and effective governance (Smalec, 2025). The integration of advanced information and communication technologies, along with data analytics, enables more efficient management of urban infrastructure, improves the quality of life for residents, and optimizes the use of resources (Giuliodori et al., 2022; Alahi et al., 2023; DeJong, Joss, Taeihagh, 2024). At the same time, the growing reliance on digital infrastructure generates new threats in the area of security (Xia et al., 2024; Sha, Taeihagh, De Jong, 2024). There is a need to build the resilience of smart cities by focusing on local capabilities to prevent threats - natural, social, and technological (Gracias et al., 2023; Jonek-Kowalska, 2018). A key role in this process is played by the development of digital infrastructure and the implementation of sustainable development principles, which together form the foundation for more functional and crisis-resilient cities (Ancillai et al., 2023). The increasing risk of threats resulting from civilizational development is one of the fundamental problems of modern cities (Chodyński, 2019). Digital security is becoming a key element of smart city management, determining the stability of urban systems and the protection of data. The complexity of the technological environment and its vulnerability to cyberattacks make it necessary to ensure user privacy. The aim of the article is to identify the main challenges related to digital security in the context of smart city management and to indicate directions for further development in this area. The following hypothesis was formulated in the article: effective smart city management requires the implementation of a comprehensive approach to cybersecurity and risk management. This hypothesis led to the formulation of the following research questions:

- What should be the main focus of future efforts aimed at integrating cybersecurity with smart city management processes?
- What are the most significant challenges related to digital security in the management of smart cities?
- In what direction should further activities and research concerning smart city management and cybersecurity be developed?

Managing smart cities requires a multi-faceted approach to risk management and cybersecurity.

2. Digital security of cities

Cities, as population centers, are interconnected and interdependent socio-economic systems (Desroches, Taylor, 2018; Dominiak, Gawkowski, Wasielewski, 2022). In a smart city, the use of data, information, and information technologies provides residents with an efficient and effective system for delivering public, social, technical, and administrative services (Braun et al., 2018). Smart city management involves using digital technologies and data analytics to effectively manage urban infrastructure, resources, and services in order to improve residents' quality of life (Ripoll González, Gale, 2023). Through the implementation of advanced technologies, the goal is to integrate and develop the distributed systems currently in use in cities (Shams et al., 2020). That is why digitalization is becoming the cornerstone of modern urban management. It enables cities to operate faster, more efficiently, more sustainably, and, above all, in a way that is better tailored to the needs of their residents. Technological solutions in cities cover various areas: from the digitization of public services, through sustainable transportation and energy efficiency, to civic engagement (Curtis, Mont, 2022). Technological changes necessitate the adoption of the highest cybersecurity standards, as this is the only way for a city to develop in a sustainable manner (Hussain et al., 2021). The key technologies supporting smart city management, such as Information and Communication Technologies (ICT) and the Internet of Things (IoT), are presented in Table 1.

Table 1.
Technologies supporting Smart Cities

Type	Application
Information and Communication Technologies (ICT)	They encompass techniques for processing, collecting, and transmitting information. They are essential in crisis management operations because they enable the representation of reality, the creation of knowledge resources, decision-making, and the coordination of initiatives.
Geographic Information System (GIS)	It is used to enter, collect, process, and visualize geographic data for the purpose of recording and visualizing changes in events, as well as analyzing statistical data and data on technical infrastructure. GIS is a key decision-making tool in urban development planning.
Internet of Things (IoT)	It enables every participant in a given process to communicate by exchanging data and information. These systems respond autonomously to events as they occur and initiate processes and actions without direct human intervention. It creates an urban sensing system that informs authorities about the current state of the city.
Internet of Services (IoS)	It uses data aggregation and integrates multiple services to support decision-making and communication. Online services streamline residents' interactions with government agencies.
Large Datasets (Big Data)	They are characterized not only by a large amount of information, but also by the diversity and speed of its processing. This refers to the rapid growth in the scale of data generated by technologies (including IoT), which require advanced analytical techniques.

Source: Own elaboration based on Sienkiewicz-Małyjurek, 2020; Drăgoicea et al., 2018; Bernardini et al., 2017; Martin et al., 2019; Jing Ran, Nedovic-Budic, 2016; Alahi et al., 2023.

In a smart city, technology is central to both infrastructure and decision-making. Rapid development is made possible by millions of sensors that collect data on various aspects of the city's operations, automated administrative procedures, strategic planning, and management based on advanced analytics (Korenik, 2017; Al-Turjman, Zahmatkesh, Shahroze 2022).

Today, there is a need to build a security system for smart cities by focusing on the ability to prevent threats, including natural, social, and technological ones (Gracias et al., 2023; Jonek-Kowalska, 2018). Resilience to threats in urban crisis management has three dimensions (Arafah, Winarso, Suroso, 2018):

- technical (e.g. resilience of critical infrastructure),
- organizational (e.g. resilience of public administration systems),
- social (resilience of citizens).

The lack of appropriate forms of digital security for increasingly advanced technological investments may hinder urban development and discourage people from investing in smart city solutions. Therefore, cybersecurity in a smart city is a key element linking social expectations with rapid development (Houichi, Jaidi, Bouhoula, 2024). Threats occurring in cities can be divided into two types, which are presented in Table 2.

Table 2.
Classification of selected threats in Smart City technology

Internal area	External area
transfer or sale of digital data to unauthorized persons or institutions	hacking attacks
sabotage	break-ins
lack of adequate control over information processing processes	false information
technical errors	hardware integrity breaches

Source: Own elaboration based on Kitchin, Dodge, 2019, p. 47.

Table 2 classifies two types of threats associated with smart city technologies. Among the internal threats, the most significant risk identified by respondents is the sharing or sale of digital data to unauthorized individuals or institutions. Among the external threats, respondents identified cyberattacks carried out by hackers as the most significant concern. Ongoing urbanization is leading to an increase in the number of people living in urban areas, which are potentially more vulnerable to cyberattacks. Consequently, smart city management cannot be considered solely in terms of efficiency and innovation but must include a comprehensive approach to digital security. The implementation of smart city solutions involves the collection and processing of vast amounts of data, often of a sensitive nature (Habib, Alsamadi, Prybutok, 2020; Ryalat, ElMoaqet, AlFaouri, 2023). In cities, the resources and systems most exposed to cyberattacks include, among others: energy networks, intelligent transport systems, monitoring and public safety systems, building management systems, and digital service platforms (Hassine et al., 2025). Traffic management, energy, public transport, and security systems are increasingly dependent on ICT networks, which makes them vulnerable to cyberattacks, system failures, and privacy breaches (Bansal, Mukherjee, Gairola, 2017). The digitalization of urban

space generates new risks, particularly in the area of digital security, which is becoming one of the key aspects of the functioning of smart cities. The spread of cyberattacks is also driven by the emergence of new types of threats resulting from the development of innovative technologies and their increasing accessibility, such as AI models.

3. Cybersecurity analysis in Poland in the years 2020-2025

Digital security in Poland is a very important element of the functioning of the state. Technological and information development requires the implementation of appropriate security procedures concerning the protection of data, IT systems, and user privacy. Therefore, in 2018, the National Cybersecurity System was established in Poland. Within this system, three national - level CSIRT teams operate at the operational level (www.gov.pl):

- 1) CSIRT GOV – the Computer Security Incident Response Team operated by the Head of the Internal Security Agency.
- 2) CSIRT MON – the Computer Security Incident Response Team operated by the Minister of National Defence.
- 3) CSIRT NASK – the Computer Security Incident Response Team operated by the Research and Academic Computer Network – National Research Institute.

In recent years, an increase in the activity of groups engaged in illegal activities in the digital world has been observed. The number of incidents recorded by CSIRTs has also increased (Figure 1).

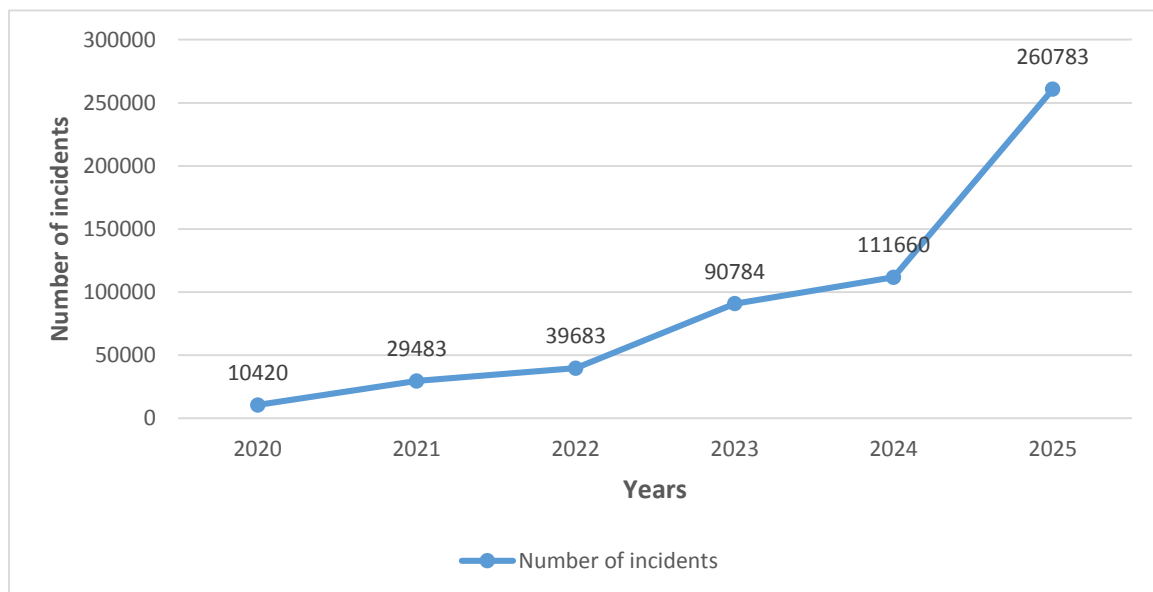


Figure 1. Statistics on cybersecurity incidents in Poland in the years 2020-2025.

Source: Data from the Annual Reports for the years 2020-2025 on the activities of CERT Polska.

The analysis of the number of cybersecurity incidents in Poland in the years 2020-2025 indicates a clear and dynamic upward trend. The data comes from the annual reports of CERT Polska teams and summaries of the national ICT security incident response system (national-level CSIRTs).

During the analyzed period, the number of cybersecurity incidents in Poland increased significantly. This trend results not only from the growing number of actual threats, but also from increasing public awareness, the development of monitoring systems, and the improvement of incident reporting procedures. This indicates the growing importance of cybersecurity as a key element of the functioning of the state and the digital economy.

Based on the data, the dynamics with the year-on-year growth rate were calculated.

$$D = \frac{W_t - W_{t-1}}{W_{t-1}} \cdot 100\% \quad (1)$$

where:

D – dynamics (percentage change),

W_t – value in the current year,

W_{t-1} – value in the previous year.

The year-on-year dynamics are presented in Table 3.

Table 3.

Year-on-year dynamics (in %)

Years	Values
2021/2020	+182,95%
2022/2021	+34,60%
2023/2022	+128,77%
2024/2023	+23,00%
2025/2024	+133,55%

Source: Own elaboration based on data from Annual Reports for the years 2020-2025 on the activities of CERT Polska.

During the analyzed period, a strong upward trend in the number of incidents is visible, characterized by irregular growth rates and sudden spikes. In 2021, there was a very sharp increase of 183%, which may indicate a sudden rise in the number of threats or an improvement in incident detection capabilities. In 2022, growth continued, but at a much slower pace, which may suggest a temporary stabilization of the situation. Another very large increase (129%) occurred in 2023, which may reflect an intensification of cyber threats or changes in reporting methods. The year 2024 showed a relatively small increase, which may indicate a period of temporary slowdown in the growth dynamics. However, in 2025, the number of incidents again increased significantly by 133%. The number of incidents is growing very dynamically, and the alternating periods of moderate growth and sudden spikes are particularly alarming. This may indicate that cyber threats are becoming increasingly serious and more difficult to control, highlighting the need to strengthen cybersecurity systems.

In research conducted by the Author in 2025, the issue of security in selected Polish cities was also examined. The author's own research was carried out in selected cities characterized by a medium and high level of advancement in the implementation of smart city initiatives. MS Excel software was used to process both primary and secondary data, applying basic descriptive statistics methods. The results were also presented graphically in the form of charts based on respondents' answers from the analyzed cities. The research was conducted from January to June 2025 using the survey method. Data collection was carried out online with the use of the Computer Assisted Web Interview (CAWI) technique. In total, 560 correctly completed questionnaires were obtained. The study involved residents of selected cities: Warsaw (85 respondents), Gdansk (79 respondents), Wroclaw (84 respondents), Poznan (80 respondents), Cracow (78 respondents), Lodz (82 respondents), and Rzeszow (72 respondents). The respondents were city residents representing various age groups, including both women and men, diversified in terms of education level and social status. The respondents assessed the level of security based on such elements as: the effectiveness of urban monitoring systems, the protection of digital infrastructure, citizen involvement, and the actions and responses of the relevant services. The following responses were obtained (Figure 2).

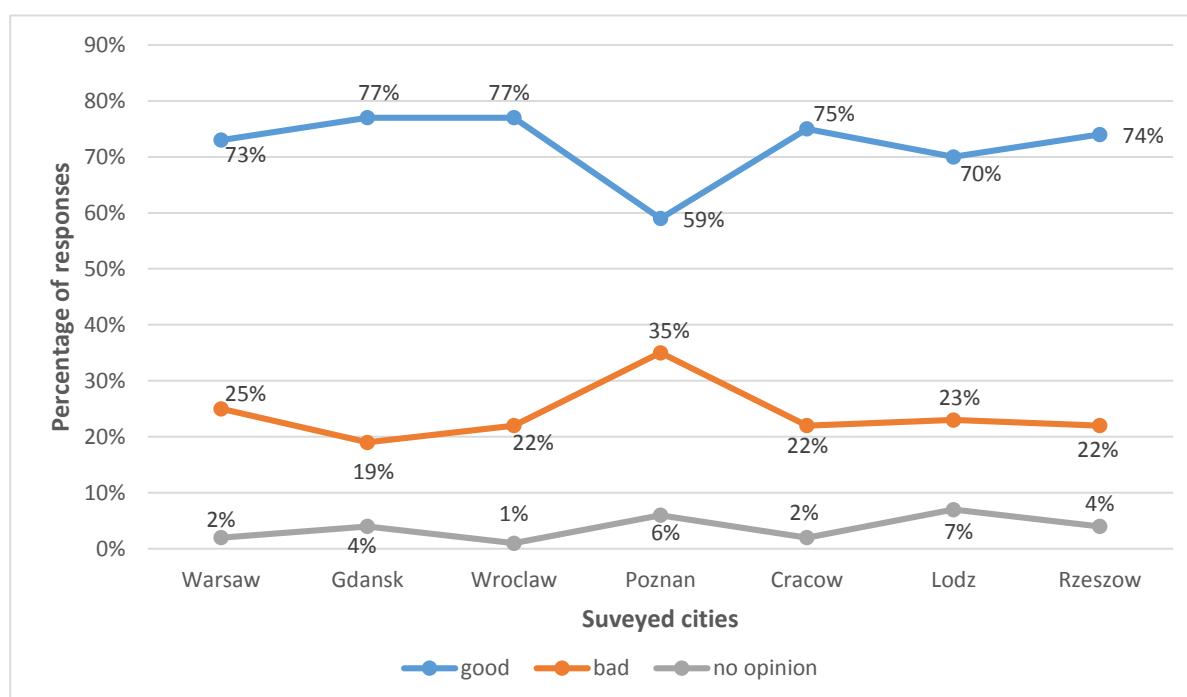


Figure 2. Structure of respondents' responses by city of residence.

Source: Own elaboration based on the survey, n = 560.

The level of safety in the surveyed cities was assessed by respondents as high at approximately 70%, which represents a positive aspect of Smart City functioning. The indicated responses are the subjective opinions of residents of selected cities, but they indicate that appropriate standards are being maintained and that the city demonstrates care for safety in the process of implementing innovative technological solutions.

Raising the level of a city's technological and information development is achieved through the implementation of modern digital technologies, data analysis and processing systems, and intelligent management tools that improve the city's functioning and enhance the quality of life of its residents (Table 4).

Table 4.

Percentage distribution of respondents indicating a high level of responses

City	Level of implementation of Smart City systems	Level of technological and information development in the city
Warsaw	76%	80%
Gdansk	77%	82%
Wroclaw	76%	70%
Poznan	74%	49%
Cracow	77%	53%
Lodz	74%	54%
Rzeszow	79%	57%

Source: Own elaboration based on the survey, n = 560.

Based on the presented data, it can be concluded that a high level of both the use of smart city systems and technological and information development is perceived by respondents across all analyzed cities. The highest values in terms of the use of smart city systems were recorded in Rzeszow (79%), as well as in Gdansk and Cracow (77% each). The remaining cities also show values above 70%, indicating a relatively uniform level of implementation of modern technological solutions in the surveyed cities. In the case of the level of technological and information development, the highest values were recorded in Gdansk (82%) and Warsaw (80%), which indicates a particularly advanced level of digitalization in these cities. Wroclaw achieved 70%, while Rzeszow 57%, Lodz 54%, Cracow 53%, and the lowest result was recorded in Poznan at 49%. This indicates a clearer differentiation between cities in this area compared to the mere use of smart systems.

The comparison of results indicates that city residents positively assess the implementation of modern technologies in urban space as well as the level of digital security. Smart systems and technological and information development are perceived as factors that improve the functioning of the city and contribute to enhancing the quality of life of its residents.

4. Challenges and directions for development

Modern cities should be resident-friendly and responsive to their changing needs. City authorities face significant challenges when seeking to advance technological progress and implement innovative solutions that support urban policies and strategies while remaining beneficial to residents. Digitalization requires a strategic approach rather than merely introducing isolated technologies. It is important to appropriately select available solutions based on existing needs and the resources of the city.

The challenges faced by city authorities are numerous, primarily including a low level of digital maturity in cities, budget constraints, and the need to invest in complex security infrastructure. It is also necessary to mention the insufficient number of specialists in this field, as well as the lack of digital competencies and awareness among residents. Cities also experience difficulties in implementing coherent security standards and face risks associated with the rapid pace of technological development. The implementation of new technologies requires the integration of multiple urban systems. Investments in digital technologies must be properly secured against system vulnerability to cyberattacks. A very important aspect of digitalization concerns legal challenges related to data protection and privacy. Cities must strive to enhance the competencies of public officials and increase citizens' awareness of digital security.

Due to digitalization across all areas of socio-economic functioning, an increase in cyber threats is expected in the future. Possible risks include attacks by foreign states on critical infrastructure, distribution of malicious software to companies and citizens, and an increase in the use of social engineering in fraud schemes targeting individuals. There may also be a rise in campaigns in which criminals use artificial intelligence to generate fake voices and likenesses.

The directions for the development of cities in terms of building resilient and secure urban systems should take into account technological, organizational, and legal aspects. In this context, the need to create integrated security strategies becomes particularly important, as they form the foundation of sustainable and responsible smart city development. Another key development direction is the control and certification of IoT devices, as well as the use of artificial intelligence to detect threats. No changes will be sustainable if residents and city officials are not properly trained and educated about modern forms of cyber threats. Cybersecurity is becoming an essential element of smart city operations, as without adequate resources, the losses resulting from potential breaches may be significantly greater than the benefits of developing a smart city.

5. Summary

In summary, the presented theoretical and practical analyses concerning smart city management and digital security demonstrate that these two areas are closely interconnected. The development of smart cities is associated with the growing importance of protecting digital infrastructure and data. The high level of integration and complexity of technological systems, as well as their significance for the functioning of key urban services, means that digital security is no longer merely an operational support function, but has become a strategic element of management. This encourages the author to conduct further research on the presented topic in

the future. The results of the study enabled the positive verification of the research hypothesis, confirming the validity of the adopted assumptions in light of the collected empirical data and the findings of the analysis. The objective of the article has been achieved through the conducted analyses, which identified the challenges faced by contemporary society regarding digital security. Furthermore, directions for the development of smart city management were indicated in the technological dimension, taking into account cybersecurity aspects. One of the main conclusions is the necessity of implementing a holistic approach to security, covering technological, organizational, and legal aspects. The development of cybersecurity competencies among both specialists and users of urban systems is also of key importance. Digital education, awareness campaigns, and building citizens' awareness are crucial elements in reducing risk and increasing resilience to threats in the digital world. In the context of further development, it is necessary to strengthen cross - sector cooperation, including public - private partnerships, as well as to develop standards and legal regulations adapted to the specific nature of smart cities. It is recommended to conduct research on the use of modern technologies, such as artificial intelligence, to enhance the ability to detect and counter threats. Ensuring digital security is a necessary condition for the sustainable and effective development of smart cities, and its proper consideration in management processes determines the durability and reliability of modern urban functioning. Future efforts should focus on the further integration of cybersecurity issues into the strategic management processes of smart cities. Particular importance should be placed on the development of real-time threat monitoring systems that, through advanced data analytics, support solutions based on artificial intelligence. In the future, it will also be essential to enhance the interoperability of urban systems while maintaining high standards of data protection and residents' privacy. Another important direction is strengthening cities' resilience to cyber incidents through regular security testing, crisis response exercises, and the establishment of municipal security operations centers. Further research should examine the impact of emerging technologies, such as the Internet of Things (IoT), 5G/6G networks, cloud technologies, and Digital Twins, on the level of security and the effectiveness of smart city management. The implementation of these measures may contribute to increasing the resilience of urban infrastructure, improving the quality of public services, and enhancing public trust in digital solutions deployed within urban environments. Future initiatives should therefore concentrate on the close integration of cybersecurity with smart city management processes through the implementation of comprehensive data protection strategies, the development of digital competencies, and the creation of resilient and secure ICT systems. The key challenges remain the growing number of cyber threats, the increasing complexity of smart city infrastructure, and the need to maintain a balance between innovation, residents' privacy protection, and the continuity of public services.

References

1. Alahi, M.E.E., Sukkuea, A., Tina, F.W., Nag, A., Kurdthongmee, W., Suwannarat, K., Mukhopadhyay, S.C. (2023). Integration of IoT enabled technologies and artificial intelligence (AI) for smart city scenario: Recent advancements and future trends. *Sensors*, 23.
2. Al-Turjman, F., Zahmatkesh, H., Shahroze, R. (2022). An overview of security and privacy in smart cities IoT communications. *Transactions on Emerging Telecommunications Technologies*, 33(3).
3. Ancillai, C., Sabatini, A., Gatti, M., Perna, A. (2023). Digital technology and business model innovation: A systematic literature review and future research agenda. *Technological Forecasting and Social Change*, 188.
4. Bansal, N., Mukherjee, M., Gairola, A. (2017). Smart cities and disaster resilience. In: F. Seta, J. Sen, A. Biswas, A. Khare (Eds.), *From poverty, inequality to smart city* (pp. 109-122). Springer.
5. Bernardini, G., Santarelli, S., Quagliarini, E., D'Orazio, M. (2017). Dynamic guidance tool for a safer earthquake pedestrian evacuation in urban systems. *Computers, Environment and Urban Systems*, Vol.65, pp. 150-161.
6. Braun, T., Fung, B.C.M., Iqbal, F., Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society*, 39, pp. 499-507.
7. Chodyński, A. (2019). Wykorzystanie dorobku nauk o zarządzaniu na rzecz podnoszenia bezpieczeństwa miast. Koncepcja smart. *Bezpieczeństwo. Teoria i Praktyka*, 4, pp. 39-62.
8. Curtis, S.K., Mont, O. (2022). Sharing economy business models for sustainability. *Journal of Cleaner Production*, 266.
9. Debnath, A., Sarkar, B. (2023). Effect of circular economy for waste nullification under a sustainable supply chain management. *Journal of Cleaner Production*, 385.
10. DeJong, M., Joss, S., Taeihagh, A. (2024). Smart cities as spatial manifestations of 21st century capitalism. *Technological Forecasting and Social Change*, 202.
11. Desroches, R., Taylor, J.E. (2018). The promise of smart and resilient cities. *Bridge*, 48(2), pp. 13-20.
12. Dominiak, B., Gawkowski, K., Wasielewski, Z. (2022). *Cyfrowe miasto – bezpieczna czy niebezpieczna przyszłość?* Warszawa.
13. Drăgoicea, M., Badr, N.G., Falcão e Cunha, J., Oltean, V.E. (2018). From data to service intelligence: Exploring public safety as a service. In: G. Satzger, L. Patrício, M. Zaki, N. Kühl, P. Hottum (Eds.), *Exploring service science* (pp. 344-357). Springer.
14. Giuliadori, A., Berrone, P., Ricart, J.E. (2022). Where smart meets sustainability: The role of smart governance in achieving the Sustainable Development Goals in cities. *BRQ Business Research Quarterly*, 26(1).

15. Gracias, J.S., Parnell, G.S., Specking, E., Pohl, E.A., Buchanan, R. (2023). Smart cities - A structured literature review. *Smart Cities*, 6(4).
16. Habib, A., Alsamadi, D., Prybutok, V. (2020). Factors that determine residents' acceptance of smart city technologies. *Behaviour and Information Technology, Taylor & Francis Journal*, vol.39(6), pp. 610-623.
17. Hassine, L., Quadar, N., Ledmaoui, Y., Chaibi, H., Saadane, R., Chehri, A., Jakimi, A. (2025). Enhancing smart grid security in smart cities: A review of traditional approaches and emerging technologies. *Applied Energy*, Vol. 398.
18. Houichi, H., Jaidi, F., Bouhoula, A. (2024). Cyber security within smart cities: A comprehensive study and a novel intrusion detection-based approach. *Computers, Materials and Continua*, 81(1), pp. 393-441.
19. Hussain, B., Haseeb, H.I., Kamarudin, M., Dacko-Pikiewicz, Z., Szczepańska-Woszczyna, K. (2021). The role of globalization, economic growth and natural resources on the ecological footprint in Thailand: Evidence from nonlinear causal estimations. *Processes*, 9(7), Article 1103.
20. Jing Ran, Nedovic-Budic, Z. (2016). Integrating spatial planning and flood risk management: A new conceptual framework for the spatially integrated policy infrastructure. *Computers, Environment and Urban Systems*, 57, pp. 68-79.
21. Jonek-Kowalska, I. (2018). Kondycja finansowa jednostek samorządu terytorialnego jako determinanta rozwoju inteligentnych miast w Polsce. *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie*, z. 120, pp. 131-140.
22. Kitchin, R., Dodge, M. (2019). The (In) security of smart cities: Vulnerabilities, risks, mitigation and prevention. *Journal of Urban Technology*, 26(2), pp. 1-19.
23. Korenik, A. (2017). Smart city jako forma rozwoju miasta zrównoważonego i fundament zdrowych finansów miejskich. *Ekonomiczne Problemy Usług*, 4, pp. 170-180.
24. Martin, C., Evans, J., Karvonen, A., Paskaleva, K., Yang, D., Linjordet, T. (2019). Smart-sustainability: A new urban fix? *Sustainable Cities and Society*, 45, pp. 640-648.
25. Ripoll González, L., Gale, F. (2023). Sustainability as economic value pluralism: Implications for urban politics and policy. *Cities*, vol.134, Article 104167.
26. Ryalat, M., ElMoaqet, H., AlFaouri, M. (2023). Design of a smart factory based on cyber-physical systems and Internet of Things towards Industry 4.0. *Applied Sciences*, 13(4).
27. Sha, K., Taeihagh, A., De Jong, M. (2024). Governing disruptive technologies for inclusive development in cities: A systematic literature review. *Technological Forecasting and Social Change*, 203.
28. Shams, G., Rehman, M.A., Samad, S., Oikarinen, E. (2020). Exploring customer's mobile banking experiences and expectations among generations X, Y and Z. *Journal of Financial Services Marketing*, vol.25(1), pp. 1-13.
29. Sienkiewicz-Małyjurek, K. (2020). Smart city w budowaniu odporności miast na zagrożenia. *Bezpieczeństwo. Teoria i Praktyka*, 4, pp. 82-95.

30. Smalec, A. (2025). Smart Cities, Smart Governance: The Role of Communication and Social Participation in Building Cities of the Future. *Scientific Papers of Silesian University of Technology. Organization and Management Series No. 227*, pp. 355-365.
31. Sprawozdanie_Pełnomocnika_Rządu_ds_Cyberbezpieczeństwa.pdf
32. www.gov.pl
33. Xia, S., Song, J., Ameen, N., Vrontis, D., Yan, J., Chen, F. (2024). What changes and opportunities does big data analytics capability bring to strategic alliance research? A systematic literature review. *International Journal of Management Reviews*, 26.