Communal Level Cybersecurity Incidents in the Slovak Republic

Miroslav Fečko, Ondrej Mital(✉), and Silvia Ručinská

Department of Public Policy and Theory of Public Administration, Faculty of Public Administration, Pavol Jozef Šafárik University in Košice, 04011 Košice, Slovak Republic
{miroslav.fecko,ondrej.mital,silvia.rucinska}@upjs.sk

Abstract. The study investigates issues surrounding cybersecurity, one of the crucial topics connected with digital transformation of society. Municipalities and cities help to shape digital transformation at local level, mainly thanks to growing use of digital solutions. This tendency also leads to higher vulnerability of municipalities and cities. The study uses a literature review and multiple case study method to examine the relevance of bottom-up approach of municipalities and cities in building cybersecurity and responding to cyberattacks. Regarding the conditions of the Slovak Republic and increasing occurrence of cyberattacks targeting municipalities and cities, 5 cases of cyberattacks were analysed, focusing on mainly on type of the attacks and caused impact. The main benefit of the study is contribution to existing empirical findings that confirm the importance of bottom-up approaches in cybersecurity agenda at local level. Municipalities and cities have become relevant actors that utilize outcomes of digital transformation on local communities, but also important actors that can formulate locally specific cybersecurity policies and face cyberattacks.

Keywords: Cybersecurity · cyberattacks · cyberincidents · municipalities and cities · bottom-up approaches · local public policies · Slovak Republic

1 Introduction

The digital transformation of society increases the use of digital technologies and new innovative solutions in almost every aspect of social life. This trend is notably identified at various levels of governance, including municipalities and cities nearest to the citizens. The implementation of new technologies facilitates the rationalisation of competencies´ execution and the provision of public services, leading to an improvement in the quality of life among local communities. This shift not only optimises the execution of competencies but also improves the responsiveness of local governments to the needs and preferences of their communities, ensuring more effective service delivery [26, 73].

At the same time, public sector organisations that use digital technologies daily are becoming more vulnerable. Cyberattacks are increasingly targeting cities and municipalities, which often have very limited resources for cybersecurity, thus, cyberattacks pose active threats to the security of public life and citizens at the local level [20, 46, 64]. The

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2026
O. Gervasi et al. (Eds.): ICCSA 2025 Workshops, LNCS 15889, pp. 39–53, 2026.
https://doi.org/10.1007/978-3-031-97603-2_3

increase in cyberattacks has led to a stronger focus on the importance of cybersecurity at all levels of governance, including municipalities and cities.

This study aims to realize preliminary research on the bottom-up responses of local governments in the face of cyberattacks. Using a multiple case study methodology, the study examines examples of cyberattacks on municipalities and cities within the Slovak Republic from 2018 to 2025. The selection of case studies on municipalities and cities helped us to identify important patterns and demonstrate the variety of cyberattacks suffered.

2 Local Government and Cybersecurity – Understanding and Challenges

2.1 Importance of Cities and Municipalities in Contemporary Democracies

Local government's current role and importance reflect decentralisation tendencies in a democratic state governed by the rule of law [62, 78]. Municipalities and cities have a natural tendency to face modern trends and challenges, thanks to which they can enrich their own functioning but mainly improve the provision of services to citizens and entrepreneurs living and residing in the given territory [71].

Many municipalities and cities, therefore, develop individual governance approaches and policies as they try to respond to different challenges and meet local stakeholders' needs [7, 81]. Local level of government is directly involved in exploring what can be achieved together with other local stakeholders, what problems can be solved, and how [8, 17]. Municipalities and cities concentrate their power and resources on providing various types of public services, mainly to increase the quality of life in a particular territory.

Municipalities and cities can be perceived as actors with a natural tendency to face modern trends and challenges, thanks to which they can enrich their functioning and execution of original and transferred competencies, but mainly improve the provision of public goods and quality of life. As irreplaceable actor in the policy process, municipalities and cities can participate in national public policies and create their own specific local public policies. Sometimes, the voice of the lowest level of public administration is the only one that can affect the outcome of higher levels of public policies in current states. Put differently, central governments are often unable to register and solve all public issues at the municipal level of governance. In other cases, municipalities and cities must react quickly because central governments need time to formulate and implement local public policy. This tendency is also underlined by the fact that municipalities and cities represent the level of governance, which can be considered as the nearest to citizens´ everyday life needs [66, 70].

2.2 Municipalities and Cities in the Centre of Digital Transition

Municipalities and cities play a central role in their rapid and sustainable development, which helps them address a wide range of contemporary challenges [25]. Cities face more significant pollution, more traffic congestion, and higher demand for energy and

sanitation services due to urban growth, thus, to resolve the problems associated with urbanisation, the cities should incorporate smart solutions [2, 75]. From the practical point of view, the important role of municipalities and cities as policy actors are irreplaceable, as was proven many times in various local public issues, such as sustainable development [9, 50], health and wellbeing [55, 68], climate change adaptation and mitigation [11, 16], as well as digital transformation [31, 57]. Mainly, digital transformation is mostly outlined as a crosscutting trend that affects many other challenges and issues in municipalities and cities [26, 35].

The complexity of managing life in municipalities and cities requires new methods and smart, innovative ways to deal with urbanisation and foster more efficient, sustainable, and habitable urban areas [10, 15]. Cities use ICT and digital solutions to improve residents' living conditions, mainly through their interconnection with other aspects of the territory [4, 49].

Municipalities and cities are increasingly dependent on digital technologies that help them rationalise their roles and competencies, making them vulnerable [6, 21, 80]. Vulnerability is higher, especially in cities that aim to be digital or technological leaders [28, 38]. The rapid growth of hyperconnectivity and digitalisation in cities accelerated interest in cybersecurity issues worldwide [14, 39, 63, 65].

2.3 Cybersecurity as a Complex Agenda for Municipalities and Cities

Cybersecurity can be defined as the adoption of real-time monitoring, detection, and identification technology to protect systems, networks, and programs from potential threats, attacks, and data leakage [40]. At the local level, especially in municipalities and cities, an integrated cybersecurity framework must be seen through a holistic approach, which includes mainly a digital trust platform, cyber response and resilience, privacy by design, cyber competencies and awareness program, cyber threat intelligence and analysis platform [63].

Cybersecurity can also be explored as a strategy for organisations to protect networks, computers, programs, and data from attacks, damage, or unauthorised access [39]. Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security [30]. Summing it up, cybersecurity has emerged as a critical part of modern urban governance at the local level, as municipalities and cities should reflect their responsibilities beyond traditional physical infrastructure and in cyberspace [37].

Cybersecurity solutions are a result of the intensive use of digital transformation and cyberattacks [33, 44]. Considering the responsibility of local governments to protect their assets, cybersecurity has become among other important functions important function because governments are under constant or nearly constant cyberattacks [3, 60]. Cyberthreats are increasing and local governments are often under-resourced and underprepared for them [27]. The increasing number of researchers demonstrates that cyberattacks at the local level are ubiquitous and can happen at any time without any indication [40, 52]. The nature of cyberattacks and threats can vary, which in turn affects the character and impact of cyber incidents affecting the functioning of IT systems and

public services [5, 53]. A cyber incident occurs when a cyberattack affects the confidentiality, integrity, or availability of an IT system [18, 58]. In other words, a cyberattack is the event that leads to the declaration of a cyberincident.

Cities should deal with different types of cyberattacks that may influence the proper execution of their functions, such as device hijacking, data theft, distributed denial of services (DDoS), man-in-the-middle attacks, and permanent denial of services (PDoS) [42]. This typology of cyberattacks can be widened, and based on the CyberPeace Institute analysis, the public sector and public administration face various cyber incidents, mainly DDoS attacks, wiper attacks, malware attacks, hack and leak, defacement, cyber-enabled information operations, cyber espionage, and ransomware [19]. To be more concrete, cyberattacks in the public sector can include following malicious actions, botnet, email compromise, denial of service (DOD) or distributed denial of service (DDOS), hack or leak, phishing, malware, malvertising, man in the middle, ransomware, spear-phishing, supply chain attack or zero-day [43]. The European Agency for Cybersecurity defines the content of cyberattacks mainly as ransomware, malware, social engineering threats, threats against data, threats against the availability of services, threats against the availability of the internet, disinformation or misinformation, and supply chain threats [24]. The main cyberattacks which may occur at the communal level´s smart applications are denial of service, malware, eavesdropping, identity spoofing, false information, message modification, and traffic analysis [1, 54].

The local level of governance can be extremely vulnerable to cyberattacks for different reasons. The most common reasons for the vulnerability of municipalities and cities to cyberattacks include mainly, the sensitivity of data, the hundreds of different-sized entities that make it challenging to handle, budgetary and personal limits of local governance, confidential document sharing with other parts of public administration, as well as the popularity of digital solutions among the local stakeholders [37].

The rising occurrence of cyberattacks at the communal level forces cities and municipalities to reconsider cybersecurity policies and cybersecurity plans significantly [28, 34, 51, 60]. The legal norms' amendments must also reflect conceptual changes and the reflection of cyberattacks in strategies and plans [41]. Put differently, technological and legal aspects cannot be separated in planning and implementing cybersecurity measures [45]. In this regard, responses to cyberattacks should be primarily observed at the organisational level of municipalities and cities. However, cybersecurity issues can also be pushed to the level of personal behaviour to utilise the personal aspect of cybersecurity [79]. Thus, cybersecurity in municipalities and cities is also the issue of individuals´ awareness and preparedness. The cybersecurity topics discussed can be seen as essential for the future development of the field and can also be explored as standalone questions.

Growing attention is cybersecurity at the local level, gaining not only in practice but also in research. Cybersecurity issues and cyberattacks were precisely analysed in Sweden [3], United States of America [59], Poland [23, 41], Italy [14], England and Wales [13], and Ukraine [29]. In this regard, there is an urgent and significant need for deeper research on local cybersecurity in order to make cybersecurity in local government more effective and resilient [67].

3 Methodology

This study aims to realize preliminary research on the bottom-up responses of local governments in the face of cyberattacks. Using a multiple case study methodology, the study examines examples of cyberattacks on municipalities and cities within the Slovak Republic from 2018 to 2025. The research question aims to analyse whether cybersecurity can be assumed as a significant priority and policy agenda at the local level. Through this analysis, the study intends to provide valuable insights into how local governments can strengthen their cybersecurity practices and effectively tackle the challenges presented by cyber threats.

This study conducts a theoretical examination of cybersecurity issues, with particular emphasis on the impact of cyber threats and cyberattacks on municipalities and cities. Furthermore, the theoretical framework presents an analysis of the significance of local government and verifies the motivation for using a bottom-up approach to address these challenges. Through this exploration, the study aims to emphasise the essential role that municipalities and cities have in strengthening their cybersecurity practices and effectively responding to emerging digital threats.

A literature review was used to integrate findings and perspectives from empirical findings. Previous research was investigated to demonstrate the contemporary state of knowledge and relationship between bottom-up responses of local government and cybersecurity issues. Theoretical analysis was used to analyze the contemporary state of research focusing on the phenomenon of cybersecurity and cyberattacks in the conditions of cities and municipalities.

In this study, we will therefore pay attention to cyberattacks cases on municipalities and cities in the conditions of the Slovak Republic. The multiple case study method was selected. The multiple case study method helps to analyse and compare conducted data to understand the similarities and differences between the cases [32, 82]. Case studies focus the attention on a description of the subject who was the target of the cyberattack, a description of the attacker and possible motives, an analysis of the cyber incident and its impacts, a description of providing information on cyberattack to the public, and also the context of the cyberattacks and created impacts. Although the attacker's identity and the cyberattack's character are important, this study primarily focuses on the significant impact of these incidents on municipalities and cities.

The analysed case studies were selected to demonstrate similarities and differences between different types of cyberattacks. In this regard, the study does not offer a comprehensive analysis of all cyberattacks on public institutions in the Slovak Republic. The selection of case studies on municipalities and cities helped us to identify important patterns and demonstrate the variety of cyberattacks suffered. The multiple case studies method leads to stronger knowledge and lessons learned from cyberattacks.

4 Results

The following case studies analyse cyberattacks on municipalities and cities in the Slovak Republic. Each of the five case studies includes a description of the subject who was the target of the cyberattack, a description of the attacker and possible motives, an analysis of

the cyber incident and its impacts, a description of providing information on cyberattack to the public, and also the context of the cyberattacks and created impacts. The identity of the attacker and the character of the cyberattack are indeed important components of the overall analysis. However, this study primarily concentrates on the impact of such incidents on municipalities and cities. Understanding these consequences is essential for examining the responses of local governments to cyber threats.

4.1 Case 1 - Attack Motivated by a Global Event

The capital city of Slovakia, Bratislava, suffered a cyberattack on Wednesday, May 31, 2023. An unnamed hacker group claimed responsibility for the realisation of this cyberattack. The group mentioned that one of the reasons for their activity is that the city was hosting an international conference with global impact focused on global security issues, GLOBSEC, organised by a think-tank established in Bratislava.

As a consequence of the cyberattack, the services of the PAAS-regulated parking system, the services of the city's public transport company, the city's website and other city services were denied and declared inoperable [12, 22]. At the same time, the city´s management guaranteed that the datasets were not lost or endangered. Most IT systems affected by the cyberattack, as well as the city's website, were restored the next day [12]. Information about the cyberattack was published on the city's website, official social media pages, as well as regional and national media. The information provided to the public was consistently updated and made readily available, ensuring timely and relevant access to necessary insights.

Cyberattack occurred during a global event has an ambition to spread fear and uncertainty among citizens, but also participants of the conference from all over the world. In this regard, the potential intention of the attackers was to create an impression that the city´s management cannot handle this kind of global event, and also that such kind of events may lead to discomfort of citizens caused by the denial of important public services. Nevertheless, the unnamed hacker group accomplished their goal and disrupted the functioning of digital solutions adopted by the city. However, the approach of the city in this situation can be perceived as appropriate.

4.2 Case 2 - Attack on IT Systems

On October 26, 2021, the city office in the city of Malacky suffered a cyberattack. No specific entity claimed responsibility for the attack, but indications pointed to the attack being carried out from abroad [56]. In this case, the attacker and the attacker's motive for the cyberattack are unknown.

The cyberattack targeted the city's IT systems. The cyberattack caused delays in processing public complaints and proposals, and at the same time, limited and slowed down communication between the public and the city office [56, 76]. In this case, the public was informed about the cyberattack via the city's website and regional media. The information provided to the public was consistently updated and made readily available, ensuring timely and relevant access to necessary insights.

In this case, a cyberattack leads to the immediate disruption of the city´s office functioning. Even when the extent of harm from the cyberattack had not been verified at the time of the cyberattack, the city office correctly informed its citizens.

4.3 Case 3 - Attack on Critical Infrastructure

On January 24, 2025, the city of Trenčín suffered a cyberattack, targeting a part of critical infrastructure, the Trenčín Waterworks and Sewerage. While the identity of the attackers remains uncertain, the incident aimed to threaten the delivery of one of the essential public services. The attacker´s anonymity also makes it impossible to identify the motive that led to the cyberattack.

In this case, the cyberattack was successfully stopped before causing a negative impact. The Trenčín Waterworks and Sewerage organisation´s cyber protection was very well secured, so the attackers did not infiltrate the IT system, and no data was lost or compromised [69].

The city´s management informed the public of the cyber incident afterwards. The public was assured that the critical infrastructure object and its functionality were not compromised.

Analysed cyberattack on the critical infrastructure was successfully stopped thanks to the existing cyber protection framework. City´s decision not to inform immediately can be perceived as very rational, thus, the public was informed after a precise check status of waterworks and sewerage systems. Informing the public without checking the operability could cause the spread of panic and fear. In this regard, the intention of the attackers to cause the mentioned negative impacts was not achieved.

4.4 Case 4 - Stolen Public Funds

In January 2024, the municipality of Kojšov became the target of a cyberattack. This incident was targeted towards the acquisition of public funds from the municipal office bank account. The identities of the attacker and the basic motives for their actions remain unverified and cannot be objectively confirmed.

As a direct financial impact of the cyberattack, public funds of up to 10,000 € were stolen from the bank account of the municipality of Kojšov [61]. In this case, the cyberattack was proven as a phishing attack, which was confirmed by law enforcement entities and also the bank in which the municipality has its bank account [48].

Information about the cyberattack was immediately published on the city website, as well as regional and national media. Information, including the results of the investigation, was published with the use of the same communication channels.

The character of this cyberattack is in its comparison to previous ones, different in that the harm caused by the attackers cannot be restored to the original state. In this regard, attackers have achieved their goal and have received the mentioned amount of public funds.

4.5 Case 5 - Attack from the Internal Environment

The city district of Košice, particularly the Sídlisko KVP, was the target of a cyberattack in November 2019. The cyberattack was carried out by an anonymous attacker, thus, the motives of the cyberattacks also remain unknown.

The attackers caused failures of the IT systems on the server and damaged the information and data stored on the server, while the virus on the server caused partial data loss, inoperability of email communication, and data on invoices and financial statements has been compromised [47]. The attack was carried out from within the city district itself, directly in the city office building, by intentionally attacking the server [77].

Information about the attack was provided after the attack, via the website, and regional and national media. The official statement of the city district summarises all known details on the cyberattack.

This case is very specific because it is the only case where a cyberattack was realised during the physical presence of the attacker in the building of the city office. Besides, only in this case was the permanent loss of data achieved by the attackers.

5 Discussion

Municipalities and cities as actors of digital transformation must reflect cybersecurity issues and cyber threats. Due to the rise in cyberattacks in the public sector from intensive digitalisation, we would expect the central government to address this challenge.

As municipalities and cities increasingly engage in digital transformation, it is inevitable that they will become potential targets for cyberattacks. Both theory and practice have confirmed that municipalities and cities are the target of cyberattacks due to the intensive digitalisation of the execution of competencies and the provision of public services. Table 1 includes a comprehensive summarisation of analysed cases focusing on the analysed aspects of cyberattacks.

Municipalities and cities can be perceived as targets of cyberattacks, regardless of their size and territorial location. The abovementioned cases demonstrated that cyberattacks might occur in the capital city with almost 500,000 citizens, but also in a city with almost 20,000 citizens (Malacky) or less than 700 citizens (Kojšov).

Identification of attackers can be very difficult in cyberattack cases. Claiming responsibility for the attack by a specific attacker or a group of attackers is usually the only opinion that can help during this process. Such identification with cyberattacks is usually associated with the need to gain attention and grow the attackers' reputation.

In four out of five cases, the attackers focused their attention on the operability or functioning of IT systems, servers or the provision of public services. Case 3 also demonstrated that critical infrastructure at the local level is a target of cyberattacks. At the same time, Case 4 demonstrated that even a relatively small amount of finances is still attractive for attackers.

Providing information on cyberattacks to the public can be crucial when cyberattacks cause the denial of public services. In this regard, when citizens cannot get benefits from the use of common public services, they should be informed about this discomfort. As was demonstrated by Case 3, even delaying information can be acceptable in some cases.

Table 1. Comprehensive summarisation of cyberattacks

	Size of municipality/city	Attacker	Type of incident	Impact	Information of the public
Case 1 Attack motivated by a global event	478 040	hacker group	DDoS	denial of public services, website	immediate
Case 2 Attack on IT systems	18 804	anonymous (external)	DDoS	delays in communication, processing	immediate
Case 3 Attack on critical infrastructure	55 416	anonymous (external)	infiltration to IT system	none	subsequent
Case 4 Stolen public funds	698	anonymous (external)	phishing	public funds stolen	immediate
Case 5 Attack from the internal environment	21 675	anonymous (internal)	internal intentional	IT system and server, data loss	immediate

Source: authors

The issues surrounding cybersecurity, including cyber threats and cyberattacks, are relevant to all levels of public administration, encompassing municipalities and cities. The extensive range of competencies held by municipalities and cities, along with the public services they deliver, indicates that cybersecurity may present significant challenges for local self-governing entities. The main reasons for the cybersecurity issues faced by local governments are primarily their limited human resources, a lack of skilled personnel, and financial constraints that restrict their ability to create effective cybersecurity infrastructure.

Based on the presented theories and case studies, it has been demonstrated that municipalities and cities are exposed to cyber threats and cyberattacks. Consequently, despite their restrictions and limitations, they need to prioritise the cybersecurity topic as a significant part of their agenda. In this regard, creating cybersecurity systems is not mandatory, but it is necessary to devote time and resources to it. However, the capacities for creating cybersecurity systems, evaluating cyber threats and preventing cyberattacks must be allocated at the expense of other activities, especially development and innovation.

Cybersecurity cannot be perceived as the original competence of municipalities and cities mentioned in legal acts. The significant role that municipalities and cities play in the digital transformation process necessitates that they develop their own cybersecurity systems. There are no viable alternatives for these local entities in ensuring the security and integrity of their digital infrastructure.

The significant role that municipalities and cities play in the digital transformation process pushes them to develop their cybersecurity systems. There are no viable alternatives for local entities in ensuring the security and integrity of their digital infrastructure. In this regard, the intention of municipalities and cities to solve cybersecurity issues confirms the municipalities' bottom-up strategy for addressing trends, challenges, and problems that the central government does not systematically tackle.

6 Conclusion

Challenges and issues surrounding cybersecurity and cyberattacks have evolved into a crucial topic of digital transformation, including municipalities and cities. Based on previous research, building cybersecurity systems at a local level of self-government is the result of intensive digital transformation, higher vulnerability of municipalities and cities and a trend of increasing occurrence of cyberattacks.

The results revealed that cybersecurity has evolved into an important local policy agenda, because cyberattacks target not only central state administration, but also municipalities and cities. According to the analysed case studies and negative impacts of cyberattacks, cybersecurity was identified as a local policy agenda that municipalities and cities must deal with. The analysed cyber incidents highlight the urgent need to strengthen the resilience and robustness of municipalities and cities, as they increasingly face a mixture of challenges, issues, crises and situations that require effective emergency and crisis management.

The study contributes to cybersecurity discussions at all levels of government, focusing mainly on the position of municipalities and cities. The importance of research is underlined by the increasing rate of cyberattacks targeting municipalities and cities and their digital solutions, enhancing the quality of local communities´ lives. At the same time, there are still numerous unanswered questions connected to cybersecurity at the local level. Realized research can be further extended from the following perspectives, mainly broadening empirical evidence, international comparison, analysis of cyberattacks in the context of different sophistication of cybersecurity infrastructures and solutions adopted by the municipalities and cities.

Acknowledgments. The article is created as a result of a project Cybersecurity Competence Center at Pavol Jozef Šafárik University in Košice supported by the Ministry of Investments, Regional Development and Informatisation of the Slovak Republic, Grant no: 17R05–04-V01–00007.

References

1. Al-Turjman, F., Zahmatkesh, H., Shahroze, R.: An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies **33**(3), e3677 (2022). https://doi.org/10.1002/ett.3677
2. Andrade, R.O., Yoo, S.G., Tello-Oquendo, L., Ortiz-Garcés, I.: A comprehensive study of the iot cybersecurity in smart cities. IEEE Access **8**, 228922–228941 (2020). https://doi.org/10.1109/ACCESS.2020.3046442

3. Andreasson, A., Artman, H., Brynielsson, J., et al.: Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval. Cogn. Technol. Work **26**, 709–731 (2024). https://doi.org/10.1007/s10111-024-00779-1
4. Anthony Jnr, B.: A case-based reasoning recommender system for sustainable smart city development. AI & Society: Knowledge, Culture and Communication **36**, 159–183 (2021). https://doi.org/10.1007/s00146-020-00984-2
5. Australian Government.: Information security manual. https://www.cyber.gov.au/sites/default/files/2025-03/04.%20ISM%20-%20Guidelines%20for%20cybersecurity%20incidents%20%28March%202025%29.pdf. Accessed 27 April 2025
6. Baig, Z.A., Szewczyk, P., Valli, C., Rabadia, P., et al.: Future challenges for smart cities: cyber-security and digital forensics. Digit. Investig. **22**, 3–13 (2017). https://doi.org/10.1016/j.diin.2017.06.015
7. Beck, D., Ferasso, M., Storopoli, J., Vigoda-Gadot, E.: Achieving the sustainable development goals through stakeholder value creation: Building up smart sustainable cities and communities. Journal of Cleaner Production **399**, article ID 136501 (2023) https://doi.org/10.1016/j.jclepro.2023.136501
8. Bjørgen, A., Fossheim, K., Macharis, C.: How to build stakeholder participation in collaborative urban freight planning. Cities **112**, article ID 103149 (2021) https://www.sciencedirect.com/science/article/pii/S0264275121000470
9. Blasi, S., Ganzaroli, A., De Noni, I.: Smartening sustainable development in cities: Strengthening the theoretical linkage between smart cities and SDGs. Sustainable Cities and Society **80**, article ID 103793 (2022) https://doi.org/10.1016/j.scs.2022.103793
10. Braga, I.F.B., Ferreira, F.A.F., Ferreira, J.J.M., Correia, R.J.C., Pereira, L.F., Falcão, P.F.: A DEMATEL analysis of smart city determinants. Technology in Society **66**, article ID 101687 (2021) https://doi.org/10.1016/j.techsoc.2021.101687
11. Brand, C., Götschi, T., Dons, E., Gerike, R., et al.: The climate change mitigation impacts of active travel: Evidence from a longitudinal panel study in seven European cities. Global Environmental Change **67**, article ID 102224 (2021) https://doi.org/10.1016/j.gloenvcha.2021.102224
12. BratislavaDEŇ.: Bratislava is under attack by hackers, several services are out of order. https://bratislavaden.sk/bratislava-je-pod-utokmi-hackerov-viacero-sluzieb-nefunguje/. Accessed 27 Mar 2025
13. Brett, M.: An overview of current issues and practice relating to local government cyber security in England and Wales. Cyber Security: A Peer-Reviewed Journal **4**(4), 330–344 (2021)
14. Busetti, S. Scani, F.M.: Evaluating incident reporting in cybersecurity. From threat detection to policy learning. Government Information Quarterly **42**(1), article ID 102000 (2025) https://doi.org/10.1016/j.giq.2024.102000
15. Carrasco-Farré, C., Snihur, Y., Berrone, P., Ricart, J.E.: The stakeholder value proposition of digital platforms in an urban ecosystem. Research Policy **51**(4), article ID 104488 (2022) https://doi.org/10.1016/j.respol.2022.104488
16. Ceci, M., Caselli, B., Zazzi, M.: Soil de-sealing for cities' adaptation to climate change. TeMA - Journal of Land Use, Mobility and Environment **16**(1), 121–145 (2023). https://doi.org/10.6093/1970-9870/9395
17. Clement, J., Manjon, M., Crutzen, N.: Factors for collaboration amongst smart city stakeholders: A local government perspective. Government Information Quarterly **39**(4), article ID 101746 (2022) https://doi.org/10.1016/j.giq.2022.101746
18. Cremer, F., et al.: Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice **47**, 698–736 (2022). https://doi.org/10.1057/s41288-022-00266-6

19. CyberPeace Institute.: Public administration: Public administration and defence; compulsory social security. https://cyberconflicts.cyberpeaceinstitute.org/impact/sectors/public-administration. Accessed 27 Mar 2025
20. CYBERSEC.: The Rise of Cyber Resilience in European Smart Cities. https://www.cybersec-365.com/articles/the-rise-of-cyber-resilience-in-european-smart-cities. Accessed 27 Mar 2025
21. de Souza, K.E., Ferrari, F.C., de Camargo, V.V., Ribeiro, M. Offutt, J.: A systematic review of fault tolerance techniques for smart city applications. Journal of Systems and Software **219**, article ID 112249 (2025) https://doi.org/10.1016/j.jss.2024.112249
22. Dopravný podnik Bratislava.: Hacker Attack Also Cranked the DPB Website. https://www.facebook.com/DPBratislava/posts/hackerský-útok-ochromil-aj-web-dpbod-dnešného-rána-čelí-bratislava-hlavné-mesto-/630368655794810/. Accessed 27 Mar 2025
23. Dudziak-Gajowiak, D., Szleszyński, A.: Resilience of public administration bodies to cyber-attacks. Scientific Journal of the Military University of Land Forces **55**(3), 182–205 (2023). https://doi.org/10.5604/01.3001.0053.8961
24. European Union Agency for Cybersecurity.: ENISA Threat Landscape 2022. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf. Accessed 27 Mar 2025
25. Evans, J., Vácha, T., Kok, H., Watson, K.: How cities learn: from experimentation to transformation. Urban Planning **6**(1), 171–182 (2021). https://doi.org/10.17645/up.v6i1.3545
26. Fečko, M., Ručinská, S., Mitaľ. O.: Trends and challenges of the communal digital and green transition. In: Ručinská, S., Bernhart, J., Cecon, F., Dumitrescu, G.C. (eds.) Exploring digital and green concepts: Knowledge base for cities and municipalities. Wolters Kluwer: Praha, pp. 32–37 (2024)
27. Frandell, A., Feeney, M.: Cybersecurity threats in local government: a sociotechnical perspective. The American Review of Public Administration **52**(8), 558–572 (2022). https://doi.org/10.1177/02750740221125432
28. Fusi, F., Jung, H., Welch, E.: Technological vulnerability and knowledge of cyber-incidents: threats to innovativeness in local governments? Public Manag. Rev. **27**(3), 545–571 (2025). https://doi.org/10.1080/14719037.2023.2250362
29. Fyshchuk, I., Noesgaard, M.S., Nielsen, J.A.: Managing cyberattacks in wartime: the case of Ukraine. Public Administration Review, pp. 1–9. (2024) https://doi.org/10.1111/puar.13895
30. Galinec, D., Steingartner, W.: Combining cybersecurity and cyber defense to achieve cyber resilience. In: 2017 IEEE 14th International Scientific Conference on Informatics, Poprad, Slovakia, pp. 87–93 (2017). https://doi.org/10.1109/INFORMATICS.2017.8327227
31. Gasco-Hernandez, M., Nasi, G., Cucciniello, M., Hiedemann, A.M.: The role of organizational capacity to foster digital transformation in local governments: the case of three European smart cities. Urban Governance **2**(2), 236–246 (2022). https://doi.org/10.1016/j.ugj.2022.09.005
32. Gustafsson, J.: Single case studies vs. multiple case studies: a comparative study. https://hh.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf. Accessed 27 Mar 2025
33. Hamid, B., Jhanjhi, N., Humayun, M., Khan, A., Alsayat, A.: Cyber security issues and challenges for smart cities: a survey. In: 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, pp. 1–7. (2019) https://doi.org/10.1109/MACS48846.2019.9024768
34. Hatcher, W., Meares, W.L., Heslen, J.: The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. J. Cyber Policy **5**(2), 302–325 (2020). https://doi.org/10.1080/23738871.2020.1792956
35. Holzinger, A., Weippl, E., Tjoa, A.M., Kieseberg, P.: Digital transformation for sustainable development goals (SDGs) - a security, safety and privacy perspective on AI. In: Holzinger,

A., Kieseberg, P., Tjoa, A.M., Weippl, E. (eds.) Machine Learning and Knowledge Extraction, vol 12844, pp. 1–20. Springer, Cham (2021) https://doi.org/10.1007/978-3-030-84060-0_1
36. Hospodárske Noviny, Bratislava was hit by a cyberattack, the city's network was overloaded. Most systems have already been restored. https://hnonline.sk/slovensko/96086311-bratislavu-postihol-kyberneticky-utok-mestska-siet-bola-pretazena-vaecsinu-systemov-uz-obnovili. Accessed 27 Mar 2025
37. Hossain, T.S., Yigitcanlar, T., Nguyen, K., Xu, Y.: Cybersecurity in local governments: a systematic review and framework of key challenges. Urban Governance (2025). https://doi.org/10.1016/j.ugj.2024.12.010
38. Houichi, M., Jaidi, F., Bouhoula, A.: Cyber security within smart cities: a comprehensive study and a novel intrusion detection-based approach. Computers, Materials & Continua **81**(1), 393–441 (2024) https://doi.org/10.32604/cmc.2024.054007
39. Chaudhuri, A., Bozkus Kahyaoglu, S.: Cybersecurity assurance in smart cities: a risk management perspective. EDP Audit, Control, and Security Newsletter **67**(4), 1–22 (2023). https://doi.org/10.1080/07366981.2023.2165293
40. Chen, D., Wawrzynski, P., Lv, Z.: Cyber security in smart cities: a review of deep learning-based applications and case studies. Sustainable Cities and Society **66**, article ID 102655 (2021) https://doi.org/10.1016/j.scs.2020.102655
41. Chodakowska, A., Kańduła, S., Przybylska, J.: Cybersecurity in the local government sector in poland: more work needs to be done: more work needs to be done. Lex Localis: Journal of Local Self-Government **20**(1), 161–192 (2022). https://doi.org/10.4335/20.1.161-192
42. Institute for Defense & Business, What Are the Cybersecurity Risks for Smart Cities?. https://www.idb.org/what-are-the-cybersecurity-risks-for-smart-cities/. Accessed 27 Mar 2025
43. Jaikaran, C.: Cybersecurity: Selected Cyberattacks. https://www.congress.gov/crs-product/R46974. Accessed 27 Mar 2025
44. Javed, R. et al.: Future smart cities: requirements, emerging technologies, applications, challenges, and future aspects. Cities **129**, article ID 103794 (2022) https://doi.org/10.1016/j.cities.2022.103794
45. Johnstone, M.N., Crowley, M., Murray, G.: Actor behaviour, notable incidents in critical infrastructures, and risks to the health sector. In: Mohiuddin, A. (eds.) Ransomware Evolution, pp. 33–49. CRC Press, Boca Raton (2025) https://doi.org/10.1201/9781003469506
46. Jones, E., Lake, M., Chaudhuri, A., Sehic, M., Rijnders, D., Coleman, Y.: For the public sector, cyber resilience has never been more important. https://www.weforum.org/stories/2022/07/how-do-you-safeguard-a-city-from-cyber-attacks/. Accessed 27 Mar 2025
47. Korzár Košice.: Hacker attack paralyzes KVP, information about old invoices is gone. https://kosice.korzar.sme.sk/c/20971804/hackersky-utok-paralyzoval-kvp-prec-su-informacie-o-starych-fakturach.html. Accessed 27 Mar 2025
48. Korzár Spiš.: Thousands of Euros Withdrawn from Municipal Account. Bank Talks About Phishing, Mayor Talks About Russian Hackers. https://spis.korzar.sme.sk/c/23436729/z-uctu-obce-vytiahli-tisice-eur-banka-hovori-o-phishingu-starostka-o-ruskych-hackeroch.html. Accessed 27 Mar 2025
49. Leclercq, E.M., Rijshouwer, E.A.: Enabling citizens' right to the smart city through the co-creation of digital platforms. Urban Transform **4**(2), 1–19 (2022). https://doi.org/10.1186/s42854-022-00030-y
50. Lee, C., He, Z., Yuan, Z.: A pathway to sustainable development: Digitization and green productivity. Energy Economics **124**, article ID 106772 (2023) https://doi.org/10.1016/j.eneco.2023.106772
51. Lewallen, J.: Emerging technologies and problem definition uncertainty: the case of cybersecurity. Regulation & Governance **15**, 1035–1052 (2021). https://doi.org/10.1111/rego.12341

52. Li, F., Yan, X., Xie, Y., Sang, Z., Yuan, X.: A review of cyber-attack methods in cyber-physical power system. In: 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), Xi'an, China, pp. 1335–1339 (2019) https://doi.org/10.1109/APAP47170.2019.9225126
53. Li, Y., Liu, Q.: A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Rep. **7**, 8176–8186 (2021). https://doi.org/10.1016/j.egyr.2021.08.126
54. Logota, E., Mantas, G., Rodriguez, J., Marques, H.: Analysis of the impact of denial of service attacks on centralized control in smart cities. In: Mumtaz, S., Rodriguez, J., Katz, M., Wang, C., Nascimento, A. (eds.) Wireless Internet. WICON 2014, pp. 91–96. Springer, Cham (2015) https://doi.org/10.1007/978-3-319-18802-7_13
55. Lowe, M., et al.: City planning policies to support health and sustainability: an international comparison of policy indicators for 25 cities. Lancet Glob. Health **10**(6), e882–e894 (2022). https://doi.org/10.1016/S2214-109X(22)00069-9
56. Malacky.: Cyber attack on city hall. https://malacky.sk/archiv/index803e.html?page=clanok_cely&id=11075. Accessed 27 Mar 2025
57. Millard, J.: Impact of digital transformation on public governance - New forms of policy-making and the provision of innovative, peoplecentric and inclusive public services. Publications Office of the European Union, Luxembourg (2023). https://doi.org/10.2760/204686, JRC133975
58. Nette, A.: What's the Difference Between a Cyber Incident and Data Breach?. https://www.hivesystems.com/blog/whats-the-difference-between-a-cyber-incident-and-data-breach. Accessed 27 Apr 2025
59. Norris, D.F., Mateczun, L.K.: Cyberattacks on local governments 2020: findings from a key informant survey. Journal of Cyber Policy **7**(3), 294–317 (2022). https://doi.org/10.1080/23738871.2023.2178319
60. Norris, D.F., Mateczun, L., Joshi, A., Finin, T.: Managing cybersecurity at the grassroots: evidence from the first nationwide survey of local government cybersecurity. J. Urban Aff. **43**(8), 1173–1195 (2022). https://doi.org/10.1080/07352166.2020.1727295
61. Noviny.: Thousands of euros have been stolen from the municipal account. The mayor talks about a hacker attack. https://www.noviny.sk/krimi/874437-z-obecneho-uctu-odisli-tisice-eur-starostka-hovori-o-hackerskom-utoku. Accessed 27 Mar 2025
62. OECD.: Making Decentralisation Work: A Handbook for Policy-Makers, OECD Multi-level Governance Studies. OECD Publishing, Paris (2019). https://doi.org/10.1787/g2g9faa7-en
63. Pandey, P., Golden, D., Peasley, S., Kelkar, M.: Making smart cities cybersecure: Ways to address distinct risks in an increasingly connected urban future. https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html. Accessed 27 Mar 2025
64. Pichlmayr, J.: Cyber Security for Our Communities. https://www.kdz.eu/en/news/blog/cyber-security-our-communities. Accessed 27 Mar 2025
65. Pinto, G., Wang, Z., Roy, A., Hong, T., Capozzoli, A.: Transfer learning for smart buildings: A critical review of algorithms, applications, and future perspectives. Advances in Applied Energy **5**, article ID 100084 (2022). https://doi.org/10.1016/j.adapen.2022.100084
66. Prebilič, V., Kukovič, S.: Cooperation between local communities and the civil protection in overcoming the COVID-19 Crisis: Ad Omnia Parati Sumus. Annals for Istrian and Mediterranean Sudies: Series Historia et Sociologia **31**(3), 535–544 (2021)
67. Preis, B., Susskind, L.: Municipal cybersecurity: more work needs to be done. Urban Affairs Review **58**(2), 614–629 (2022). https://doi.org/10.1177/1078087420973760
68. Rebecchi, A., Capolongo, S.: Healthy Design and Urban Planning Strategies framing the SDG 11 Sustainable Cities and Communities. European Journal of Public Health **31**, ckab164.733 (2021). https://doi.org/10.1093/eurpub/ckab164.733

69. Regióny Trenčín.: Another CYBER ATTACK! Hackers attacked a critical infrastructure facility: It is believed to be the same group as the cadastre. https://trencin.zoznam.sk/dalsi-kyberneticky-utok-hackeri-napadli-objekt-kritickej-infrastruktury-ma-ist-o-tu-istu-skupinu-ako-pri-katastri/. Accessed 27 Mar 2025
70. Ručinská, S., Fečko, M., Mitaľ, O., Jesenko, M.: Bottom-up response: the role of municipalities and citie in compensating and supporting central government's role. Journal of Comparative Politics **16**(1), 25–42 (2023)
71. Ručinská, S., Fečko, M.: eServices as a challenge for small municipalities: slovak republic experiences. In: Hemker, T., Müller-Török, R., Prosser, A., Scola, D., Szádeczky, T., Urs, N. (eds.) Central and Eastern European eDem and eGov Days 2020: Conference Proceeding. Facultas Verlags: Wien, pp. 383–392 (2020). https://doi.org/10.24989/ocg.338.30
72. Ručinská, S., Mitaľ, O., Fečko, M.: Dobré spravovanie a odolnosť obcí a miest v dobe digitálnej transformácie. Leges: Praha (2024)
73. Ručinská, S., Fečko, M., Mitaľ, O.: Municipalities and cities in the center of the digital and green transition. In: Lisowski, R., Scholz, L., Trüe, Ch. (eds.). Academia, Administration, Digitalization and Sustainability. Nomos: Baden-Baden, pp. 19–38 (2025). doi.org/https://doi.org/10.5771/9783957104434-19
74. Schlegel, T.: Cyber Attacks on Municipalities. https://abouttrust.tuvsud.com/en/digitization/cyber-attacks-on-municipalities. Accessed 27 Mar 2025
75. Szymoniak, S., Kubanek, M., Kesar, S.: AI-based enhancing of the smart city residents' safety. In: Marcinkowski, B., Przybylek, A., Jarzębowicz, A., Iivari, N., Insfran, E., Lang, M., Linger, H., Schneider, C. (eds.) Harnessing Opportunities: Reshaping ISD in the post-COVID-19 and Generative AI Era, Gdańsk, Poland, pp. 1–4. University of Gdańsk, Gdansk (2024) https://doi.org/10.62036/ISD.2024.10
76. Teraz.sk.: Malacky City Hall restores systems after hacker attack. https://www.teraz.sk/regiony/malacky-mestsky-urad-obnovuje-chod-sy/586905-clanok.html. Accessed 27 Mar 2025
77. TVNoviny.sk.: Hacker paralyzes local office in Košice: Experts now investigating whether sensitive information was leaked. https://tvnoviny.sk/domace/clanok/95866-hacker-paralyzoval-miestny-urad-v-kosiciach-experti-teraz-skumaju-ci-neunikli-citlive-informacie?__tuu7ntqxozayndugcxfzydhlntyyxndhzhe=dnywatdn&__tuu7ntqxozkzmj0gcxfzydhlntyyxndhzhe=-a1-v3&__tuu7ntqxozy0nzagcxfzydhlntyyxndhzhe=-a1-v3&__tuu7ntqxpda%20mjagcxfzydhlntyyxndhzhe=-a1-v3&__tuu7ntqxpda2pd0gcxfzydhlntyyxndhzhe=-a1-v3&__tuu7ntqxpdu3mtqgcxfzydhlntyyxndhzhe=-a1-v3. Accessed 27 Mar 2025
78. Vasyltsiv, T., Biletska, I., Mulska, O.: Organizational and financial instruments of decentralizaton and development of united territorial communities in Ukraine: Poland´s experience. Management Theory and Studies for Rural Business and Infrastructure Development, **43**(2), 276–287 (2021). https://doi.org/10.15544/mts.2021.24
79. Verhulsdonck, G., Weible, J.L., Helser, S., Hajduk, N.: Smart cities, playable cities, and cybersecurity: a systematic review. International Journal of Human-Computer Interaction **39**(2), 378–390 (2021). https://doi.org/10.1080/10447318.2021.2012381
80. Vitunskaite, M., He, Y., Brandstetter, T., Janicke, H.: Smart cities and cyber security: are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Comput. Secur.Secur. **83**, 313–331 (2019). https://doi.org/10.1016/j.cose.2019.02.009
81. Voytenko Palgan, Y., Mont, O., Sulkakoski, S.: Governing the sharing economy: Towards a comprehensive analytical framework of municipal governance. Cities **108**, article ID 102994. https://doi.org/10.1016/j.cities.2020.102994
82. Yin, R.K.: Case Study Research Design and Methods. SAGE Publications, Thousand Oaks (2013)