Pakistan Journal of Criminology
Vol. 16, No. 02, April—June 2024 (827-841)

International Experience in Ensuring Cybersecurity in Local Self-Government Management as a Component of the National Security of Ukraine

Svitlana Serohina[1], Ilona Harashchuk[2], Alina Murtishcheva[3], Olena Poproshaieva[4] & Svitlana Fomina[5]

Abstract

The study examines the critical relationship between cyber security as a component of national security and its provision in local government administration. The purpose of the study is to evaluate the international experience of ensuring cyber security in the management of local self-governments in Germany, Poland and Ukraine. In research were used visual and graphic methods, a set of methods of processing, comprehension and interpretation of information. This highlights the level of trust in local authorities in Poland, Germany and Ukraine, as well as a comparison of the systems of local self-government entities in the selected countries. It was established that there is a need to create and develop an adequate cybersecurity system. The result of the study is an analysis of the cyber security strategies of Germany, Poland and Ukraine. Prospects for further research are the analysis of the possibility of consolidation and differentiation of powers by subjects of local self-government in ensuring cyber security. An analysis of the real need for the powers related to providing cyber security and the ability to perform them is appropriate.

Keywords: cybersecurity, cybersecurity entities, local self-government management, national security, international experience.

[1] The author is a Doctor of Legal Sciences, Head of the Department of State Building, Yaroslav Mudryi National Law University, Ukraine. She can be reached at s.g.serohina@gmail.com
[2] The author is a Candidate of Juridical Science, Senior Lecturer of the Department of State Building, Yaroslav Mudryi National Law University, Ukraine. She can be reached at ilona.harashchuk@ukr.net
[3] The author is a Candidate of Legal Sciences, Associate Professor of the Department of State Building, Yaroslav Mudryi National Law University, Ukraine. She can be reached at a.murtishcheva565@gmail.com
[4] The author is a Candidate of Legal Sciences, Associate Professor of the Department of State Building, Yaroslav Mudryi National Law University, Ukraine. She can be reached at o.a.poproshaieva@yahoo.com.ua
[5] The author is a Candidate of Legal Sciences, Assistant of the Department of State Building, Yaroslav Mudryi National Law University, Ukraine. She can be reached at sv.v.fominaa@hotmail.com

Introduction

In recent years, national security issues have been high on the agenda of many countries. At the same time, the development of information technology, in addition to other components of national security (in particular, national border protection, economic security, and labour protection system), aroused interest in another element – cybersecurity (Kavyn et al., 2021). At the same time, there is a need to specify the subjects of its provision, if any, to create such subjects if necessary or to vest existing subjects with specific powers. For example, among the entities responsible for ensuring cybersecurity, local self-government entities occupy a prominent place (Nayak et al., 2021).

Therefore, it is vital to study and assess the international experience of ensuring cybersecurity in local self-government through the prism of their responsibilities, powers and the level of public trust in these entities, such as Germany, Poland, and Ukraine. When selecting the countries for analysis, attention was focused on the geographical distance of the countries from Ukraine; similarities in the form of government and administrative-territorial division; membership in the European Union (in particular, through the European vector of Ukraine's development). In addition, due to the emigration of many Ukrainians to Germany and Poland, we chose these countries based on the criterion of security and cybersecurity in managing local self-government bodies.

The study aims to assess the international experience of ensuring cybersecurity in local self-government in Germany, Poland, and Ukraine.

Research objectives

1. To determine the level of trust in local self-government in Poland, Germany and Ukraine.

2. To study cybersecurity in local self-government in Poland, Germany, and Ukraine through the prism of the bodies in the local self-government system responsible for ensuring cybersecurity in the selected countries.

3. Analyse the Cybersecurity Strategies of Germany, Poland, and Ukraine as a formal reflection of state policy towards cybersecurity, particularly in managing local self-government.

4. To propose recommendations for improving cybersecurity in local government.

1. Methods

The research procedure involves several stages, namely: identification of countries whose experience in ensuring cybersecurity in local self-government will be studied; identification of bodies in the local self-government system

responsible for ensuring cybersecurity in the selected countries; carrying out a comparative analysis of the structural organisation of bodies in the local self-government system, their duties, rights and tasks entrusted with the responsibility for ensuring cybersecurity in Ukraine, Poland and Germany, and identification of common and distinctive features.

The consequences of inadequate cybersecurity include cyberattacks, data loss, and access to classified information. All of these consequences affect citizens in one way or another, so a comparative analysis of the level of trust in local government in Poland (CBOS, 2018), Germany (Kommunal politik, 2019) and Ukraine (Association of Cities of Ukraine, 2019) was carried out. The results of these studies were aimed at assessing the state of local democracy and preparing plans to improve local government efficiency in specific areas and in general. The research methodology involved graphical comparison methods, which made it possible to display the level of trust in local self-government in the analysed countries as a percentage. Determining the level of trust is a prerequisite for the further creation/improvement of effective policies and setting priorities and goals in various areas (including cybersecurity).

When selecting countries for analysis, attention was focused on their geographical distance from Ukraine; similarities in the form of government and administrative and territorial division; membership in the European Union (providing the European vector of Ukraine's development). In addition, due to the emigration of many Ukrainians to Germany and Poland, who chose these countries based on the criterion of security, the cybersecurity in the local self-government of these countries was selected for comparison with the national one.

A comparative analysis of the structural construction of bodies in the management system was conducted based on the research procedure and methodology. The analysis was carried out regarding the duties, rights, and tasks of subjects entrusted with ensuring cyber security in Ukraine, Poland and Germany. Several empirical methods were used in the implementation of this study. Using the analysis-synthesis method, it was possible to compare the bodies in the local self-government management system, which are entrusted with the responsibility of ensuring the cyber security of the selected countries. The result of using the visual-graphic method was the creation of a graph, which shows the level of trust in local self-government in Poland, Germany, and Ukraine in percentage ratios. The method of scientific observation made it possible to clearly define the goal, methodology and develop a research plan. The processing, comprehension and interpretation methods of the obtained data array provided the possibility of theoretical definition of concepts in the researched topic. The dialectical method contributed to achieving the research goal by analysing

debatable issues. The formal-logical method provided a qualitative study of the provision of cyber security in the management of local self-government through the study of delegated powers.

Literature review

The study of the organisational and practical aspects of local self-government, characterisation of the administrative and legal status of these bodies, analysis of the effectiveness of the tasks assigned to these bodies, management of local self-government, and the role of local self-government in ensuring national security have always been the subject of scientific research by various scholars.

Some studies of local self-government in Poland suggest that local self-government was created by delegating public administration as entities designed to meet the needs of local and regional communities, including security, which is an essential public need. Three levels of local self-government entities perform public security tasks, which differ in intensity, scope and coverage (Mykytyuk et al., 2021; Serohina et al., 2019). The position of a governmental commissioner of local self-government in the field of public security in martial law and state of emergency is introduced. The ability of municipalities and cities in Poland to respond to disasters has been analysed and compared (Czuryk & Kostrubiec, 2019; Cvetković et al., 2021). Scientific explorations of the management of local self-government in Poland were carried out with an emphasis on the need to increase the effectiveness of local self-government through digitalisation. In particular, improving electronic services, implementing electronic governance, improving the quality of services, increasing transparency of activities and reducing costs (Rudyte & Kontrimaite, 2020).

At the same time, digitalisation measures lead to an increase in the amount of digital data that needs to be protected from cyberattacks and malware. Accordingly, it is vital to ensure adequate digital infrastructure protection to prevent cyber threats. State institutions should sufficiently address these cybersecurity issues to avoid unauthorised information leakage, personal data, their sale and other actions to protect citizens' data (Garcia-Perez et al., 2023).

Scientific research on the management of security and public order in Poland has been carried out in governance by two organisational solutions: centralist and decentralist. At the same time, security responsibilities are shared between local, mainly municipal, self-government institutions, which is associated with the decentralisation of public responsibilities. Local self-government's role in ensuring citizens' security in Poland is defined, and it should meet citizens' expectations regarding security to ensure high efficiency, quality, and innovation (Misiuk et al., 2020).

Local self-government management in Croatia must be improved by creating and using a hybrid flexible model. The existing functional path of the organisational structure of local self-government bodies does not meet the existing requirements. At the same time, negative circumstances of the functional organisational structure of local self-government were revealed (Car-Pušić et al., 2020).

Ukrainian scholars' research in the field of local self-government management is limited to several areas: the possibility of introducing the institution of risk management in the activities of local self-government in Ukraine (Bortnik, 2021); interaction of local self-government with other government institutions (Faradzhov, 2021);

Ensuring national security by local self-government is considered by scholars in the aspect of analysing specific components of national security, in particular:

- protection of the national borders (Polovnikov, 2019), emphasising the need to participate in the protection of the state border and ensuring the security of the state border of Ukraine and the cross-border security of Ukraine. Security must be carried out by all subjects of the country's authorities, particularly in matters of stability of crossing the border, marking, order of security, crossing and maintenance;

- Economic security is considered a management system in terms of existing factors that contribute to a holistic picture of economic security as an essential component of the country's national security (Polzun, 2020).

An additional study of individual entities that ensure the economic security of Ukraine and their interaction with local self-government was carried out (Melnik, 2019);

- healthcare system (Brinkerhoff et al., 2019), analysing the results of the implementation of healthcare reform by local governments and other actors through the prism of organisational, managerial and regulatory frameworks;

- information security (Alguliyev et al., 2020), examining it in the context of ensuring information security by local self-government. Such provision is carried out in compliance with the balance of the interests of the individual, society, and the state and their effective cooperation in the global information space;

- cybersecurity (Fichtner, 2018), in the context of analysing local self-government as a general subject of cybersecurity. In particular, determining their place and role, functions, powers, as well as the grounds, conditions, and directions of their interaction in the process of implementing measures to ensure security in cyberspace;

- the labour protection system (Delgado & Escorihuela, 2020), through the prism of taking the necessary measures by local self-government. Such measures are aimed at preserving a person's life, health, and working capacity in the work process and preventing future accidents. An analysis of the regulatory and legal provision of labour protection was carried out, taking into account the processes of European integration of Ukraine and the clarification of the regulatory and legal context of the reform of its system.

At the same time, ensuring cybersecurity is essential for all public authorities, including local governments, primarily to prevent cyberattacks aimed at government agencies and critical infrastructure (Senol & Karacuha, 2020).

At the same time, the issue of applying international experience to ensure cybersecurity in local government management as a component of national security remains poorly researched, given its relatively short-term need.

Results

Using the method of comparative analysis and the indicators already available in the studies, we will obtain the corresponding indicators of the level of trust in local government in Poland, Germany, and Ukraine. The results of the survey are answers to the question "To what extent do you trust the local self-government of your country?" in terms of "high trust/openness", "medium or low confidence", "ambivalent attitude", "slight to moderate distrust", "high distrust/cautiousness" in 2022.

Based on the results (Figure 1), it should be noted that there is a higher level of trust/openness and medium/low confidence in local self-government in Poland, Germany, and Ukraine. At the same time, the lion's share of the survey results is the ambivalent attitude, which makes it possible to assert that the respondents have not made up their minds or their attitude is ambiguous.

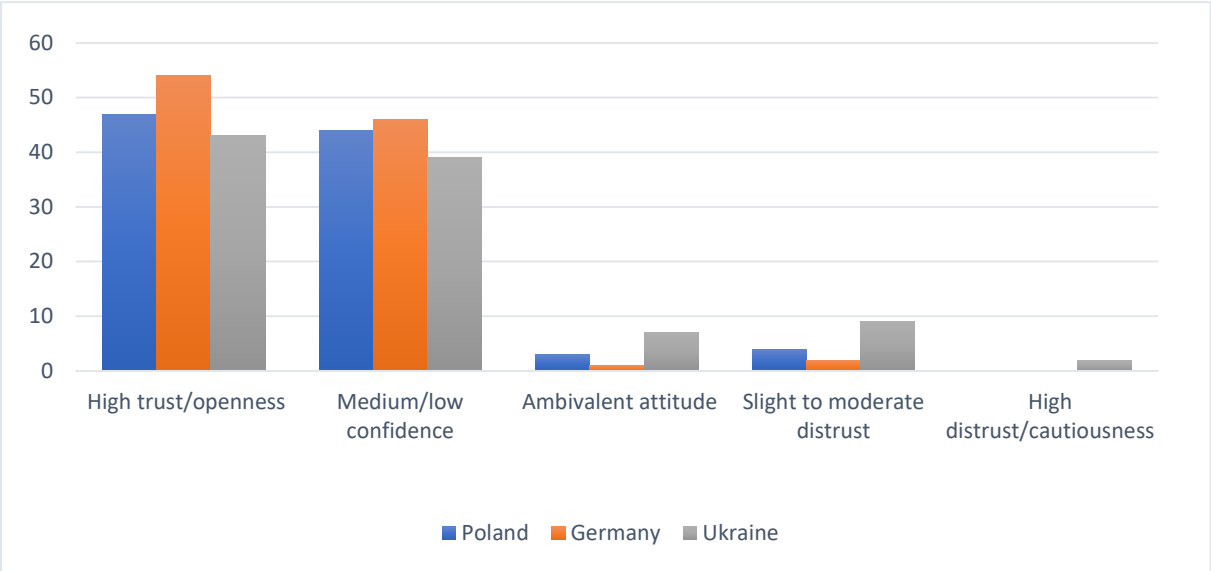

Figure 1. Indicators of the level of trust in local self-government in Poland, Germany and Ukraine in 2022

We will consider cybersecurity in local government in Poland, Germany and Ukraine through the prism of the bodies in the local self-government system responsible for ensuring cybersecurity in the selected countries (see Table 1).

Table 1.
Local self-government bodies in Poland, Germany, and Ukraine and their cybersecurity responsibilities.

	Poland	**Germany**	**Ukraine**
Local self-government bodies	Local and municipal councils, district councils, and district boards chaired by the head marshal of the province.	Municipal or city councils, administrations, civic unions, and districts.	Village, settlement, district, district in cities, city, oblast councils
The duty to ensure cybersecurity	The Law on the National Cybersecurity System explicitly provides for cybersecurity by local self-government entities. In	Local self-government entities ensure cybersecurity by fulfilling their	Local self-government bodies are not part of the security and

	particular, local self-governments appoint two persons to liaise with the national cybersecurity system. They are also obliged to provide access to the strategic security network operator to place telecommunications infrastructure facilities and equipment on their territory.	duties, including conducting an inventory of protection levels, analysing the level of IT security, and implementing a basic protection profile for local self-government entities.	defence sector or entities that directly carry out cybersecurity activities within their competence, and cybersecurity functions are not a core part of their activities.

The study's results show that not all analysed countries have a regulatory obligation for local self-government entities to ensure cybersecurity.

There is a need to create and develop an adequate cyber security system and distribute the responsibilities to ensure cyber security among all subjects of authority. It is updated due to the constant growth in cyber threats. Cyber threats are often aimed at capturing information data from a certain remote source, gaining control over the resources of a certain source, or disabling the system of this source. The result of cyber threats can be cyber attacks that violate the integrity, stability, reliability, and confidentiality of resources containing electronic information data.

The importance of cybersecurity in the local government system depends on the degree of actual and potential cyber threats to the proper functioning of the territorial community's life support system. The importance of protecting a person's and a citizen's vital interests when using cyberspace in local self-government will only grow as cyberspace has no administrative-territorial division and no interstate or internal borders.

Among the responsibilities that may be imposed on local self-government authorities about cybersecurity are the following: informing the public, in particular through the media, about their activities related to cybersecurity; cooperating in certain areas with security and defence actors; exercising democratic civilian control over the security and defence sector; conducting an inventory of the existing degrees of protection in the internal system of local self-government entities; analysing the level of IT security; monitoring the state of pre-

conscription training of citizens for military service (including those who will later serve in cybersecurity units).

In addition, the determination of powers and duties of local self-government management subjects should be differentiated for each type of subject. Differentiation should depend on the place in the system of subjects, the real need for such powers, as well as the possibility and ability to implement them. At the same time, such powers may also have a delegated nature.

The need for additional research, in particular, an analysis of the actual capabilities of each local self-government entity in ensuring cyber security, is being updated. The analysis should consider their importance for national security and defence. Also, critical infrastructure facilities are located in the territory to which a certain entity of local self-government management extends its activity.

Discussion

It should be noted that the research methodology was based on countries selected by the criteria of geographical distance from Ukraine; similarity in the form of government and administrative and territorial division; and membership in the European Union (providing the European vector of Ukraine's development). In addition, due to the emigration of many Ukrainians to Germany and Poland, who chose these countries based on the criterion of security, the cybersecurity in the local government of these countries was selected for comparison with the national one (Boldyriev et al., 2019).

The study's results confirm that the existing data is not widely considered in the scientific literature, particularly the lack of proper cybersecurity in local government management as a component of national security. Scientists (Salman & Mustafa, 2023; Awais, et al., 2018*)* have mostly considered cybersecurity actors with exclusive powers in this area, leaving out entities for which such powers are not the main but additional ones or entities whose powers could include cybersecurity.

At the same time, agreeing with scholars *(*Dunn Cavelty, & Wenger, 2020*)*, it should be noted that state policy in cybersecurity reflects the state's strategic course in this area of public relations.

The analysis of the indicators showed that the formal reflection of state policy in the area of cybersecurity, in particular in local government management, is the development and implementation of appropriate cybersecurity strategies. Many scholars have reached such conclusions (Song et al., 2021; Senol & Karacuha, 2021). In sharing these conclusions, it is advisable to analyse the current cybersecurity strategies in Ukraine, Germany, and Poland.

The Cybersecurity Strategy of Ukraine was approved in 2021 and is envisaged for the period 2021-2025. It has become particularly relevant during martial law due to constant cyberattacks on the information systems of state and local governments, systems of state and private enterprises and organisations (Verkhovna Rada of Ukraine, 2021). The need to update the previous strategy is also becoming more urgent due to the growing technical level of cyber threats, the continuous improvement of tools, and the development of cyber-attack mechanisms. The trend of using cyberattacks as a tool for special information operations, manipulating public opinion, and influencing electoral processes is growing. The strategy is aimed at ensuring the security of cyberspace, conditions for its operation, protection of the state, citizens and individual individuals *(*Verkhovna Rada of Ukraine, 2018). The central cybersecurity system is a set of cybersecurity entities. Each occupies a special place in this system and solves specific tasks within its competence, principles of functioning, tasks, and legal status, as defined by law.

The Cybersecurity Strategy for Germany was also adopted in 2021. This document describes the framework within which the German Federal Government will develop its activities, including creating transparency and traceability for all actors from government, business, academia and society, establishing reporting and control at the strategic level for cybersecurity by all actors, and systematically preparing future assessments and continuous development. Given the similarity of their subject matter, this strategy analyses the correlation between cybersecurity and information security. It is emphasised that the complexity of IT systems and algorithms often leads to undesirable system behaviour and security gaps, the so-called vulnerabilities. Therefore, attackers use the global availability of systems due to their vulnerability to criminal intent.

As rightly noted by scholars (Štitilis et al., 2020), an actual cyberattack is accompanied by blackmail attempts, for example, the threat of publishing customer data on the Internet or the danger of transferring confidential information to competitors. Ransomware is now causing significant damage, especially as the affected areas are often networked across the globe and are so large that individual parts of companies or entire regions of infrastructure can be taken down in the event of such an attack.

It is noted that advisory services provided by, among others, the Federal Office for Information Security (BSI), government-funded research and preventive measures from various security agencies ensure that minimum requirements for IT security are established and met, that cyberattacks are detected and investigated, and that perpetrators of security and law enforcement agencies

identify and prosecute criminals – it is often a particular problem due to their global reach (Federal Ministry of the Interior, Building and Community, 2021*).*

Poland's Cybersecurity Strategy was adopted in 2019 for 5 years, meaning that 2024 it will be updated, and its implementation will be analysed. The strategy aims to increase resilience to cyber threats and protect public, military, and private information. The main tasks of the strategy are aimed at the effective prevention of problems in cyberspace and the development of the cybersecurity system in Poland. The goal is also to consolidate Poland's strong position in cyber security at the international level and increase citizens' awareness in this field.

At the same time, in the context of ensuring cyber security in local self-government management, it is indicated that it is necessary to increase the competence of personnel not only in subjects important for the cyber security system of Poland. It is important to implement systemic solutions to provide substantial support for improving the competence of the state administration and local self-government employees. Due to the many challenges related to cyber security, it is important to continuously raise public awareness through, among other things, special education programs and awareness campaigns. Among other things, measures will be taken to develop and build an information exchange system resistant to cyber threats, which will contribute to national security management. In addition, to increase the security of key and digital services, as well as critical infrastructure: the Integrated Cyberspace Security Management System of the Republic of Poland will be implemented. An important element that increases the level of cybersecurity is developing and implementing risk assessment methodology at the national level (Ministry of Digitization, 2019).

Even though the state cybersecurity policy has a long-term purpose, its components may change depending on the threats, which may evolve into new forms.

Agreeing with the scholars (Salman & Mustafa, 2023), it should be noted that despite the progress made in ensuring cybersecurity in local self-government management in different countries. Appropriate policy and regulatory measures should be taken continuously to ensure the resilience of information systems, key service providers, critical infrastructure operators, digital service providers, and public administration bodies to cyber threats. The development and implementation of a risk assessment methodology at the national level is also an essential element that increases the level of cybersecurity.

Conclusion

The article demonstrates the multifaceted nature of these relations thanks to a multidimensional analysis of the complex relationship between national

security and cybersecurity as its component and the identification of international experience in ensuring cybersecurity in local self-government. In particular, it was established that ensuring cyber security for the local self-government management system depends on the degree of real and potential cyber threats. The study reveals the difference in the provision of cyber security in managing local self-government in Germany, Poland and Ukraine. The differences depend on the territorial structure, the extent of the granted powers and their detailed specification, the level of development of the states, and the understanding of the importance of ensuring cyber security as a component of national security. Based on the research results, it can be seen that not all analysed countries have the obligation of local self-government entities to ensure cyber security at the regulatory level.

In light of the results of the study, the actualisation of the need to create and develop an adequate cyber security system becomes obvious. The distribution of responsibilities to ensure cyber security among all subjects of power is important because of the constant growth in the level and number of cyber threats. Cyber threats are often aimed at capturing information data from a certain remote source, gaining control over the resources of a certain source, or disabling the system of this source. The result of cyber threats can be cyberattacks that violate the integrity, stability, reliability, and confidentiality of resources.

Recommendations

- analysis of the actual cybersecurity capabilities of each type of local self-government entity, taking into account the criticality of the national security and defence system, the territory of their operation, and the location of critical infrastructure facilities in this territory;
- development of proposals for differentiation for each type of local self-government entity, depending on their place in the system of local self-government entities, the real need for powers related to cybersecurity and the ability to exercise them;
- analysing the need to enshrine local self-government entities as components of the security and defence sector, in particular in the area of cybersecurity;
- analysing the possibility of assigning permanent and limited powers (for example, for the period of martial law) to local self-government entities to ensure cybersecurity;
- specifying the possible competence and powers of local self-government entities, assigning them specific responsibilities, and determining the need for reporting.

References

Alguliyev, R., Imamverdiyev, Y., Mahmudov, R., & Aliguliyev, R. (2020). Information security as a national security component. *Information Security Journal*, *30*, 1-18. https://doi.org/10.1080/19393555.2020.1795323

Association of Cities of Ukraine. (2019). Results of the survey on the level of trust of the community in the local government. Retrieved from https://auc.org.ua/novyna/rezultaty-opytuvannya-shchodo-rivnya-doviry-gromady-do-miscevoyi-vlady-provedene-ukrayinsko

Boldyriev, S. V., Steshenko, T. V., Frolov, O. O., Chyrkin, A. S., & Shestopal, S. S. (2019). Institutional transformation of the financial basis of the local self-government. *Opcion, 35*(90-2), 614–630. Retrieved from https://dspace.nlu.edu.ua/bitstream/123456789/17782/1/614-630.pdf

Bortnik, O. (2021). Risk management in local self-government based on international standards. *Investytsiyi: Praktyka ta Dosvid, 1,* 141-144. Retrieved from http://www.investplan.com.ua/pdf/1_2021/24.pdf

Brinkerhoff, D., Cross, H., Sharma, S., & Williamson, T. (2019). Stewardship and health systems strengthening. *Public Administration and Development, 39*(1), 1-39. https://doi.org/10.1002/pad.1846

Car-Pušić, D., Marović, I., & Bulatović, G. (2020). Development of a hybrid agile management model in local self-government units. *Tehnicki Vjesnik, 27*(5), 1418-1426. https://doi.org/10.17559/TV-20190205140719

CBOS. (2018). Distrust and trust. Retrieved from https://www.cbos.pl/SPISKOM.POL/2018/K_035_18.PDF

Cvetković, V., Tanasić, J., Ocal, A., Kešetović, Ž., Nikolić, N., & Dragašević, A. (2021). Capacity development of local self-governments for disaster risk management. *International Journal of Environmental Research and Public Health, 18,* 1-33. https://doi.org/10.3390/ijerph181910406

Czuryk, M., & Kostrubiec, J. (2019). The legal status of local self-government in the field of public security. *Studia nad Autorytaryzmem i Totalitaryzmem, 41*(1), 33-47. https://doi.org/10.19195/2300-7249.41.1.3

Delgado, J., & Escorihuela, U. (2020). Protección social. In J. Delgado (Ed.), *La Economía Aplicada: Políticas Económicas de los Gobiernos* 1st ed (pp. 211-226). Barcelona: J.M Bosch. https://doi.org/10.2307/j.ctv14t46dx

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Faradzhov, Sh. (2021). Powers of local self-government in the national security system. *Investytsiyi: Praktyka ta Dosvid, 6,* 109–114. Retrieved from http://www.investplan.com.ua/pdf/6_2021/20.pdf

Federal Ministry of the Interior, Building and Community. (2021). Cybersecurity strategy for Germany 2021. Retrieved from https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=2#:~:text=Die%20%E2%80%9ECybersicherheitsstrategie%20f%C3%BCr%20Deutschland%202021,ist%20eine%20Analyse%20der%20Bedrohungslage

Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review, 7*(2), 1-39. https://doi.org/10.14763/2018.2.788

Garcia-Perez, A., Cegarra-Navarro, J., Sallos, M., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation. 121*. https://doi.org/10.1016/j.technovation.2022.102583

Kavyn, S., Bratsuk, I., & Lytvynenko, A. (2021). Regulatory and legal enforcement of cyber security in countries of the European Union: The experience of Germany and France. *Teisė, 121*, 135–147. https://doi.org/10.15388/Teise.2021.121.8

Kommunal politik. (2019). Main page. Retrieved from https://kommunal.de/

Melnik, V. (2019). The role of tax police units of the State Tax Service of Ukraine as subjects of ensuring the system of economic security of the state. *Legal Horizons*, *18*, 71–78. http://dx.doi.org/10.21272/legalhorizons.2019.i18.p71

Ministry of Digitization. (2019). Cybersecurity Strategy of the Republic of Poland for 2019-2024. Retrieved from https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024

Misiuk, A., Sulowski, S., Gierszewski, J., & Urbanek, A. (2020). The role of territorial self-government in ensuring personal security of citizens in Poland. *European Research Studies Journal, XXIII*(1), 601-616. Retrieved from https://ersj.eu/journal/1574

Mykytyuk, P., Semenets-Orlova, I., Blishchuk, K., Skoryk, H., Pidlisna, T., & Trebyk, L. (2021). Outsourcing as a tool of strategic planning in public administration. *Estudios de Economia Aplicada, 39*(3). https://doi.org/10.25115/eea.v39i3.4718

Nayak, P., Singh, K., & Dave, P. (2021). Does data security and trust affect the users of fintech? *International Journal of Management (IJM), 12*(1), 191-206. http://doi.org/10.34218/IJM.12.1.2021.016

Polovnikov, V. (2019). Protection and control of the state border as a component of ensuring national security of Ukraine. *Bulletin of Kharkiv National University of Internal Affairs, 86*(3), 89-100. https://doi.org/10.32631/v.2019.3.09

Polzun, D. (2020). Economic security of the region as a component of national security of Ukraine. *Ekonomika ta Derzhava, 8*, 89–94. Retrieved from http://www.economy.in.ua/?op=1&z=4725&i=15

Rudyte, D., & Kontrimaite, M. (2020). New public management at local self-government institutions. *Eurasian Studies in Business and Economics, 13*(1), 169-180. https://doi.org/10.1007/978-3-030-40375-1_12

Salman, H., & Mustafa, R. (2023). Subject review: Detecting cyber security attacks. *International Journal of Advances in Scientific Research and Engineering, 9*(8), 44-52. https://doi.org/10.31695/IJASRE.2023.9.8.5

Senol, M., & Karacuha, E. (2020). Creating and implementing an effective and deterrent national cyber security strategy. *Journal of Engineering, 2020*, 5267564. https://doi.org/10.1155/2020/5267564

Serohina, S., Bodrova, I., & Novak, A. (2019). Delegation of state powers to local self-government bodies: Foreign experience and Ukrainian realities. *Baltic Journal of European Studies, 9*(3), 262–285. http://dx.doi.org/10.1515/bjes-2019-0033

Song, M., Kim, D., Bae, S., & Kim, S. (2021). Comparative analysis of national cyber security strategies using topic modelling. *International Journal of Advanced Computer Science and Applications, 12*, 62-69. https://dx.doi.org/10.14569/IJACSA.2021.0121209

Štitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., & Khorunzhak, N. (2020). National cyber security strategies: Management, unification and assessment. *Independent Journal of Management & Production, 11*(9). http://dx.doi.org/10.14807/ijmp.v11i9.1431

Verkhovna Rada of Ukraine. (2018). About the national security of Ukraine. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text

Verkhovna Rada of Ukraine. (2021). On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 «On the Cybersecurity Strategy of Ukraine». Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text