Institutiones Administrationis – Journal of Administrative Sciences Vol. 5 (2025) No. 1, 101–109
DOI: 10.54201/iajas.123

The Correlation of Digital Competence and Crisis Management

Evidence from the Polish Public Administration

Krzysztof Kaczmarek[*], **Mirosław Karpiuk**[**], **Jarosław Kostrubiec**[***]

[*]Assistant Professor, Faculty of Humanities, Koszalin University of Technology in Koszalin, Koszalin, Poland. E-mail: krzysztof.kaczmarek@tu.koszalin.pl

[**]Full Professor, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, Olsztyn, Poland. e-mail: miroslaw.karpiuk@uwm.edu.pl

[***]University Professor and Dean, Institute of Legal Sciences, Faculty of Law and Administration, Maria Curie-Skłodowska University, Lublin, Poland. e-mail: jaroslaw.kostrubiec@mail.umcs.pl

Abstract

In the age of digitalization, when almost all aspects of social activity are effected and novel threats to a rapidly changing environment are being posed, the ability of public servants to use digital tools competently is crucial for an effective crisis management. This article examines the two-dimensional importance of digital competence, which includes both an ability to operate modern technologies and an awareness of potential cyber threats. The study draws on a literature analysis coupled with qualitative and behavioral methods to explore how digital competence affects the effectiveness of crisis management. The results indicate that it is not only technical proficiency that is important but ongoing cyber security training too is of crucial importance. These two combined form the basis for effective prediction, monitoring and response to crises. The article highlights the need to integrate digital competence as a fundamental element of crisis management strategies in public administrations while suggesting directions for further research in this area.

Keywords

crisis management, digital competence, digital tools, public administration, data security

1 Introduction

Crisis management covers a wide range of activities undertaken by various actors. Most frequently, it is the government that bears responsibility for these activities, coordinating actions at different levels of administration. Crisis management is the totality of systemic solutions for the protection of the population carried out by public authorities at all levels in cooperation with specialized organizations and institutions (Olech, 2020, 97). In this system, civil servants constitute an important element, being a group of personnel specialized in carrying out the tasks

Article is licensed under CC BY 4.0 © 2025 The Author(s)

of executive authorities through public administration (Włodyka, 2022, 191). In addition to crisis and emergency management, their responsibilities also include monitoring and responding appropriately to warning signals. However, what is a problem for many organizations is the effectiveness of their perception of warning signals, which manifests itself most frequently in their failure to recognize important signals in time and, as a result, the ensuing lack of adequate preparation for the arrival of negative events. That is why the so-called unexpected incidents may occur, which could be characterized by the sudden emergence of a series of high-intensity events capable of causing significantly negative impact. At the same time, information emerges after the fact that some warning signals were, in fact, at hand. The cause of the problems referred to above lies in the distortions and disruptions of the processes of signal perception (Ćwik, 2017, 28). But changes in the security landscape, including an increased importance of non-military, paramilitary and hybrid threats, present new challenges to the crisis management system as well (Szczurek, 2023, 7).

Nowadays, digital tools such as artificial intelligence (AI), big data or geographic information system (GIS) are increasingly used in crisis management (Kostrubiec, 2021). These tools allow for better management of resources and coordination of various services. However, besides bringing greater efficiency to many segments of life, these new digital ecosystems also bring a number of risks along (Włodyka, 2024, 104). Thus, an effective use of the potential of digital tools requires high qualifications and analytical skills of those responsible for crisis management. Moreover, the use of advanced technologies also requires adequate security procedures, which is essential to prevent data protection abuses during crises. Only then can digital tools effectively support decision-making processes and enable rapid responses to changing conditions and minimize any undesirable outcomes of potentially harmful events (Karpiuk, 2021, 46).

The ability to use these digital tools effectively and being able to recognize and protect oneself against cyber threats is what we may call digital competence. The second aspect is rather crucial as in cyber-attacks the perpetrators often take advantage of the users' lack of awareness for potential cyber threats (Karpiuk et al., 2023, 647). It follows that emergency and crisis managers ought to possess both digital proficiency and cyber-security competence. As such, in the context of crisis management, the digital competence of public administration personnel should be analyzed in a two-dimensional manner, encompassing both an ability to use digital tools effectively and an awareness of cyber-security risks. Understanding these two aspects of digital competence is crucial for anticipating, monitoring and responding effectively to challenges in a dynamically changing security environment, and therefore for effective crisis management as well.

For further considerations and analyses of the importance of digital competencies of public administration employees in crisis management, it is necessary to determine the content of these competences. According to the European Commission's definition, digital competence is the "confident, critical, and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society. It is defined as a combination of knowledge, skills, and attitudes" (European Commission, 2019, 10). For present purposes, we accept this definition and proceed along these lines with our inquiry.

The main objective of this article, then, is to investigate and evaluate the impact of such a digital competence of public administration personnel on their effectiveness in managing crisis situations. According to our research hypothesis, there is a correlation between the level of digital competence of public servants and their effectiveness of crisis management. This hypothesis is tested on examples of Polish public administration which serves as the limitation of the study as well.

In terms of methods, our research utilizes mixed-research methods. A thorough overview of scholarly literature is used to yield a base of comparison for determining the nexus of effective crisis management and the use of digital tools. A systems analysis method is employed to place crisis management in a broader context of security processes and events. A comparative method is used to compare the effectiveness of various crisis management approaches. A dogmatic-legal method is endorsed to identify the normative aspects of crisis management. Finally, a qualitative method is employed to capture crisis management in its natural context.

2 Literature review and state of research

A review of research results on the digital competences of public administration personnel in the context of crisis management reveals several key challenges faced by organizations around the world. Some of them are concerned with rather obvious phenomena, while others present some general discussion on digitalization. To date, a number of results have been published from research conducted during the COVID-19 pandemic, showing that digital competences significantly affect the effectiveness of crisis response. However, there focus is clearly on the private sector (see e.g.: Leonard et al., 2020; Guo et al., 2020), and significantly less are concerned with the correlation between the digital competence of public officials responsible for crisis management and the effectiveness of their actions.

There is a recurrent emphasis on the nexus of effective digital transformation of public administration and technological and inter-institutional cooperation and collaboration with users and the private sector, which fosters innovation and better coordination of public services. As Verhoest et al. (2024) point out, successful digitalization of public services depends on close cooperation between public sector units and external stakeholders, which facilitates innovation and coordination. Studies in the Portuguese public sector have shown that low digital competence levels and lack of training are serious obstacles to digital transformation, although most employees express a willingness to develop their skills, especially in data management, cybersecurity and communication (see Lopes et al., 2023). Budai et al. (2023) demonstrate that effective development of digital competence among future public administration personnel requires not only formal training but also work on digital awareness and attitudes, as self-declared skills often differ significantly from actual ones.

The problem of shortage of staff qualified in the area of modern technologies in public administration is often mentioned in the literature. It is also emphasized that their level of digital competence should, by no means, be reduced to purely technical expertise, and that technology is not an end in itself, since the administrative personnel should focus on building practical skills for applying digital tools in everyday decision-making and service delivery (Łukaszuk, 2022, 289). Since they are obliged to respond to any threat that triggers a crisis situation, and given the response is a follow-up to the crisis situation, including activities aimed at removing the resulting threat (Czuryk et al., 2016, 21), the effectiveness of these actions is determined, among other things, by the competence of those carrying out their duties in this area, including digital competence. That is basic IT skills and the ability to confidently utilize digital tools, identify common threats (e.g., phishing, misinformation), and operate within digital communication and coordination systems in emergency scenarios.

However, effective crisis management also requires public managers to be able to build relationships with stakeholders and function efficiently in a dynamic political and administrative environment (Van der Wal, 2020), and a high level of digital competences among public

administration students is crucial for their future effectiveness in the public sector, but requires constant adaptation of educational programs to changing technologies (Budai et al., 2023). On the other hand, the use of machine learning methods can significantly improve the crisis management process through better analysis and prediction of potential threats (Okpala et al., 2023). The bulk of the literature points out that the implementation of digital crisis management tools brings not only organizational benefits, but also increased cyber risk, which requires effective mechanisms for protecting IT systems (Radanliev et al., 2020).

3 Digital competence in crisis management

The Act of 26 April 2007 on Crisis Management[1] in Art. 3 Item 1 defines the crisis situation as a situation adversely affecting the level of security of people, property of significant size or the environment, causing significant limitations in the operations of the relevant public administration bodies due to the inadequacy of their forces and resources. Crisis situation management, as an activity of public administration bodies in the sphere of national security focuses on the prevention of negative phenomena threatening security, thus preventing an emergence of consequences that will not only be difficult to remove but will also involve high costs.

Crisis situations may also trigger cyber threats, which is why both reliable IT infrastructure and the digital competence of public administration personnel are essential for effective response. In this context, digital competence refers not to advanced technical skills, but to the ability to securely use digital tools, follow established protocols, and cooperate with specialized IT units responsible for cyber security. One of the responsibilities of the public administration is to ensure cyber security as understood in Art. 2 Item 4 of the Act of 5 July 2018 on the National Cyber Security System,[2] as the resilience of information systems to actions that violate the confidentiality, integrity, availability and authenticity of data processed or related services offered by these systems.

Cyber security threats, as well as any other security threats, may lead to a crisis situation in which case crisis management measures are to be activated that may also result in a limitation of the exercise of civic liberties (Karpiuk, 2022, 121). Limitations of the exercise of constitutional freedoms and rights may only be established by an act and only when they prove necessary in a democratic state for its security or public order, or for the protection of the environment, health and public morals, or the freedoms and rights of others; however, such limitations may not violate the essence of these freedoms and rights. Tackling crisis situations may also require appropriate restrictions on individual freedoms (Hoffman & Kostrubiec, 2022, 51). Although, the source of human and civil rights lies in the inalienable dignity of the human being, crisis situations may justify their temporary limitation, provided that such measures remain proportional and do not infringe on fundamental values (Czuryk, 2022, 32). This legal and ethical constraint is highly relevant for public administration, as the use of digital technologies in emergency management, such as surveillance systems or access to personal data, must balance efficiency with respect for civil liberties (Czuryk, 2022, 32). Nevertheless, it should be taken into account that personal safety is the most vital principle that cannot be endangered by unrestrained respect for individual freedoms.

---

[1] Journal of Laws from the year 2023, Item 122, as amended.

[2] Journal of Laws from the year 2023, Item 913, as amended.

In the context of crisis management, the digital competences of public administration personnel are of crucial importance. The dynamics of change in the security environment and the development of digital tools require the said personnel to continuously develop new skills and deepen their knowledge (OECD, 2021). However, in some countries, the use of certain digital tools is not regulated by law. This is particularly the case for social media platforms, which may be used to reach a large part of the population or obtain the information necessary to effectively counter the effects of emergencies (Catakli, 2022, 125). Since digital competences include not only technical proficiency but also the ability to assess risks and verify sources, public administration employees must be capable of using social media both effectively and critically. In this context, the ability to recognize unreliable content or disinformation becomes an essential element of digital awareness that directly supports the effectiveness of crisis response. Digital competences in public administration are not just about knowing how to use technology, they also involve the ability to assess risks, verify information, and respond appropriately in complex situations. This is especially important when using social media during crises. While such platforms can help spread important messages quickly, they are also full of misleading or false information, and that is why public officials need to equipped with the ability of fact-checking.

Given that digital competences encompass both the ability to use new technologies and the awareness of their potential risks, public administration employees must not only be proficient in digital tools but also capable of recognizing and mitigating the challenges posed by unregulated digital spaces, such as social media. Social media can be used for real-time updates, sending alerts and messages or disseminating guidance to the public. It should also be stressed that, in order to avoid misinformation, it is crucial to remain critical of the information obtained from social media (Hulkó, 2021, 297). However, simply possessing data is useless if it is not properly interpreted. Once information is available, use of analytical tools to process large amounts of crisis-related data is crucial for a rapid and effective response (Qadir et al., 2016).

It should also be noted that, while this study focuses predominantly on Poland, the following constraints apply more broadly to democratic states, where the use of digital tools by public administrations is subject to limitations arising from the following requirements:

- Data security: public administration handles large amounts of sensitive personal data, which requires a high level of security. In this context, the risk of cyber attacks and data breaches constitutes a major challenge;
- Costs: implementation of modern technological solutions can be costly. These costs include the purchase of hardware and software, staff training as well as ongoing maintenance and upgrades of systems;
- Legal compliance: public administration has to comply with strict data protection and other legal regulations, which may limit the scope of digital solutions that can be implemented;
- Employee resistance: there may be resistance to change in public administration, particularly among employees who are accustomed to hierarchical structures, paper-based workflows, and routine procedures. This resistance may stem from a lack of digital competences, fear of making mistakes in new systems, or insufficient motivation and support for engaging with technological innovation.

In crisis management, it is of the utmost importance to protect human life and health and to minimize property damage. In this case, an ability to make effective use of the available digital

tools by public administration staff responsible for crisis management should be an absolute requirement. However, recognition of relevant qualifications should not be based solely on documentation related to the completion of relevant training and courses but on ongoing monitoring of skills. This is important given the speed of the development of digital tools and changes in the security environment. Lack of appropriate skills as regards those responsible for managing emergencies may result in threat signals not being perceived, or misinterpreted, in a timely manner.

Additionally, crisis management teams should include people who are skilled in designing and implementing information systems which are integrated with social media monitoring and analysis systems. This allows crisis management to be not only reactive but also proactive in its nature. This may also help minimize risks associated with external interference with the systems in use, as outsourcing of IT processes and data analytics requires a transfer of sensitive information and data to third parties, which involves the risk of data leaks and potential cyber-attacks. Furthermore, an integration of external systems with internal networks may create new attack vectors that can be exploited by cybercriminals.

In the context of crisis management, the experience of public administration staff in this area is also important; awareness of the unreliability of digital systems and tools should also be part of digital skills. Any IT system, regardless of its sophistication, is vulnerable to failure. In emergency situations, relying on these systems alone can pose serious risks to human life and health. It is therefore essential that emergency management systems have procedures in place to deal with digital system failures. These failures may result not only from a system error, a human error or cyber-attacks but also from power failures. This in turn can also be due to a number of factors that cannot be prevented. However, it is important to be prepared for these circumstances. An example of such a factor is the solar storm that caused a blackout in 1989 in the Canadian province of Quebec (Phillips, 2021).

In terms of crisis management, digital competence is particularly important in the case of cyber security incidents. Public administration is required to appoint a contact person with cyber competence to report public entity incidents to cyber security institutions and to handle them accordingly; these are those incident that cause or are likely to cause a reduction in the quality or interruption of the public task carried out by a public entity (Karpiuk, 2020, 61).

4 Conclusions and recommendations

In the context of crisis management, relevant digital competences of public administration employees are becoming increasingly important. Knowledge of and ability to use digital tools such as AI, big data or GIS enables effective coordination of activities and management of resources, which is crucial for a prompt and effective response to a crisis. In this respect, knowledge in the area of cyber security is also essential; this helps to ensure that data and systems are protected from potential cyber-attacks, which may not only disrupt the crisis management process but also cause further crises.

At the same time, in order to use digital tools effectively in practice, employees should continuously update their knowledge. Studies and research carried out indicate that lack of appropriate competences may lead to an inefficient use of the potential of digital tools, which has a negative impact on crisis management.

In summary, effective crisis management depends heavily on the level of preparedness on the part of public administration employees in terms of their digital competence. A two-dimensional

approach, encompassing both an ability to use digital tools effectively and awareness of cyber-security risks, is key to anticipating, monitoring and responding to dynamically changing challenges in the security environment.

Therefore, the research hypothesis, stating that there is a correlation between the level of digital competence of public administration employees and the effectiveness of crisis management has been positively verified. At the same time, in the case of crisis and emergency management, the dynamics of change in the security environment and the pace of the evolution of digital tools must be taken into account. This refers to the emergence of new forms of threats, such as cyber-attacks, which are becoming more sophisticated and more difficult to predict. And these developments may result from policies, technological innovations, as well as actions taken by hostile actors. For public administration, this means that they need to constantly monitor these threats and adapt their security strategies accordingly.

Based on an analysis of the impact of the rapid development of digital technologies and dynamic changes in the security environment on the ways in which crises are managed, recommendations can be made to public administration that may enhance the use of digital tools in this regard, such as:

- continuing education and training for crisis management personnel to help maintain a high level of preparedness and adaptation to rapidly changing technologies;
- strengthening cyber-security by investing in advanced cyber-security systems that can effectively counter new threats and ensure protection of critical infrastructure and data;
- creation of interdisciplinary crisis management teams, ones that include experts from different fields, including IT, security, communications and crisis management;
- developing partnerships and networks at the international level to share good practices, experiences and solutions in the field of crisis management;
- implementing advanced real-time monitoring systems that can detect early signals of threats and enable rapid response;
- use of predictive analytical tools and big data;
- regular reviews of existing crisis management procedures to identify areas for improvement or updating.

When implementing the recommendations proposed above, it is also important to take into account the possibility of risks that do not yet exist or have not yet occurred.

The digital skills of public administration employees are a derivative of the level of these skills in the entire society, which in turn depends on the level of education in a given country. At the same time, this level largely depends on the knowledge and skills of teachers. However, in the context of crisis management, the most important thing is the level of basic digital skills in a given society. In the countries of the European Union, the average level of basic digital skills is possessed by 54% of its citizens. However, this is internally diversified, with the highest values for Finland and the Netherlands and the lowest for Romania and Bulgaria (European Commission, 2023). At the same time, these skills are treated as a pillar of the state's resilience (European Commission, 2023).

It should also be noted that the level of digital skills in a given society directly implies the resistance of that society to disinformation. It is important that, in the event of a crisis, when immediate action by services is required, the possibility of access to their communication channels by outsiders can have serious consequences, and the consideration of whether the regulations have been broken is carried out only after the fact. It can be hypothetically assumed

that in the event of the immobilization (due to a failure, accident, external factors) of a transport of materials that can be used to produce explosives or dirty bombs, the emergency services will be redirected to another location. This gives the possibility of taking over these materials by criminals, terrorists, or saboteurs. Therefore, prevention and compliance with security procedures seem to be the most important. Even a one-time disregard of them by one person can have serious consequences for the entire crisis management system (Kaczmarek, 2023, 27–28).

Therefore, the appropriate level of digital skills of officials who are part of society is important not only in managing crisis situations, but above all in preventing them. On the other hand, too low a level of these skills means not only a lack of effective crisis management, but also the possibility of generating threats.

References

Budai, B. B., Csuhai, S., & Tózsa, I. (2023). Digital Competence Development in Public Administration Higher Education. *Sustainability*, 15(16), Article 12462. https://doi.org/10.3390/su151612462

Catakli, D. (2022). *Verwaltung im digitalen Zeitalter: Die Rolle digitaler Kompetenzen in der Personalakquise des höheren Dienstes*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-38958-1

Ćwik B. (2017). Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji. *Modern Management Review*, 24(3), 27–37. https://doi.org/10.7862/rz.2017.mmr.24

Czuryk, M. (2022). Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues. *Studia Iuridica Lublinensia*, 31(3), 31–43, https://doi.org/10.17951/sil.2022.31.3.31-43.

Czuryk, M., Dunaj, K., Karpiuk, M., & Prokop, K. (2016). *Prawo zarządzania kryzysowego. Zarys systemu*. UWM.

European Commission. (2019). *Key competences for lifelong learning*. Publications Office. https://doi.org/10.2766/569540

European Commission. (2023). *Report on the State of the Digital Decade 2023: Annex – All Member States*. Publications Office of the European Union. Online: https://ec.europa.eu/newsroom/dae/redirection/document/98669

Guo, H., Yang, Z., Huang, R., & Li, X. (2020). The digitalization and public crisis responses of small and medium enterprises: Implications from a COVID-19 survey. *Frontiers of Business Research in China*, 14, 19. https://doi.org/10.1186/s11782-020-00087-1

Hoffman, I., & Kostrubiec, J. (2022). Political Freedoms and Rights in Relation to the Covid-19 Pandemic in Poland and Hungary in a Comparative Legal Perspective. *Bialystok Legal Studies*, 27(2), 31–53. https://doi.org/10.15290/bsp.2022.27.02.02

Hulkó, G. (2021). Fake news és social media: szabályozás és közigazgatási intézkedések Szlovákiában [Fake news and social media: regulation and administrative measures in Slovakia]. *In Medias Res*, 10(2), 297–311. https://doi.org/10.59851/imr.10.2.7

Kaczmarek, K. (2023). Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych [Disinformation as a Risk Factor in Crisis Situations]. *Roczniki Nauk Społecznych*, 51(2), 19–30. https://doi.org/10.18290/rns2023.0017

Karpiuk, M. (2020). The obligations of public entities within the national cybersecurity system. *Cybersecurity and Law*, 4(2), 57–72. https://doi.org/10.35467/cal/133971

Karpiuk, M. (2021). Cybersecurity as an element in the planning activities of public administration. *Cybersecurity and Law*, 5(1), 45–52. https://doi.org/10.35467/cal/142179

Karpiuk, M. (2022). Crisis management vs. cyber threat. *Sicurezza, Terrorismo e Società*, 16(2), 113–123. Online: https://shorturl.at/9vcEw

Karpiuk, M., Pizło, W., & Kaczmarek, K. (2023). Cybersecurity Management – Current State and Directions of Change. *International Journal of Legal Studies*, 14(2), 645–663. https://doi.org/10.5604/01.3001.0054.2880

Kostrubiec, J. (2021). *Sztuczna inteligencja a prawa i wolności człowieka*. Instytut Wymiaru Sprawiedliwości. Online: https://shorturl.at/HDYbc

Leonard, H. B., Howitt, A. M., & Giles, D. W. (2020). *Crisis Management for Leaders Coping with COVID-19*. Program on Crisis Leadership, Harvard Kennedy School. Online: https://shorturl.at/0Qpic

Lopes, A. S., Sargento, A., & Farto, J. (2023). Training in digital skills—The perspective of workers in public sector. *Sustainability*, 15(13), Article 10577. https://doi.org/10.3390/su151310577

Łukaszuk, A. (2022). Problematyka kompetencji cyfrowych kadr administracji publicznej jako istotnego czynnika procesu transformacji cyfrowej jednostek samorządu terytorialnego w Polsce. *Studia Prawnoustrojowe*, 58, 287–313. https://doi.org/10.31648/sp.7985

OECD. (2021). *Public Employment and Management 2021: The Future of the Public Service.* OECD Publishing. https://doi.org/10.1787/938f0d65-en

Okpala, I., Halse, S., & Kropczynski, J. (2023). *Machine Learning Methods for Evaluating Public Crisis: Meta-Analysis*. 9th IEEE International Conference on Computational Science and Computational Intelligence (CSCI'2022), Las Vegas, NV, USA. https://doi.org/10.48550/arXiv.2302.02267

Olech, A. (2020). Fazy zarządzania kryzysowego w kontekście zagrożeń terrorystycznych. In K. Śmiałek (Ed.), *Zarządzanie kryzysowe wobec wyzwań i zagrożeń dla bezpieczeństwa wewnętrznego państwa* (pp. 95–109). Wojskowa Akademia Techniczna.

Phillips, T. (2021). *The Great Québec Blackout*. Online: https://spaceweatherarchive.com/2021/03/12/the-great-quebec-blackout/

Qadir, J., Ali, A., ur Rasool, R., Zwitter, A., Sathiaseelan, A., & Crowcroft, J. (2016). Crisis analytics: big data-driven crisis response. *Journal of International Humanitarian Action*, 1(12). https://doi.org/10.1186/s41018-016-0013-9

Radanliev, P., De Roure, D., & Van Kleek, M. (2020). *Digitalization of COVID-19 Pandemic Management and Cyber Risk from Connected Systems*. IEEE Internet of Things. https://doi.org/10.48550/arXiv.2005.12409

Szczurek, T. (2023). Resort obrony narodowej w systemie zarządzania kryzysowego [Ministry of National Defense in the Crisis Management System]. *Roczniki Nauk Społecznych*, 51(2), 7–18. https://doi.org/10.18290/rns2023.0020

Van der Wal, Z. (2020). Being a Public Manager in Times of Crisis: The Art of Managing Stakeholders, Political Masters, and Collaborative Networks. *Public Administration Review, 80*(5), 759–764. https://doi.org/10.1111/puar.13245

Verhoest, K., Hammerschmid, G., Rykka, L. H., & Klijn, E. H. (2024). *Collaborating for Digital Transformation. How Internal and External Collaboration Can Contribute to Innovate Public Service Delivery*. Edward Elgar Publishing. https://doi.org/10.4337/9781803923895

Włodyka E. M. (2024). Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce. In M. Karpiuk (Ed.), *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe* (pp. 104–123). Wydawnictwo Akademii Sztuki Wojennej.

Włodyka, E. M. (2022). Konsolidować, nie konsolidować… głos do dyskusji o połączeniu korpusu służby cywilnej i pracowników samorządowych. *Studia Iuridica*, 92, 179–196. https://doi.org/10.31338/2544-3135.si.2022-92.11