E-administracja

Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej

E-Government

Challenges for Digital Public Services in the EU

REDAKCJA / EDITED BY

Sławomir Dudzik · Inga Kawka · Renata Śliwa

Krakow Jean Monnet Research Papers

E-administracja

Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej

E-Government

Challenges for Digital Public Services in the EU

Krakow Jean Monnet Research Papers

3

E-administracja

Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej

E-Government

Challenges for Digital Public Services in the EU

REDAKCJA / EDITED BY

Sławomir Dudzik · Inga Kawka · Renata Śliwa

WYDAWNICTWO
KSIĘGARNIA AKADEMICKA
Sp. z o.o.
Kraków

Kraków 2024

Sławomir Dudzik
Uniwersytet Jagielloński, Kraków
✉ s.dudzik@uj.edu.pl

Inga Kawka
Uniwersytet Jagielloński, Kraków
✉ inga.kawka@uj.edu.pl

Renata Śliwa
Uniwersytet Komisji Edukacji Narodowej, Kraków
✉ renata.sliwa@up.krakow.pl

Recenzja: dr hab. Grzegorz Krawiec, prof. UKEN

Opracowanie redakcyjne: Artur Foryt (j. francuski), Dorota Ilnicka (j. polski), Christopher Thornton (j. angielski)

Projekt okładki: Marta Jaszczuk

ISBN 978-83-8368-025-5
https://doi.org/10.12797/9788383680255

Publikacja dofinansowana przez Wydział Prawa i Administracji Uniwersytetu Jagiellońskiego oraz Uniwersytet Komisji Edukacji Narodowej w Krakowie

With the support of Jean Monnet Activities within ERASMUS+ Programme of the European Union

Projekt współfinansowany w
ramach programu Unii Europejskiej
Erasmus+

Wsparcie Komisji Europejskiej dla produkcji tej publikacji nie stanowi poparcia dla treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie może zostać pociągnięta do odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

WYDAWNICTWO KSIĘGARNIA AKADEMICKA
ul. św. Anny 6, 31-008 Kraków
tel.: 12 421-13-87; 12 431-27-43
e-mail: publishing@akademicka.pl

Księgarnia internetowa: akademicka.pl

Spis treści | Table of contents

Część III / PART III
Perspektywy rozwoju cyfrowych usług publicznych w Europie / Prospects for the Development of Digital Public Services in Europe

Część IV / Part IV
Wyzwania dla rozwoju e-usług publicznych w Polsce / Challenges in the Development of Public e-Services in Poland

E-administracja. Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej
E-Government: Challenges for Digital Public Services in the EU | s. 171-188
https://doi.org/10.12797/9788383680255.09

Iryna Fyshchuk[1]

Strengthening Municipalities' Resilience against Cyber Attacks in Ukraine

Abstract: A full-scale war was preceded by cyberattacks on the websites of public authorities in Ukraine in the spring of 2022. Joint efforts between IT professionals from the public and private sectors have produced positive experience and resilience in resisting cyberattacks. Ukraine's ongoing decentralization process created new administrative-territorial system, where municipalities acquired more functions and responsibilities. This transformational period involves a weaker governance structure that is highly vulnerable to cyberattacks. Strengthening municipalities' resilience in Ukraine during the ongoing war refers to the ability of a community to manage itself with cyberattack challenges and to overcome change and crisis. The resilience of a municipality should be to understand, and capacity to respond against cyberattacks and describe institutional structures should be developed at the local level. Leadership is one of the key elements of municipal resilience at the local level. Furthermore, Ukraine's accession to the Digital Europe 2027 Programme could potentially provide municipalities with better funding for cybersecurity implementation and move closer to EU standards. The Digital Europe Programme is available through other EU programs, such as Connecting Europe Facility for digital infrastructure and the Recovery and Resilience Facility, to which Ukrainian municipalities will be able to apply.

Keywords: municipalities, resilience, cyberattacks, cybersecurity, digitalization, decentralization, public administration

[1] Iryna Fyshchuk, Scholar at Risk Fellow, Associate Professor, University of Agder, Department of Political Science and Management, Norway, https://orcid.org/0000-0002-7645-3490.

Wzmacnianie odporności gmin na ataki cybernetyczne na Ukrainie

Abstrakt: Wojnę na pełną skalę poprzedziły cyberataki na strony internetowe władz publicznych na Ukrainie, z którymi wiosną 2022 r. zetknęły się gminy. Wspólne wysiłki specjalistów IT z sektorów publicznego i prywatnego przyniosły pozytywne doświadczenia i podniosły odporność w zakresie przeciwstawiania się cyberatakom. Trwający proces decentralizacji Ukrainy stworzył nowy system administracyjny i terytorialny, w którym gminy otrzymały więcej funkcji i obowiązków. Ten okres transformacji wiąże się ze słabszą strukturą zarządzania, bardzo podatną na cyberataki. Wzmocnienie odporności gmin na Ukrainie podczas trwającej wojny odnosi się do zdolności społeczności do radzenia sobie z wyzwaniami związanymi z atakami cybernetycznymi oraz do przezwyciężania trudności wynikających ze zmian i kryzysu. Odporność gminy powinna polegać na zrozumieniu i rozwinięciu na poziomie lokalnym zdolności do reagowania na cyberataki oraz opisaniu zajmujących się cyberbezpieczeńtwem struktur instytucjonalnych. Przywództwo jest jednym z kluczowych elementów odporności gmin na poziomie lokalnym. Ponadto przystąpienie Ukrainy do programu „Cyfrowa Europa 2027" mogłoby potencjalnie zapewnić gminom lepsze finansowanie wdrażania cyberbezpieczeństwa i zbliżenie się do standardów UE w tym zakresie. Program „Cyfrowa Europa" jest dostępny za pośrednictwem innych programów UE, takich jak instrument „Łącząc Europę", dotyczący infrastruktury cyfrowej, oraz Instrument na rzecz odbudowy i zwiększania odporności. O środki z tych programów będą mogły ubiegać się ukraińskie gminy.

Słowa kluczowe: gminy, odporność, cyberataki, cyberbezpieczeństwo, cyfryzacja, decentralizacja, administracja publiczna

1. Introduction

Rapid development information and telecommunication technologies and the rising dependence on these systems has led to increased risks for these infrastructures,[2] including cyber attacks, as numerous examples have shown.[3] The Ukrainian case is not an exception, but attention is even more intensified at the moment, since the country is undergoing war and cyber attacks are becoming more frequent, especially on the

[2] M. Baram, *Resilience and Essential Public Infrastructure* [in:] *Exploring Resilience. A Scientific Journey from Practice to Theory*, S. Wiig, B. Fahlbruch (eds), Cham 2019, pp. 33-40.

[3] B. W. Wirtz, J. C. Weyerer, *Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats*, "International Journal of Public Administration" 2017, vol. 40, no. 13, pp. 1085-1100.

websites of municipal authorities, as they have less funding and therefore less attention and protection, which poses a threat to the resilience of communities.[4]

Cyber attacks are a type of terror attacks, as they are directed against public authorities or private companies and concerned with obtaining sensitive information; disclosing and threatening publication, or self-publication. of information about the functioning of the information infrastructure of the state; the capture of mass media channels for the purpose of misinformation dissemination and to gain access to the administrative rights of the company that administers the sites.[5] For example, during 13-14 January there was a global hacker attack on Ukrainian government websites. The websites of the Ministry of Education and Science, the Ministry of Foreign Affairs, the State Emergency Service, the Cabinet of Ministers, the Ministry of Energy and "Diya" (a mobile application developed by the Ministry of Digital Transformation of Ukraine for Ukrainian citizens) were not working. The attack presented a step towards the imminent Russian invasion on February 24.

Destructive attacks are a component of Russian wartime cyberoperations. Cyberattacks continue and threaten the well-being of the civilian population. The combination of cyber-physical attack was aimed at disrupting the functioning of the Ukrainian government and the army, undermining the public's faith in these institutions, damaging objects of critical infrastructure and causing irreversible catastrophic consequences.

Decentralization of public authorities is a mechanism that ensures the sustainable development of regions of the state on the basis of the legislative and regulatory transfer of functions, powers and budgets from the central executive bodies to local self-government.[6] The development of the state and the decentralization situation is a transfer of powers and resources to lower levels of public administration. In addition, decentralization stands out as one of the forms of the development of democracy, which allows the state and its institutions to expand local self-government. Also, decentralization allows to activate the population to make decisions and implement them for their own needs and interests. Furthermore, decentralization narrows the sphere of influence of the state on society, replacing it by self-regulation mechanisms

[4] A. Duit, *Resilience Thinking: Lessons for Public Administration*, "Public Administration" 2016, vol. 94, no. 2, pp. 364-380.

[5] R. V. Bondarenko, *Кібератаки як одна з форм кібертероризму* [*Cyberattacks as a Form of Cyber Terrorism*], "Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки" 2021, Том 32 (71), Ч. 1, № 1. 2021, С. 45-50.

[6] В. П. Гордієнко, М. Л. Оніщенко, І. С. Мальонкіна, *Зарубіжний досвід децентралізації публічної влади та можливості його трансформації в Україні*, "Вісник Сумського державного університету. Серія Економіка" 2019, № 3, С. 83-89.

developed by society itself, which reduces the expenses of the state and taxpayers for the maintenance of the state apparatus.

A review of the literature proves that significant scientific interest researchers study various aspects of decentralization of the modern state, the challenges and problems of the decentralization processes and administrative and territorial reform. R. Rhodes and M. Bevir have determined the general methodological principles of the theory of decentralization by proposing the "distinctive interpretive theory."[7] Some scientists mentioned that successful implementation of decentralization depends on strengthening the potential of local bodies power and the government's capacity for assistance and support for decentralization.[8] It is important that local authorities and communities make the most of their territorial features even if they are unfavorable.[9]

2. Resilience in municipalities and organizational difficulties

Resilience is very multidisciplinary, and each discipline has put forward its own definitions and central bibliographic references. Regarding methodological approaches, case studies received the highest rating and surveys were given the least preference: "as a resilience-based research area has developed, the focus is becoming more empirically focused," and there is a wide space for theoretical developments.

Over the past decades, resilience has been defined and used in different ways and in several scientific and practical fields. The term derives from the Latin verb *salire* (to climb or jump) and in particular from its extension, *resilire*, meaning to jump back or recoil.[10] Resilience thinking refers to the study of complex, interconnected and new models of relations between subjects and their respective subjects.[11] Bhamra states that "regardless of context, the concept of sustainability is about achieving stability in the functioning of an element or system."[12] Table 1 shows the definitions of resilience

[7] H. Wagenaar, *Meaning in Action: Interpretation and Dialogue in Policy Analysis*, London–New York 2014.

[8] C. Dyer, P. Rose, *Decentralisation for Educational Development? An Editorial Introduction*, "Compare" 2005, vol. 35, no. 2, pp. 105-113.

[9] O. Mikuš, M. Kukoč, M. Jež Rogelj, *The Coherence of Common Policies of the EU in Territorial Cohesion: A Neverending Discourse? A Review*, "Agricultural Economics" 2019, no. 65, pp. 143-149, https://agricecon.agriculturejournals.cz/artkey/age-201903-0005_the-coherence-of-common--policies-of-the-eu-in-territorial-cohesion-a-never-ending-discourse-a-review (12.10.2023).

[10] A. Zolli, A. M. Healy, *Resilience: Why Things Bounce Back*, New York 2012.

[11] K. Grove, *Resilience*, New York 2018.

[12] R. Bhamra, *Organisational Resilience: Concepts, Integration, and Practice*, Boca Raton 2016, p. 18.

from different perspectives – individual, organizational, sociotechnical systems and multilevel governance.

Table 1. Definitions of Resilience

Author	Context	Definition
Coutu[13]	Individual	Resilient individuals possess three common characteristics: an acceptance of reality, a strong belief that life is meaningful and the ability to improvise.
McDonald[14]	Organizational	Adapting to the requirements of the environment and being able to manage the environment's variability
Schaffer and Schneider[15]	Sociotechnical systems	Protect a system's integrity by strengthening links to other systems and tolerating or even fostering structural changes
European Commission (2019)[16]	Multilevel governance	The ability to face shocks and persistent structural changes in such a way that social well-being is preserved without compromising the heritage of future generations

Source: Own elaboration.

In recent years, resilience has been the subject of numerous studies, and a quick search on Google Scholar showed a large number of references, about 294,000, on "municipality resilience," which means that there is a great demand for studying and analyzing ways of resilience in society. Scholars within the fields of environmental studies, science and psychiatry were rather prominent (Table 2).

[13] D. L. Coutu, *How Resilience Works*, "Harvard Business Review" 2002, vol. 80, no. 5, pp. 46-56.

[14] N. McDonald, *Organisational Resilience and Industrial Risk* [in:] *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. D. Woods, N. Leveson (eds), Aldershot 2006, pp. 155-179.

[15] A. Schaffer, M. Schneider, *Towards a Responsible Resilience* [in:] *Handbook on Resilience of Sociotechnical Systems*, M. Ruth, S. Goessling-Reisemann (eds), Cheltenham 2019, pp. 9-29.

[16] European Commission, *Resilience*, 2019, https://ec.europa.eu/jrc/en/research/crosscutting--activities/resilience (12.10.2023).

Table 2. Resilience papers (title) by disciplinary domain

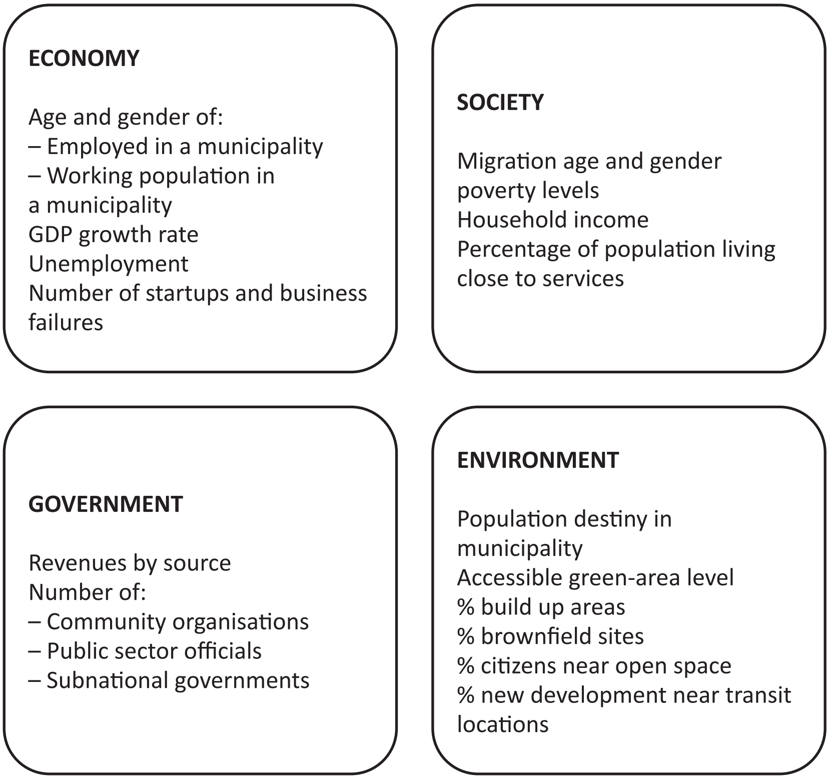
Psychiatry – 1,914	Environmental studies – 1,354	Engineering electrical electronic – 950	Ecology – 914
	Public, environmental occupational, health – 1,175	Neurosciences – 809	Clinical psychology – 663
Environmental sciences – 1,446	Psychology, multidisciplinary – 1,151	Water resources – 732	

Source: elaborated based on M. L. Frigotto, M. Young, R. Pinheiro, *Resilience in Organizations and Societies: The State of the Art and Three Organizing Principles for Moving Forward* [in:] *Towards Resilient Organizations and Societies A Cross-Sectoral and Multi-Disciplinary Perspective*, R. Pinheiro, M. L. Frigotto, M. Young (eds), Cham 2022, pp. 3-40.

There is no clear solution in the literature regarding ways to strengthen community resilience. The paucity of empirical research and the diversity of disciplines involved hinder and complicate the development and understanding of ways to enhance municipality resilience. At the same time, the general opinion is that after determining the components of the municipality's resilience, their improvement will lead to the development of its potential. Measuring resilience in a municipality can include four pillars (Picture 1):

- Economy, which will analyse the age and gender of employed people in a municipality and the working population in a municipality, GDP growth rate in a municipality, unemployment, number of startups and business failures;
- Society, where migration age and gender poverty levels will be reviewed – household income and percentage of population living close to services;
- Government, where the analysis will be carried out according to the revenues by source, number of community organisations and public sector officials;
- Environment, where population destiny in a municipality will be analysed, accessible green-area level, percentage of buildup areas, percentage of brownfield sites, percentage of citizens near open space and percentage of new development near transit locations.

Picture 1. Measuring resilience in a municipality



ECONOMY

Age and gender of:
– Employed in a municipality
– Working population in a municipality
GDP growth rate
Unemployment
Number of startups and business failures

SOCIETY

Migration age and gender
poverty levels
Household income
Percentage of population living close to services

GOVERNMENT

Revenues by source
Number of:
– Community organisations
– Public sector officials
– Subnational governments

ENVIRONMENT

Population destiny in municipality
Accessible green-area level
% build up areas
% brownfield sites
% citizens near open space
% new development near transit locations

Source: Own elaboration.

The concept of community resilience is discussed at many levels.[17] According to Canyon,[18] the focus of increasing resilience to change should be to understand and develop capacity at the local level to adapt, respond and describe institutional structures. One of the key elements of community resilience at the local level is leadership.[19]

[17] G.A. Wilson, *Community Resilience, Globalization, and Transitional Pathways of Decision-Making*, "Geoforum" 2012, vol. 43, no. 6, pp. 1218-1231.

[18] D. V. Canyon, F. M. Burkle, R. Speare, *Managing Community Resilience to Climate Extremes, Rapid Unsustainable Urbanization, Emergencies of Scarcity, and Biodiversity Crises by Use of a Disaster Risk Reduction Bank*, "Disaster Medicine and Public Health Preparedness" 2015, vol. 9, no. 6, pp. 619-624.

[19] O. Cohen et al., *Community Resilience, Globalization, and Transitional Pathways of Decision-making*, "Technological Forecasting and Social Change" 2017, vol. 121, August, pp. 119-125.

In recent years resilience, which generally refers to a system's ability to withstand stresses and shocks, has been widely adopted by international and national organizations as an imperative policy and very important element. It seems that every system, every organization, and municipalities in particular, can and should be resilient, with an extension to research on municipality resilience, particularly as it relates to understanding those factors that enable proactive community responses to change. Community resilience is often defined in terms of physical infrastructure, economic resources, and community capacities and capabilities necessary to respond adversity.[20]

In a broader context, some organizations have described resilient communities as having taken "intentional action to enhance the personal collective capacity of its citizens and institutions to respond to, and influence the course of social and economic change."[21] They contend that communities must develop their capacity to respond to adversity in ways that draw upon those internal resources and competencies needed to manage changes.[22] Tobin[23] further elaborates on this theme and suggests several practical steps that communities might pursue to secure greater resilience capacity. These include:

- Reducing exposure to geophysical events through structural and nonstructural measures;
- Reducing the vulnerability of all members of the community, especially those politically or economically marginalized;
- Ensuring that commitments to long-term sustainability goals stay at the forefront of all community planning efforts;
- Ensuring that high-level support and political "buy-in" and cooperative arrangements are in place with agencies and political leaders, embracing partnerships and cooperation across the various levels of government and organizations.

Resilience tends to arise when smaller municipalities cooperate and benefit from scaling up through the costs of „shared" services, and when governance arrangements

[20] D. Paton, D. Johnson, *Disasters and Communities: Vulnerability, Resilience and Preparedness*, "Disaster Prevention and Management" 2011, vol. 10, no. 4, pp. 270-277.

[21] Centre for Community Enterprise (CCE), *The Community Resilience Manual: A Resource for Rural Recovery and Renewal*, 2000, http://communityrenewal.ca/sites/all/files/resource/P200_0.pdf (12.10.2023).

[22] V. A. Sheppard, P. W. Williams, *Factors that Strengthen Tourism Resort Resilience*, "Journal of Hospitality and Tourism Management" 2016, vol. 28, September, pp. 20-30.

[23] G. A. Tobin, *Sustainability and Community Resilience: The Holy Grail of Hazards*, "Global Environmental Change. Part B: Environmental Hazards" 1999, vol. 1, no. 1, pp. 13-25.

minimize problems.[24] Three main mechanisms are suggested below, where the first relates to operating size, where many studies suggest that larger organizations withstand disruptions better than smaller entities.[25]

The second mechanism is related to balancing the difficulties that different participants of the intermunicipal partnership experience unevenly. Kahn et al.[26] argued that in large multi-departmental organisations the same difficulties may not be equally felt in different parts, meaning that less affected departments can share the burden by reallocating resources to "hot spots." The same argument applies even more to interorganizational cooperation, as variation in the degree of distress experienced and mitigation capacity will be even greater between organizations than within an organization.

A third mechanism is related to the commitment effect, a type of "lock-in"[27] that occurs when organizations adopt quasi-contractual agreements. Fearful of shirking or abandoning others,[28] intermunicipal partners establish governance mechanisms that seek to overcome commitment issues, reducing the potential for "poaching" and reallocation of resources for other purposes.

3. Peculiarities of cybersecurity in municipalities in Ukraine

According to the Digital Agenda for Ukraine, adopted in 2018, the government and the State Agency for the eGovernance of Ukraine laid the groundwork for the future. It was the main strategic document providing the direction for the Ukrainian government and the country's economic development. The Digital Agenda for Ukraine consists of seven main pillars, such as: (1) telecommunications and ICT infrastructure; (2) digital skills; (3) eMarket; (4) digital governance; (5) innovation and R&D; (6) trust and cybersecurity; and (7) benefits from ICT for society and economy.

[24] T. Elston, G. Bel, *Does Inter-Municipal Collaboration Improve Public Service Resilience? Evidence from Local Authorities in England*, "Public Management Review" 2023, vol. 25, no. 4, pp. 734-761.

[25] M. K. Linnenluecke, *Resilience in Business and Management Research: A Review of Influential Publications and A Research Agenda*, "International Journal of Management Reviews" 2017, vol. 19, no. 1, pp. 4-30.

[26] W. A. Kahn et al., *The Geography of Strain: Organizational Resilience as a Function of Intergroup Relations*, "Academy of Management Review" 2018, vol. 43, no. 3, pp. 509-529.

[27] F. Law, *Breaking the Outsourcing Path: Backsourcing Process and Outsourcing Lock-in*, "European Management Journal" 2018, vol. 36, no. 3, pp. 341-352.

[28] R. C. Feiock, *The Institutional Collective Action Framework*, "Policy Studies Journal" 2013, vol. 41, no. 3, pp. 397-425.

The trust and cybersecurity pillar lays down actions that can help to modernise Ukraine's national cybersecurity system, which can prevent cyberattacks in municipalities in Ukraine. The pillar includes, among others, the development of a frontline system against cyberthreats and technical vulnerabilities, enhancing protection from cyberthreats and the provision of learning courses on cybersecurity.[29]

The "Cybersecurity" online course was created on the Zrozmilo platform, where municipalities can be engaged in training to improve their digital literacy.[30] The course is aimed at representatives of the public sector, especially representatives from municipalities, which provides an opportunity to strengthen personal and corporate cybersecurity and teach participants learn how to work correctly with your own gadgets, namely, to set up privacy and take security rules into account, as well as to be able to communicate without mobile phone networks and the Internet.

The structure of the course includes 10 lectures with practical tasks:

Lecture 1: Introduction. What is the course about?

Series 2: Auditing cybersecurity and personal data in Google accounts.

Series 3: Audit of cybersecurity and personal data in Facebook accounts.

Series 4: What are password managers and how can they be used?

Series 5: What should be paid attention to when choosing a messenger? Communication in Viber and Telegram.

Series 6: Communication on WhatsApp and Signal.

Series 7: Communicating in the absence of a cellular connection.

Series 8: Encrypting important documents.

Series 9: Backing up important documents.

Series 10: Protecting documents from online fraudsters.

On 5 September 2022, Ukraine joined the Digital Europe Programme 2027, which potentially provides municipalities with better funding to implement recommendations for cyber protection.[31] The Digital Europe Programme (DIGITAL) is a new EU-funded programme focused on bringing digital technology to businesses, citizens and public administrations. It means that Ukrainian municipalities can integrate their digital possibilities according to EU standards.

[29] *Digital Public Administration Factsheet: 2022, Ukraine*, https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_Ukraine_vFinal.pdf (12.10.2023).

[30] *Кібербезпека для ГО*, https://courses.zrozumilo.in.ua/courses/course-v1:eef+EEF--034+March2023/about (12.10.2023).

[31] European Commission, *The Digital Europe Programme*, https://digital-strategy.ec.europa.eu/en/activities/digital-programme (12.10.2023).

According to the Digital Europe Programme, the strategic funding will provide support in different five key projects, such as:

- Supercomputing,
- Artificial intelligence,
- Cybersecurity,
- Advanced digital skills,
- Ensuring wide use of digital technologies across the economy and society, including through digital innovation hubs.

Moreover, a planned budget of €7.5 billion (in current prices) aims to accelerate economic recovery and shape the digital transformation of Europe's society and economy, bringing benefits to everyone, but in particular to small and medium-sized enterprises. In addition, the Digital Europe Programme will not address these challenges in isolation, but rather complement the funding available through other EU programmes, such as the Horizon Europe programme for research and innovation, and the Connecting Europe Facility for digital infrastructure, the Recovery and Resilience Facility and the Structural Funds. Furthermore, it is a part of the next long-term EU budget and the Multiannual Financial Framework for 2021-2027, for which Ukrainian municipalities can apply.

In particular, the Ministry of Digital Transformation of Ukraine, in cooperation with ULEAD with Europe. started to conduct a series of digitalization events in an open format within the framework of the Smart Regions Community. This is a new initiative designed to coordinate digital transformation in the regions and in the municipalities, especially to share experiences, solve problematic issues, present digital products, and develop competencies. The plan of joint activities of the Ministry of Digital Transformation and "ULEAD with Europe" includes:

- Digital Community Leader: People driving digital transformation at a local level.
- How to plan digital transformations in municipalities?
- Open data: how to conduct an open data audit in municipalities?
- Design of digital services: needs, solutions, piloting.
- Cybersecurity. how to ensure data protection in municipalities?

On February 8, 2023, the following cybersecurity trainings were held in the Kozyn hromada of the Rivne region.[32] Officials and the administrative staff of the municipality received information about cyber hygiene and the importance of the safe use of the Internet. The following information was provided during the training: protection of

[32] *Кібербезпека: пам›ятки, інструкції, рекомендації*, https://kozynska-gromada.gov.ua/kiberbezpeka-pamyatki-instrukcii-rekomendacii-14-30-02-10-03-2022/.

online accounts and use of complex passwords that consist of upper- and lowercase letters, numbers and symbols. The issue of using the same password for multiple accounts was also discussed. It was proposed to set up two-factor authentication everywhere possible and then to log in to the account, in addition to the login and password to enter the confirmation code that comes by phone, email or corresponding application. It was noted that citizens shouldn't follow dubious hyperlinks because they can hide a phishing resource. Phishing requires attackers to obtain valuable data, including bank card details. Officials and the administrative staff were advised to download software and applications only from official sources, to use antivirus software, update their operating system on time and make backup copies in order not to lose important information.

"From February 24, 2022 to February 23, 2023, the team manually investigated 1,880 such incidents of cyber attacks. More than a quarter of them are attacks on local authorities and government organizations. Also, energy, the security and defense sector, telecommunications and software development, the financial sector, and logistics are among the industries that are most often targeted by cyberattacks," said Volodymyr Kondrashov, spokesman for the State Special Forces of Ukraine.[33]

In Ukraine there are cyberattacks on the official information resources of various municipalities. At the end of May 2023 a major failure occurred on the websites of the municipalities of the Uman region, located in the Cherkasy region in central Ukraine. The sites were not available to users or the owners and administrators themselves. Thus, on 25 May 2023, the websites of the following municipalities did not work: Ivankivska, Babanskaya, Butska, Dmitrushkivska, Zhashkivska, Ladyzhynska, Mankivska, Monastyryshchenska, Palanska, Khrystynivska. There was also no access to the website of the Uman District State Administration and the Uman District Council.[34] Hackers had launched a DDoS attack on the server.

A DDoS attack means sending attackers large volumes of traffic or data through the target network until the network is overloaded ("denial of service"). Typically, a DDoS attack grows through a single computer or the single central location of computers. A popular category of DDoS attack is distributed denial of service (DDoS

[33] *Понад чверть кібератак були спрямовані проти українського уряду та органів місцевої влади,* 23.02.2023, https://www.ukrinform.ua/rubric-ato/3674096-ponad-cvert-kiberatak-buli--spramovani-proti-ukrainskogo-uradu-ta-miscevih-organiv-vladi.html.

[34] *Віртуальна шкода за поразки на фронті: триває кібератака на офіційні сайти громад Уманського районуб*, 25.05.2023, https://umannews.city/articles/289379/virtualna-shkoda-za--porazki-na-fronti-trivaye-kiberataka-na-oficijni-sajti-gromad-umanskogo-rajonu.

attack), which differs from a typical DDoS attack by the number of computers involved. These computers work together over the Internet to transmit traffic to target networks.[35]

There are two options for organizing DDoS attacks:

- Botnet – infection of a certain number of computer programs that at a certain moment start making requests to the attacked server;
- Flash mob – agreement of a large number Internet users to begin to make certain types of requests to the attacked server.[36]

On May 14, 2023, Vitaliy Nemerets, head of the Kakhov city military administration of the Kherson region, located in the south of Ukraine, announced on his Facebook page that the official account of the municipality had been hacked. On May 14, 2023, Vitaliy Nemerets, the head of the Kakhov city military administration of the Kherson region, also located in the south of Ukraine, announced on his Facebook page that the official account of the municipality had been hacked. As Nemerets noted, the hackers took possession of only public information, and there is no important, secret information there. The danger lies primarily in the fact that, on behalf of the hacked page, messages about illegal fundraising or information discrediting certain individuals, or the administration itself, may have been received.[37]

In April 2022, the Sandworm hackers, allegedly a Russian cyber-military unit, attacked the company Vinnytsiaoblenergo, located in the Vinnytsia region, and tried to leave 1.5-2 million citizens without electricity. However, Ukrainian cyber actors successfully warded off this attack. Since then, Ukraine has repelled the enemy and holds the cyber front.[38] In the same period, the head of the Vinnytsia regional administration, Serhii Borzov, noted that cyberattacks were carried out on the websites of regional state administrations and municipalities of the region. Borzov noted that computer algorithms have learned to "revive" photos, synthesize a person's voice and replace a face in a certain video.

During 2022 there were also challenges regarding cyberattacks that took place in the municipalities of Rivne, located in the west of Ukraine, official Ivanyshyn noted.

[35] Р. В. Бараненко, А. Ю. Задорожна, *Аналіз методів протидії кібератакам*, "Юридичний бюлетень" 2018, № 6, С. 148-161.

[36] В. В. Торяник, А. Ю. Чмирь, *Актуальність проблеми атаки на відмову в обслуговуванні. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: матеріали Міжнар. наук.-практ. конф.*, м. Харків, 12 листоп. 2014 р., МВС України, Харків. нац. ун-т внутр. справ. Харків: Права людини, 2014.

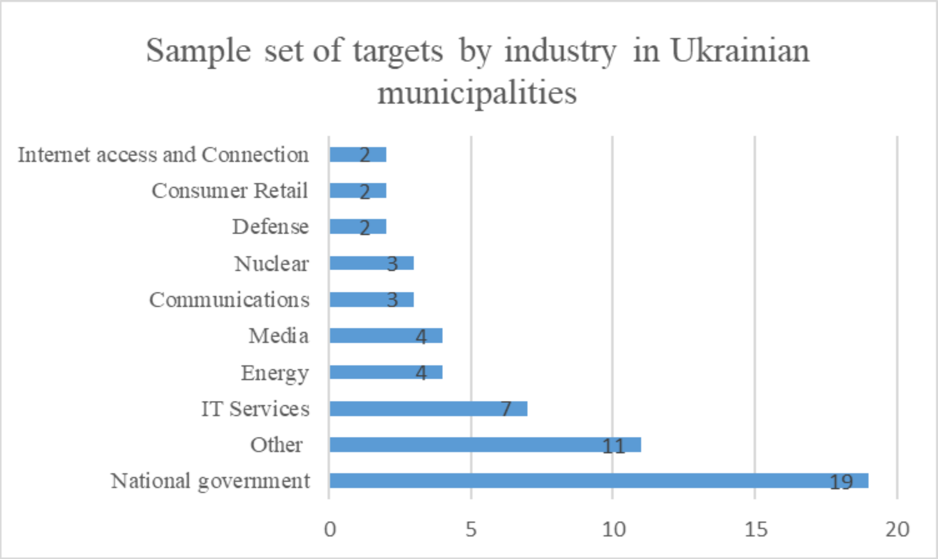
[37] *Сторінка Каховської громади в фейсбуці зазнала кібератаки*, 14.05.2023, https://novakahovka.city/articles/286868/storinka-kahovskoi-gromadi-v-fejsbuci-zaznala-kiberataki.

[38] В. Скрипін, *Росія готує масовані кібератаки на енергосистему України, Польщі та країн Балтії*, 26.09.2022, itc.ua/ua/novini/rosiya-kiberataki-na-energosistemu-ukrayini/ (12.10.2023).

As for cyberattacks carried out on the website of the Rivne Council in early spring 2022,[39] these had mostly psychological content.

It is worth noting that during the spring of 2022, due to the full-scale war in Ukraine, 13 centers for the provision of administrative services (TSNAPs) – Kyiv, Chernihiv, Zhytomyr and the Sumy regions – were left with destroyed premises and without equipment. The Swedish-Ukrainian PROSTO Project "Supporting the availability of services in Ukraine" purchased and handed over to the municipalities the most necessary sets of equipment for TSNAPs in the amount of 780,000 hryvnias at the request of the Ministry of Digital Transformation.[40]

Picture 2. Sample set of targets by industry in Ukrainian municipalities



Source: Microsoft. Digital Security Unit, *Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine*, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd ((12.10.2023)).

[39] *Цифровізація Рівного у період повномасштабної війни: ситуація і тенденції*, 2.11.2022, https://decentralization.gov.ua/news/15705 (12.10.2023).

[40] Ministerstvo ta Komitet tsyfrovoyi transformatsiyi Ukrayiny, *U deokupovanykh hromadakh z'yavyt'sya dostup do derzhposluh*, 26 travnya 2022 roku [Ministry and Committee for Digital Transformation of Ukraine, *Access to Public Services Will Be Available in Deoccupied Communities*, May 26, 2022], https://thedigital.gov.ua/news/u-deokupovanikh-gromadakh-zyavitsya-dostup--do-derzhposlug (12.10.2023).

In particular, this a list of a sample of Ukrainian industries affected by cyber attacks during the Russian invasion of Ukraine. The main targets were national government organizations and critical infrastructure sectors in municipalities. The "Other" percentage represents 11 other categories of victims' organizations, including regional and city authorities, agriculture, the defense-industrial base, health care, transport and finance, and many others (Picture 2).

4. Conclusion

Cooperation between municipalities may strengthen resilience and improve cybersecurity at the local level as the servant will have more information and communication possibilities with other employees. Conducting a series of digitization trainings as the Smart Regions Community in municipalities with an emphasis on cybersecurity will help improve digital skills and reduce the number of cyberattacks. Nowadays it is very important to reflect on the privacy risk, induced by digital activities, and gain awareness on how to protect themselves against: data theft, profiling, tracing. In addition, it is worth it to have a basic theoretical understanding of the evolution of emerging technologies and the impact this could have on cybersecurity in general. Building a simplified personal cyber-safety action plan, starting from assets identification to threats and vulnerabilities, to solutions and implementation for the public servants may be a solution to prevent a cyberattack.

An active leadership position between public and private servants proved the minimization of cyberattacks in different regions in Ukraine during spring 2022. So, appointment of a digital community leader in municipalities may deepen the driving digital transformation at local levels, and public administration in general. Ukraine's participation in the Digital Europe program will provide support for projects on cybersecurity and advanced digital skills, and will also ensure the widespread use of digital technologies in municipalities, including through digital innovation centres.

Bibliography

Baram M., *Resilience and Essential Public Infrastructure* [in:] *Exploring Resilience: A Scientific Journey from Practice to Theory*, S. Wiig, B. Fahlbruch (eds), Cham 2019.

Baranenko R. V., Zadorožna A. Û., *Analìz metodìv protidìï kìberatakam*, "Ûridičnij bûlleten'" 2018, № 6 [Бараненко Р. В., Задорожна А. Ю., *Аналіз методів протидії кібератакам,* "Юридичний бюллетень" 2018, № 6].

Bhamra R., *Organisational Resilience: Concepts, Integration, and Practice*, Boca Raton 2016.

Bondarenko R. V., *Кібератаки як одна з форм кібертероризму* [*Cyberattacks as a Form of Cyber Terrorism*], "Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки" 2021, Том 32 (71), Ч. 1, № 1, https://doi.org/10.32838/2663-5941/2021.1-1/07.

Canyon D. V., Burkle F. M., Speare R., *Managing Community Resilience to Climate Extremes, Rapid Unsustainable Urbanization, Emergencies of Scarcity, and Biodiversity Crises by Use of a Disaster Risk Reduction Bank*, "Disaster Medicine and Public Health Preparedness" 2015, vol. 9, no. 6, https://doi.org/10.1017/dmp.2015.124.

Castleden M. et al., *Resilience Thinking in Health Protection*, "Journal of Public Health" 2011, vol. 33, no. 3, https://doi.org/10.1093/pubmed/fdr027.

Centre for Community Enterprise (CCE), *The Community Resilience Manual: A Resource for Rural Recovery and Renewal*, 2000, http://communityrenewal.ca/sites/all/files/resource/P200_0.pdf.

Chandra A. et al., *Understanding Community Resilience in the Context of National Health Security: A Literature Review*, Santa Monica 2010, http://www.rand.org/pubs/working_papers/2010/RAND_WR737.pdf.

Cifrovìzacìâ Rìvnogo u perìod povnomasštabnoï vìjni: situacìâ ì tendencìï [*Цифровізація Рівного у період повномасштабної війни: ситуація і тенденції*], 2.11.2022, https://decentralization.gov.ua/news/15705.

Cohen O. et al., *Community Resilience, Globalization, and Transitional Pathways of Decision--Making*, "Technological Forecasting and Social Change" 2017, vol. 121, August.

Coutu D. L., *How Resilience Works*, "Harvard Business Review" 2002, vol. 80, no. 5.

Digital Public Administration Factsheet: *2022, Ukraine*, https://joinup.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_Ukraine_vFinal.pdf.

Duit A., *Resilience Thinking: Lessons for Public Administration*, "Public Administration" 2016, vol. 94, no. 2, https://doi.org/10.1111/padm.12182.

Dyer C., Rose P., *Decentralisation for Educational Development? An Editorial Introduction*, "Compare" 2005, vol. 35, no. 2, https://doi.org/10.1080/03057920500129809.

Elston T., Bel G., *Does Inter-Municipal Collaboration Improve Public Service Resilience? Evidence from Local Authorities in England*, "Public Management Review" 2023, vol. 25, no. 4, https://doi.org/10.1080/14719037.2021.2012377.

European Commission, *Resilience*, 2019, https://ec.europa.eu/jrc/en/research/crosscutting-activities/resilience.

European Commission, *The Digital Europe Programme*, https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

Feiock R. C., *The Institutional Collective Action Framework*, "Policy Studies Journal" 2013, vol. 41, no. 3, https://doi.org/10.1111/psj.12023.

Frigotto M. L., Young M., Pinheiro R., *Resilience in Organizations and Societies: The State of the Art and Three Organizing Principles for Moving Forward* [in:] *Towards Resilient Organizations and Societies: A Cross-Sectoral and Multi-Disciplinary Perspective*, R. Pinheiro, M. L. Frigotto, M. Young (eds), Cham 2022, https://doi.org/10.1007/978-3-030-82072-5_1.

Gordìênko V.P., Onìŝenko M.L., Mal'onkìna Ì.S., Zarubìžnij dosvìd decentralìzacìï publìčnoï vladi ta možlivostì jogo transformacìï v Ukraïnì, "Vìsnik Sums'kogo deržavnogo unìversitetu. Serìâ Ekonomìka" 2019, № 3 [*Гордієнко В.П., Оніщенко М.Л., Мальонкіна І.С., Зарубіжний досвід децентралізації публічної влади та можливості його* *трансформації в Україні,* "*Вісник Сумського державного університету. Серія Економіка*" 2019, № 3], https://doi.org/10.21272/1817-9215.2019.3-11.

Grove K., *Resilience*, New York 2018.

Kahn W. A. et al., *The Geography of Strain: Organizational Resilience as a Function of Intergroup Relations*, "Academy of Management Review" 2018, vol. 43, no. 3, https://doi.org/10.5465/amr.2016.0004.

Kìberbezpeka dlâ GO [*Кібербезпека для ГО*], https://courses.zrozumilo.in.ua/courses/course-v1:eef+EEF-034+March2023/about.

Kìberbezpeka: pam'âtki, ìnstrukcìï, rekomendacìï [*Кібербезпека: пам›ятки, інструкції, рекомендації*], https://kozynska-gromada.gov.ua/kiberbezpeka-pamyatki-instrukcii-rekomendacii-14-30-02-10-03-2022/.

Law F., *Breaking the Outsourcing Path: Backsourcing Process and Outsourcing Lock-in*, "European Management Journal" 2018, vol. 36, no. 3, https://doi.org/10.1016/j.emj.2017.05.004.

Linnenluecke M. K., *Resilience in Business and Management Research: A Review of Influential Publications and A Research Agenda*, "International Journal of Management Reviews" 2017, vol. 19, no. 1, https://doi.org/10.1111/ijmr.12076.

McDonald N., *Organisational Resilience and Industrial Risk*, [in:] *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. D. Woods, N. Leveson (eds.), Aldershot 2006.

Microsoft. Digital Security Unit, *Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine*, April 27, 2022, https://query.prod.cms.rt.microsoft.com/cms/ api/am/binary/RE4Vwwd.

Mikuš O., Kukoč M., Jež Rogelj M., *The Coherence of Common Policies of the EU in Territorial Cohesion: A Neverending Discourse? A Review*, "Agricultural Economics" 2019, no. 65, https://agricecon.agriculturejournals.cz/artkey/age-201903-0005_the-coherence-of--common-policies-of-the-eu-in-territorial-cohesion-a-never-ending-discourse-a--review.

Ministerstvo ta Komitet tsyfrovoyi transformatsiyi Ukrayiny, *U deokupovanykh hromadakh z'yavyt'sya dostup do derzhposluh*, 26 travnya 2022 roku. [Ministry and Committee for Digital Transformation of Ukraine, *Access to Public Services Will Be Available in Deoccupied Communities*, May 26, 2022], https://thedigital.gov.ua/news/u-deokupovanikh-gromadakh-zyavitsya-dostup-do-derzhposlug.

Patton D., Johnson D., *Disasters and Communities: Vulnerability, Resilience and Preparedness*, "Disaster Prevention and Management" 2011, vol. 10, no. 4, https://doi.org/10.1108/EUM0000000005930.

Ponad čvert' kìberatak buli sprâmovanì proti ukraïns'kogo urâdu ta organìv mìscevoï vladi [*Понад чверть кібератак були спрямовані проти українського уряду та органів місцевої влади*], 23.02.2023, https://www.ukrinform.ua/rubric-ato/3674096-ponad-cvert-kiberatak-buli-spramovani-proti-ukrainskogo-uradu-ta-miscevih-organiv-vladi.html.

Schaffer A., Schneider M., *Towards a Responsible Resilience*, [in:] *Handbook on Resilience of Socio-Technical Systems*, M. Ruth, S. Goessling-Reisemann (eds.), Cheltenham 2019.

Sheppard V.A., Williams P.W., *Factors That Strengthen Tourism Resort Resilience*, "Journal of Hospitality and Tourism Management" 2016, vol. 28, September, https://doi.org/10.1016/j.jhtm.2016.04.006.

Skripìn V., *Rosìâ gotuê masovanì kìberataki na energosistemu Ukraïni, Pol'šì ta kraïn Baltìï* [*Скрипін В., Росія готує масовані кібератаки на енергосистему України, Польщі та країн Балтії*], 26.09.2022, itc.ua/ua/novini/rosiya-kiberataki-na-energosistemu-ukrayini/.

Storìnka Kahovs'koï gromadi v fejsbucì zaznala kìberataki [*Сторінка Каховської громади в фейсбуці зазнала кібератаки*], 14.05.2023, https://novakahovka.city/articles/286868/storinka-kahovskoi-gromadi-v-fejsbuci-zaznala-kiberataki.

Tobin G.A., *Sustainability and Community Resilience: The Holy Grail of Hazards*, “Global Environmental Change. Part B: Environmental Hazards” 1999, vol. 1, no. 1, https://doi.org/10.1016/S1464-2867(99)00002-9.

Torânik V. V., Čmir' A. Û., *Aktual'nìst' problemi ataki na vìdmovu v obslugovuvannì. Aktual'nì pitannâ dìâl'nostì pravoohoronnih organìv u sferì protidìï kìberzločinnostì: materìali Mìžnar. nauk.-prakt. konf., m. Harkìv, 12 listop. 2014 r.*, MVS Ukraïni, Harkìv. nac. un-t vnutr. sprav. Harkìv: Prava lûdini, 2014 [*Торяник В. В., Чмирь А. Ю., Актуальність проблеми атаки на відмову в обслуговуванні. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: матеріали Міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р.*, МВС України, Харків. нац. ун-т внутр. справ. Харків: Права людини, 2014].

Vìrtual'na škoda za porazki na frontì: trivaê kìberataka na ofìcìjnì sajti gromad Umans'kogo rajonub [*Віртуальна шкода за поразки на фронті: триває кібератака на офіційні сайти громад Уманського районуб]*, 25.05.2023, https://umannews.city/articles/289379/virtualna-shkoda-za-porazki-na-fronti-trivaye-kiberataka-na-oficijni-sajti-gromad-umanskogo-rajonu.

Wagenaar H., *Meaning in Action: Interpretation and Dialogue in Policy Analysis*, London–New York 2014, https://doi.org/10.4324/9781315702476.

Wilson G. A., *Community Resilience, Globalization, and Transitional Pathways of Decision-Making*,“Geoforum”2012,vol.43,no.6,https://doi.org/10.1016/j.geoforum.2012.03.008.

Wirtz B. W., Weyerer J. C., *Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats*, “International Journal of Public Administration” 2017, vol. 40, no. 13, https://doi.org/10.1080/01900692.2016.1242614.

Zolli A., Healy A. M., *Resilience: Why Things Bounce Back*, New York 2012.

Niniejsza monografia powstała jako trzecia w serii Krakow Jean Monnet Research Papers w ramach realizowanego przez Katedrę Prawa Europejskiego Uniwersytetu Jagiellońskiego projektu Jean Monnet Module pt. „E-administracja – europejskie wyzwania dla administracji publicznej w państwach członkowskich UE i krajach partnerskich/eGovEU+".

Przedstawia ona analizę wdrożenia i funkcjonowania cyfrowych usług publicznych w Polsce i w Europie ze szczególnym uwzględnieniem związanych z tym wyzwań. Dotyczą one m.in. rozwoju infrastruktury teleinformatycznej, zapobiegania wykluczeniu cyfrowemu oraz zapewniania ochrony prywatności i bezpieczeństwa obywatelom.

Książka adresowana jest do badaczy zajmujących się administracją, prawem administracyjnym i europejskim oraz do praktyków w wymienionych dziedzinach. Mamy nadzieję, że publikacja poszerzy wiedzę czytelników na temat cyfryzacji usług publicznych oraz zachęci środowisko naukowe do dalszych badań w tym zakresie.

This monograph is the third in the Krakow series of Jean Monnet Research Papers and was written as part of the Jean Monnet Module project, carried out by the Chair of European Law at the Jagiellonian University, "E-government – European Challenges for Public Administration in EU Member States and Partner Countries/eGovEU+."

The book presents an analysis of the implementation and functioning of digital public services in Poland and Europe with a particular focus on the challenges involved. These include the development of ICT infrastructure, preventing digital exclusion and ensuring privacy and security of citizens.

The monograph is addressed to researchers in administration, administrative and European law as well as to practitioners in the mentioned fields. We hope the publication will broaden the readers' knowledge of the digitization of public services and encourage the scientific community to further research in this area.

WYDAWNICTWO
KSIĘGARNIA AKADEMICKA
Sp. z o.o. Kraków

https://akademicka.pl

ISBN 978-83-8368-025-5
9 788383 680255