

BEZPIECZEŃSTWO

TEORIA I PRAKTYKA

SECURITY

THEORY AND PRACTICE

DOSKONAŁOŚĆ ZARZĄDZANIA BEZPIECZEŃSTWEM
redakcja
Andrzej Chodyński, Dariusz Fatuła, Izabela Kapera

BEZPIECZEŃSTWO

TEORIA I PRAKTYKA

SECURITY

THEORY AND PRACTICE

DOSKONAŁOŚĆ ZARZĄDZANIA BEZPIECZEŃSTWEM
redakcja
Andrzej Chodyński, Dariusz Fatuła, Izabela Kapera

Kraków 2026
Nr 1

Czasopismo punktowane w rankingu Ministerstwa Nauki i Szkolnictwa Wyższego oraz indeksowane w następujących bazach / The journal is ranked by the Ministry of Science and Higher Education and indexed in the following bases:

Repozytorium eRIKA. Repozytorium Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie; PBN. Polska Bibliografia Naukowa; Index Copernicus; CEJSH. The Central European Journal of Social Sciences; CEEOL. Central and Eastern European Online Library; BazHum; EBSCO

Rada Wydawnicza Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie:

Filip Gołkowski (Przewodniczący), Przemysław Kowalczewski, Grażyna Dębska, Dariusz Fatuła, Katarzyna Gibek, Krzysztof Ingarden, Agnieszka Kubiak-Cyruł, Janusz Ligęza, Sławomir M. Mazur, Oleg Aleksejczuk (Sekretarz)

Rada Naukowa / Editorial Board:

Isabela de Andrade Gama (Brazylia), Mieczysław Bieniek (Polska), Ján Buzalka (Słowacja), Anatolij Demianczuk (Ukraina), Taras Finikov (Ukraina), Jochen Franzke (Niemcy), Marco Gestri (Włochy), Adam Jabłoński (Polska), Marek Jabłoński (Polska), Thomas Jäger (Niemcy), Łukasz Jureńczyk (Polska), Arie M. Kacowicz (Izrael), Lutz Kleinwächter (Niemcy), Marcin Lasoń (Polska), Magdolna Lácay (Węgry), Krzysztof Malinowski (Polska), Sławomir Mazur (Polska), Beata Molo (Polska), Ben D. Mor (Izrael), Yu-Chung Shen (Tajwan), Jan Widacki (Polska)

Redaktor naczelny / Editor-in-Chief: Andrzej Chodyński

Zastępca redaktora naczelnego / Deputy Editor-in-Chief: Krzysztof Waśniewski

Redaktorzy tematyczni / Subject Editors:

Andrzej Chodyński – nauki o zarządzaniu i jakości
Janusz Ziarko – nauki o bezpieczeństwie

Redaktor statystyczny / Statistic Editor: Piotr Stefanów

Sekretarz redakcji / Managing Editor: Kamil Jurewicz

Adiustatorzy / Sub-editors: Kamil Jurewicz, David Lilley

Projekt okładki / Cover design: Oleg Aleksejczuk

Skład i redakcja techniczna / Dtp, and technical editing: Oleg Aleksejczuk

Copyright© by Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
Kraków 2026

e-ISSN 2451-0718
ISSN 1899-6264

Wersją pierwotną czasopisma jest wydanie elektroniczne. „Bezpieczeństwo. Teoria i Praktyka” jest w pełni otwartym czasopismem (Open Access Journals) wydawanym na licencji CC BY-NC-ND 4.0 / The journal is originally published in the electronic version. *Security. Theory and Practice* is an open-access journal published under the CC BY-NC-ND 4.0 licence

Na zlecenie / Commissioned by:

Uniwersytetu Andrzeja Frycza Modrzewskiego w Krakowie
www.ka.edu.pl

Wydawca / Publisher: Oficyna Wydawnicza AFM

Spis treści

Andrzej Chodyński, Dariusz Fatuła, Izabela Kapera: Doskonałość zarządzania bezpieczeństwem. Wprowadzenie	9
The importance of specific research areas in non-military security management: A conversation with Prof. Adam Jabłoński, BEng., PhD, DSc, and Dr. Marek Jabłoński, BEng., DSc, Assoc. Prof., members of the Scientific Council of the <i>Security: Theory and Practice</i>	
Interviewer: Prof. Andrzej Chodyński, PhD, DSc, Eng.	13

ARTYKUŁY

Marta du Vall: Key barriers to inter-organizational learning in the European security ecosystem	21
Izabela Kapera: Postrzeganie bezpieczeństwa przez turystów przyjeżdżających do Zjednoczonych Emiratów Arabskich w kontekście usług hotelarskich segmentu premium	37
Andrzej Chodyński: Świadomość interesariuszy odnośnie do zagrożeń a przywództwo w modelach organizacji rezylientnej	53
Andrzej Chodyński, Vladyslava Kornilova: Leveraging the intellectual capital of a resilient organization in crisis threat situations (case studies)	67
Anna Bałamut, Michał Przygoda: Managing organisational resilience in the onshore wind energy sector in Poland	81
Dariusz Fatuła: Bezpieczeństwo i analiza ryzyka we wdrażaniu sztucznej inteligencji w bankowości detalicznej	97
Paweł Ptaszek: Rola strategii we wzmacnianiu odporności jednostek samorządu terytorialnego	117

Spis treści

Janusz Liber: The involvement of employees in retailers' operational departments in loss prevention in distribution logistics	131
Iryna Kravets, Valentyna Yakobchuk: The transformation of the European economic environment under the impact of the war in Ukraine: An analytical assessment of key challenges and future development trajectories	147
Oksana Pyatkovska: Civic engagement of Ukrainian forced migrants in Estonia: Key challenges and perspectives	165

Contents

Andrzej Chodyński, Dariusz Fatuła, Izabela Kapera: Safety Management Excellence: Introduction	9
The importance of specific research areas in non-military security management: A conversation with Prof. Adam Jabłoński, BEng., PhD, DSc, and Dr. Marek Jabłoński, BEng., DSc, Assoc. Prof., members of the Scientific Council of the <i>Security: Theory and Practice</i>	
Interviewer: Prof. Andrzej Chodyński, PhD, DSc, Eng.	13

ARTICLES

Marta du Vall: Key barriers to inter-organizational learning in the European security ecosystem	21
Izabela Kapera: Perception of safety by tourists visiting the United Arab Emirates in the context of premium hospitality services	37
Andrzej Chodyński: Stakeholder awareness of threats and leadership in resilient organization models	53
Andrzej Chodyński, Vladyslava Kornilova: Leveraging the intellectual capital of a resilient organization in crisis threat situations (case studies)	67
Anna Bałamut, Michał Przygoda: Managing organisational resilience in the onshore wind energy sector in Poland	81
Dariusz Fatuła: Security and risk analysis in the implementation of artificial intelligence in retail banking	97
Paweł Ptaszek: The role of strategy in strengthening the resilience of local government units	117
Janusz Liber: The involvement of employees in retailers' operational departments in loss prevention in distribution logistics	131

Contents

Iryna Kravets, Valentyna Yakobchuk: The transformation of the European economic environment under the impact of the war in Ukraine: An analytical assessment of key challenges and future development trajectories	147
Oksana Pyatkovska: Civic engagement of Ukrainian forced migrants in Estonia: Key challenges and perspectives	165

Copyright© 2026 by Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
Opublikowano w wolnym dostępie (Open Access) na licencji CC BY-NC-ND 4.0



Doskonałość zarządzania bezpieczeństwem. Wprowadzenie

Andrzej Chodyński

prof. dr hab., Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
(Andrzej Frycz Modrzewski Krakow University)
<https://orcid.org/0000-0003-4962-5143>

Dariusz Fatuła

dr hab., prof. UAFM, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
(Andrzej Frycz Modrzewski Krakow University)
<https://orcid.org/0000-0002-6704-2585>

Izabela Kapera

dr hab., prof. UAFM, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
(Andrzej Frycz Modrzewski Krakow University)
<https://orcid.org/0000-0003-1691-5275>

Osiąganie doskonałości w odniesieniu do bezpieczeństwa może być rozpatrywane jako stan lub proces, a osiągnięcie pożądanego poziomu bezpieczeństwa można realizować poprzez zarządzanie bezpieczeństwem. Zarządzanie bezpieczeństwem jako zespół działań odnosi się nie tylko do systemów, obszarów działalności, projektów i procesów, ludzi i zasobów, ale dotyczy także technologii i produktów (Chodyński 2024: 7–12).

Problematyka doskonałości jako stanu lub rezultatu działania wiąże się m.in. z ideą doskonałości organizacyjnej, a także odnosi się do świadomości bezpieczeństwa członków organizacji. Brany jest pod uwagę proces pozytywnie ocenianych zmian obiektu z punktu widzenia określonego kryterium lub zbioru kryteriów, prowadzący do osiągnięcia poziomu doskonałego. Zamierzeniem jest osiągnięcie określonego stanu lub wzorca. Doskonałość organizacji jest opisywana w Modelu Doskonałości EFQM (*European Foundation for Quality Management*), łączącym orientację na wyniki

z podejściem strategicznym i koncentracją na działalności operacyjnej. Uwzględnia się także specyfikę organizacji sektora publicznego (rozwiązanie znane jako *Common Assessment Framework*, CAF). W prezentowanych modelach i propozycjach podkreślane jest znaczenie interesariuszy (*Doskonałość biznesowa...* 2024: 13, 20, 23, 24, 48, 82). Model EFQM w pierwotnej wersji obejmował dziewięć kryteriów (pięć z nich dotyczyło obszaru Potencjał, a cztery – obszaru Wyniki). Zmodyfikowany model z roku 2020 zawiera trzy części: Kierunek, Wykonanie i Rezultaty; akcentuje ocenę osiągnięć organizacji przez kluczowych interesariuszy z uwzględnieniem wyników strategicznych i operacyjnych (Szewczyk 2024: 69–74). Szewczyk podaje, że model EFQM odnosi się do dojrzałości/doskonałości, wskazując równocześnie na różnice między tymi pojęciami: „dojrzałość” (związana ze sposobem zorganizowania) jest kojarzona z rosnącymi możliwościami organizacyjnymi, zaś „doskonałość” (skupiona na wynikach organizacji) dotyczy osiągnięcia i utrzymania najwyższego poziomu tych wyników (Szewczyk 2024: 69).

W przypadku organizacji wskazuje się na pięć atrybutów jej doskonałości: spójność, adaptacyjność, inteligencję (dotyczą doskonałości funkcjonowania) oraz efektywność organizacyjną i ekonomiczną (dotyczy doskonałości wyniku) (Romanowska 2020: 499–512). Doskonałość organizacyjna powinna uwzględniać nie tylko sytuację „w miarę normalnego” funkcjonowania organizacji, ale także ich zachowania w sytuacjach kryzysowych, w tym zakres objęty pojęciem rezyliencji organizacyjnej (Chodyński, Huszłak 2024: 15–41).

Tematyka zeszytu dotyczy problematyki zarówno organizacji, jak i zjawisk i zagrożeń związanych z zarządzaniem bezpieczeństwem. Doskonałość zarządzania – także bezpieczeństwem – można odnosić do pojęcia jakości zarządzania. Wiąże się ona z jakością realizowanej usługi zarządzczej. W przypadku konkretnej organizacji można ją rozpatrywać w układzie menedżer – podwładni. Jakość zarządzania jest określana jako stopień spełnienia potrzeb i oczekiwań organizacji oraz jej interesariuszy (zarówno wewnętrznych, jak i zewnętrznych) w oparciu o (poprzez) realizację usługi zarządzczej. Jakość zarządzania może być także odnoszona do spełnienia potrzeb i oczekiwań obywatelskich w danym czasie i miejscu (Wawak 2019: 69).

Numer rozpoczyna rozmowa z członkami Rady Naukowej czasopisma „Bezpieczeństwo. Teoria Praktyka”, Panami Profesorami Adamem i Markiem Jabłońskimi, wybitnymi ekspertami m.in. w dziedzinach bezpieczeństwa w ruchu kolejowym i zarządzania podmiotami gospodarczymi wobec zagrożeń klimatycznych. Są to ważne aspekty zarządzania bezpieczeństwem pozamilitarnym, będące przedmiotem zainteresowania naszego czasopisma.

W niniejszym numerze problematykę bezpieczeństwa rozpatrywano w różnych aspektach warunkujących osiąganie doskonałości zarządzania:

- roli międzyorganizacyjnego uczenia się w europejskim systemie bezpieczeństwa (tekst autorstwa M. du Vall);

- specyfiki bezpieczeństwa usług hotelarskich (artykuł I. Kapery) na przykładzie obiektów hotelarskich w Zjednoczonych Emiratach Arabskich – przy czym wskazana problematyka wpisuje się w szerszą dyskusję dotyczącą zapewnienia rezyliencji w sektorze hotelarskim, podejmowaną także na gruncie polskim w oparciu o doświadczenia epidemii COVID-19 (Suder et al. 2025: 1–16);
- wykorzystania modeli rezyliencji organizacyjnej, z uwzględnieniem znaczenia przywództwa dla kształtowania i wykorzystania świadomości zagrożeń przez interesariuszy (tekst A. Chodyńskiego);
- wykorzystania kapitału intelektualnego organizacji rezyliентnej wobec zagrożeń o zróżnicowanym charakterze (na podstawie konkretnych studiów przypadków) (autorzy: A. Chodyński, V. Kornilova);
- budowania organizacji rezyliентnych funkcjonujących w sektorze energetyki wiatrowej (tekst A. Bałamut i M. Przygody).

Kolejna grupa artykułów dotyczy problematyki zarządzania bezpieczeństwem w odniesieniu do konkretnych grup podmiotów gospodarczych, jednostek lub realizowanych procesów:

- D. Fatuła podejmuje ten temat w aspekcie wdrażaniu sztucznej inteligencji w bankowości detalicznej;
- J. Liber, odnosząc się do aspektów logistyki dystrybucji, podejmuje problematykę zapobiegania stratom w sieciach handlowych;
- P. Ptasek rozpatruje rolę strategii we wzmacnianiu odporności jednostek samorządu terytorialnego.

Dwa kolejne artykuły podejmują tematykę skutków wojny w Ukrainie: I. Kravets analizuje jej następstwa ekonomiczne dla krajów Unii Europejskiej, zaś O. Pyatkovska rozpatruje problemy związane z migracją obywateli Ukrainy do Estonii. Zbliżona problematyka pojawiała się już w poprzednich numerach czasopisma „Bezpieczeństwo. Teoria i Praktyka” (2025 nr 1 oraz 2024 nr 4).

Bibliografia

- Chodyński, A. (2024). Zarządzanie kryzysowe wobec zagrożeń ekologicznych – rola organizacji komercyjnych i niekomercyjnych. Wprowadzenie. *Bezpieczeństwo. Teoria i Praktyka*, 1, s. 7–12. <https://doi.org/10.48269/2451-0718-btip-2024-1-000>
- Chodyński, A., Huszlak, W. (2024). Społeczne i ekologiczne aspekty audytów – od ECSR do ESG. [W:] D. Fatuła, A. Bałamut (red.). *Społeczne aspekty zarządzania organizacjami wobec zmienności otoczenia*. Oficyna Wydawnicza AFM. <https://doi.org/10.48269/978-83-67491-42-6-01>
- Rogała, P., Martusewicz, J., & Wierzbic, A. (red.) (2024). *Dokształcanie biznesowe. Istota i modele*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu. https://dbc.wroc.pl/Content/131369/Rogała_Martusewicz_Wierzbic_Dokskalnosc_biznesowa.pdf, <https://doi.org/10.15611/2024.73.4>

- Romanowska, M. (2020). Atrybuty doskonałości organizacji. [W:] S. Gregorczyk, G. Urbanek (red.). *Zarządzanie strategiczne w dobie cyfrowej gospodarki sieciowej*. Wydawnictwo Uniwersytetu Łódzkiego. <https://doi.org/10.18778/8220-335-6>
- Suder, M., Kusa, R., Kallmuenzer, A., Glinka, B., Kłobukowski, P. (2025). Building resilience in hotels: Unveiling the nexus of entrepreneurial orientation, firm performance and fear of crisis. *International Journal of Hospitality Management*, 131, artykuł 104252, <https://doi.org/10.1016/j.ijhm.2025.104252>
- Szewczyk, K. (2024). *Model dojrzałości organizacji do wdrożenia koncepcji Przemysłu 4.0 w przedsiębiorstwie produkcyjnym*, rozprawa doktorska. Uniwersytet Ekonomiczny we Wrocławiu.
- Wawak, T. (2019). *Doskonalenie jakości zarządzania w szkołach wyższych*. Wydawnictwo Uniwersytetu Jagiellońskiego.

Copyright© 2026 by Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie
Opublikowano w wolnym dostępie (Open Access) na licencji CC BY-NC-ND 4.0



The importance of specific research areas in non-military security management: A conversation with Prof. Adam Jabłoński¹, BEng., PhD, DSc, and Dr. Marek Jabłoński², BEng., DSc, Assoc. Prof., members of the Scientific Council of the *Security: Theory and Practice*

Interviewer:

Prof. Andrzej Chodyński, PhD, DSc, Eng.

Andrzej Frycz Modrzewski Krakow University
Editor-in-Chief of the Journal
<https://orcid.org/0000-0003-4962-5143>

A. Chodyński: I invited you to a conversation regarding the importance of developing security topics in business and economic sectors, particularly the railway sector. This relates to the need to ensure the resilience of economic entities in the face of contemporary climate threats. In recent years, our journal has devoted considerable attention to the issue of resilience models, particularly in the face of environmental and energy threats, and the potential use of “clean” energy sources, including hydrogen-based ones.

The need to leverage modern technological solutions, including artificial intelligence, is leading to the creation of new organizational resilience models and business models. Your achievements in promoting climate threats (with the participation of the Andrzej Frycz Modrzewski Krakow University employees)

¹ WSB Merito University in Poznań, <https://orcid.org/0000-0003-4008-941X>

² WSB Merito University in Poznań, <https://orcid.org/0000-0001-7964-6522>

are presented in issue 1/2024 of the *Security: Theory and Practice* (A. Jabłoński 2024). We also discussed the issue of safety in railway traffic, taking into account, among others, ecological aspects, climate, energy transformation and renewable energy sources, in an interview with the authorities of the European Railway Clusters Initiative ASBL with your participation in the issue 2/2022 of the *Security: Theory and Practice* (Conversation... 2022). The topic of business models has been the subject of research for many years, from proposals for pro-ecological, pro-efficiency and entrepreneurial business models (Chodyński 2011: 208–238) to the business models proposed by the Professors, taking into account the double transformation: digital and climate (Jabłoński & Jabłoński 2025).

Please share your achievements, also at the international level, in the field of new concepts for building business models, particularly in the face of climate threats and contemporary solutions for rail security.

A. Jabłoński, M. Jabłoński: The research area we have been involved in for many years focuses on two closely interconnected pillars. The first pillar concerns a broad understanding of the concept of business models against the backdrop of ongoing changes in the economy, business, and society related to the operation of enterprises in the so-called multi-crisis environment (economic, social, military, health, climate, etc.). Here, we focus on developing various types of business models (analog, digital, technical, power, climate, ecological, AI-driven, etc.) and their attributes: scalability, consistency, sustainability, circularity, etc.). The second pillar is related to the management of rail transport safety and cybersecurity by High Reliability Organizations (HROs), such as rail transport operators. In this area, we broadly develop the principles of safety culture, technical compliance, safe integration, and digital rail traffic control systems and digital data transmission, as well as their impact on safety management criteria in rail transport. These activities influence the creation of various solutions related to operational safety, operational cybersecurity, the physical protection of infrastructure critical to national security, such as rail infrastructure, and the cybersecurity of infrastructure, ICT systems, and devices used on the railways. The connecting factor between these two pillars of our scientific development is creating a framework for organizations' ability to ensure business continuity and achieve high efficiency through key ontological entities, which include business models, strategies, processes, and projects, creating a specific strategic hybrid in managers' decision-making processes under conditions of pressure, constraints, opportunities, possibilities, and threats.

A. Chodyński: How do you perceive the interrelationships between the concepts leading to the construction of business models and organizational resilience models?

A. Jabłoński, M. Jabłoński: One of the key attributes of business models, in the context of the automation, robotics, IT, ICT, technical diagnostics, cybernetics, and

artificial intelligence solutions being developed and incorporated into them, is the resilience and agility of business models. Resilience is more focused on the external protection of business models against their potential imitation by competitors, thus weakening the market potential of enterprises. In our interpretation, agility is primarily focused on the internal capacity of enterprises to strategically renew the organization's key resources and thus the capacity to sustainably develop them. Combining these two components creates a vertical-horizontal model for managing an organization's business security.

A. Chodyński: In my proposed model of responsible innovative behavior for organizations (Chodyński 2021: 203–222), including those facing extreme environmental turbulence that threatens security, and taking into account the assumptions of organizational resilience, a special role is assigned to collaboration with stakeholders. How do you see the potential for utilizing these views in implementing business models?

A. Jabłoński, M. Jabłoński: The relational dimension of enterprises operating on the edge of the real and virtual worlds through the joint construction of analog and digital identities requires openly shaping relationships with all stakeholders, or otherwise known as actors in the relationship network (stakeholders and net stakeholders). This is achieved by combining the contributions and incentives of various stakeholder groups, thus creating and developing progressive and inclusive business models for enterprises. In such a space, the subjective nature of decision-making determines the organization's ability to survive even in the most difficult conditions, creating platforms for market dialogue and value exchange with them, becoming their first choice as the purchasing power of customers declines.

A. Chodyński: Given the occurrence of extreme environmental turbulence that threatens the security of organizations, I proposed building a model for non-economic crisis in organizations, along with an analysis of the resilience curve of these organizations (Chodyński 2022). How do you see the relationship between these views and the business models you are building and their practical application?

A. Jabłoński, M. Jabłoński: The economic nature of an organization's business existence is no longer sufficient to survive in a multi-crisis environment. Only a well-integrated system for creating sets of multiple values embedded in value propositions for various types of stakeholders, and a dedicated revenue-generating logic embedded in the configuration of business models, can create the right space and climate for achieving results in the short and long term. Creating multiple values, including financial, social, climatic, safety-related, and other values, can only be achieved through organizations proactively developing a multi-business model

environment as a response to the dynamic response to the chaos occurring in a multi-crisis environment. Therefore, a non-economic model of organizational functioning based on the principles of resilience is the correct response to uncontrolled phenomena within the network of the economy, business, and society. It should also be noted that the greatest threats to enterprises currently stem not from microeconomic and sectoral conditions, but from macroeconomic decisions related to political and regulatory factors that have a multidimensional impact on the existential dimension of various types of economic entities. In this interpretation, developing non-economic attributes of organizations is fully justified and necessary.

A. Chodyński: How do you assess the chances of integrating the scientific community, including management science specialists, on the issues raised?

A. Jabłoński, M. Jabłoński: These issues are particularly important from the perspective of their applicability. It is important to remember that the discipline of management and quality science is an applied science, and therefore, it is the responsibility of every scientist to create and develop research areas that will inspire and stimulate a creative decision-making system for managers. The scientific community should propose feasible solutions appropriate to the state of development of the economy, business, and society. There is a noticeable underestimation of technology and its impact on the entire development structure of the discipline of management and quality science. For example, classic paradigms and solutions previously used in management are often inapplicable in the digital environment. It is worth noting, for example, that the logic, methodology, and conceptual framework present in the dynamic digital, climate, and energy transformations are significantly different from the principles operating in traditional value chains. Therefore, research opportunities exist in the design and implementation of technical and digital business models driven by Artificial Intelligence solutions. Furthermore, managers, aware of market challenges, should receive tools from scientists to solve even the most challenging business problems. For example, we believe that the scientific community has not fully appreciated the concept of Evidence-Based Management as a new scientific area and the future of modern management. Evidence-Based Management allows for the elimination of errors and decision-making problems for managers, who make better decisions thanks to broad online access to scientific evidence embedded in scientific publications using large datasets. Currently, we believe that combining the concepts of Artificial Intelligence and Data Science with technical, digital, and climate-related solutions supported by Evidence-Based Management opens a new dimension of scientific exploration and exploitation in management and quality sciences.

A. Chodyński: You are involved not only in research but also hold various leadership positions in organizations that influence the implementation of specific requirements and international standards in the area of security management.

A. Jabłoński, M. Jabłoński: Yes, that's true, hence we strive to confront scientific theory with business practice and the direct expectations of managers in creating a scientific panacea for their problems in the organizational-managerial, economic-financial, technical, and operational areas. Above all, in our scientific research and the solutions we present, we strive to be useful to the economy, business, and society. In this cognitive space, the criteria we develop for managing security and cybersecurity in its various dimensions and varieties take on a different driving force.

A. Chodyński: Thank you for the interview. The presented views will allow for a better focus on the thematic areas of the *Security: Theory and Practice*, particularly in the area of security management for economic entities operating in situations of threat. The considerations largely concern crisis management, including for entities that are part of critical infrastructure.

References

- Chodyński, A. (2011). *Odpowiedzialność ekologiczna w proaktywnym rozwoju przedsiębiorstw*. Oficyna Wydawnicza AFM.
- Chodyński, A. (2021). *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*. Oficyna Wydawnicza KAAFM.
- Chodyński, A. (2022). Kryzys pozaekonomiczny przedsiębiorstwa – ekologiczny aspekt reziliencji organizacyjnej. In: A. Chodyński, D. Fatuła, M. Leśniewski (Eds.). *Zrównoważony rozwój, systemy informacyjne i zarządzanie bezpieczeństwem w perspektywie długoterminowej przedsiębiorstw*. Oficyna Wydawnicza AFM, pp. 11–31. <https://repozytorium.uafm.edu.pl/items/48066866-483a-4467-b4bf-cab375d68999>
- Conversation on and presentation of opinions about safety management in railway traffic of the European Union (2022). Moderated by Professor Andrzej Chodyński. *Bezpieczeństwo. Teoria i Praktyka*, 2, pp. 13–19. <https://doi.org/10.48269/2451-0718-btrip-2022-2-Con>
- Jabłoński, A. (2024). Aspekty bezpieczeństwa w kontekście zmian klimatycznych. Sprawozdanie z Międzynarodowej Konferencji Naukowej „Zmiany klimatyczne w środowisku wielu kryzysów – nowa przestrzeń dla biznesu i gospodarki. Jak transformacja cyfrowa i klimatyczna zmienia modele biznesu przedsiębiorstw?”, 21–23 listopada 2023, Chorzów, Uniwersytet WSB Merito w Poznaniu Filia w Chorzowie. *Bezpieczeństwo. Teoria i Praktyka*, 1, pp. 125–129. <https://doi.org/10.48269/2451-0718-btrip-2024-1-007>
- Jabłoński, A., & Jabłoński, M. (2025). Digital and Climate Changes on the Business Models of Companies. In: A. Jabłoński & M. Jabłoński (Eds.). *Effect of Digital and Climate Changes in the Business Models of Companies*. Taylor & Francis Group. <https://doi.org/10.1201/9781032628783>

Artykuły/ Articles

Key barriers to inter-organizational learning in the European security ecosystem

Marta du Vall

PhD, DSc, Associate Professor, Faculty of Management, Media and Technology,

Andrzej Frycz Modrzewski Krakow University, Kraków, Poland

<https://orcid.org/0000-0003-1245-730X>

Introduction

The contemporary security environment of the European Union (EU) is characterized by increasing complexity and the interdependence of threats. These threats, ranging from terrorist networks and international organized crime to advanced cyberattacks, are fundamentally transnational in nature. Their networked nature means that no single Member State, acting in isolation, is able to respond effectively. This leads to an obvious functional necessity for deepened cooperation, information exchange, and, most importantly, collective learning (European Commission, 2025).

In response to this necessity, the European Union has systematically expanded its institutional architecture in the Area of Freedom, Security, and Justice over the last two decades. Specialized agencies have been established, such as Europol (European Union Agency for Law Enforcement Cooperation) (European Union Agency for Law Enforcement Cooperation [Europol], n.d.-a), Frontex (European Border and Coast Guard Agency) (Frontex, n.d.-a), and ENISA (European Union Agency for Cybersecurity) (European Union Agency for Cybersecurity, n.d.-a), whose mandates are directly related to the aggregation, analysis, and dissemination of specialized knowledge.

However, this process of institutionalization encounters a fundamental obstacle: national security, intelligence, and policing remain strictly within the purview of

Member States, constituting the core of their sovereignty (European Commission, 2025). This leads to a phenomenon that can be termed the sovereignty paradigm: Member States create supranational agencies to address problems they cannot solve alone, while simultaneously and deliberately limiting their powers, resources, and access to key intelligence to protect their own decision-making autonomy (Walsh, 2006).

As a result, the European security architecture is torn between the rhetoric of integration and the practice of fragmentation. The central research problem of this article is the discrepancy between the declared need for Inter-Organizational Learning (IOL) and the actual capacity and will of the organizations forming this architecture to implement it. The article posits that inter-organizational learning is a key but underutilized strategic resource of the European Union. Its effectiveness is inhibited not by technological deficits – however significant – but by deep-seated political, cultural, and institutional barriers. Among them, the absolute primacy belongs to a chronic lack of trust (Safjański, James, 2020), which prevents the transformation of distributed data into collective, operational knowledge. The article synthesizes the main barriers and recommends a strategic shift of emphasis from technological platforms to building human and relational capital.

Methodology

This article employs a qualitative approach, combining a targeted literature and document review with an analytical synthesis of selected case studies. The primary methodological objective is to systematically map empirical data regarding the EU security architecture onto two established theoretical frameworks: the 4I organizational learning model and the concept of Absorptive Capacity (ACAP).

The analysis is based on a targeted selection of official EU agency evaluations, policy reports, and peer-reviewed academic literature. Source materials were purposefully selected based on their direct relevance to information-sharing protocols, the institutional mandates of Europol, Frontex, and ENISA, and documented operational challenges within the collaborative governance networks of the EU security sector.

Case studies were chosen using a purposive sampling strategy to illustrate contrasting extremes of IOL effectiveness in practice, allowing for a comparative analysis of learning mechanisms:

1. strategic failure – the Paris (2015) and Brussels (2016) terrorist attacks were selected as a paradigmatic, highly documented example of a catastrophic IOL breakdown. This case serves to illustrate systemic failure at the *integration* stage of the 4I model;
2. operational success – Joint Investigation Teams (JITs) and cross-border Network Operations (e.g., Operation EMMA) were selected as contrasting examples of

functional, bottom-up IOL. These cases were chosen to demonstrate how temporary organizational units can maximize *absorptive capacity* and overcome inherent trust barrier.

The collected empirical data was systematically mapped against the theoretical models to precisely diagnose structural breaking points. The 4I model was used to differentiate between deficits in national-level *interpretation* versus failures in inter-organizational *integration*. Concurrently, the ACAP model was applied to shift the analytical focus from the data senders (EU agencies) to the critical interface and processing capabilities of the receivers (Member States).

Inter-organizational learning (IOL) in the context of security

Organizational Learning (OL) theory largely originates from the analysis of the private sector, where the capacity for adaptation and innovation is a condition for survival and competitive advantage. These elements collectively form an organizational culture conducive to absorbing and utilizing new knowledge. Inter-Organizational Learning (IOL) extends this concept beyond the boundaries of a single firm, describing how knowledge is transferred, assimilated, and co-created between organizations operating within a network.

In the public sector, to which security agencies belong, IOL acquires specific significance. The goals here are not profit or market share, but the improvement of public service efficiency, increased citizen security, or more effective crisis response (Harvey et al., 2010). This collaboration often relies on complex collaborative governance networks rather than simple market mechanisms. Transferring IOL models to the security sector requires accounting for its radical specificity. While private sector cooperation may be based on mutual benefit, the security sector (especially intelligence and police services) operates in a “high stakes, low trust” environment (Boardman, 2006).

Analysis of communication barriers within the intelligence community reveals that the default organizational culture is *not* sharing information (Boardman, 2006). This is perceived as a rational strategy, motivated by the necessity to protect sensitive sources and methods, as well as defending one’s own institutional mandates (so-called “turf wars”) (Boardman, 2006). This culture is so deeply ingrained that agencies operate in an environment “hostile to intelligence sharing,” viewing knowledge as a resource in a “zero-sum game” (Boardman, 2006).

Furthermore, in the complex security ecosystem of the EU, IOL is hampered by a fundamental conflict of mandates. This problem is perfectly visible in the relationships between Computer Security Incident Response Teams (CSIRTs), supported by ENISA, and Law Enforcement (LE), supported by Europol (ENISA, 2020). The mandate of a CSIRT is the mitigation of cyber incident effects and the fastest possible restoration of system functioning (ENISA, 2020). The mandate of law enforcement

is the prosecution of perpetrators, which requires securing and preserving digital evidence (ENISA, 2020). As the ENISA report indicates, CSIRT actions (aimed at rapid repair) can “seriously impede the collection of evidence necessary for criminal investigation, or even destroy it” (ENISA, 2020). Effective IOL in this context does not consist of naive “sharing everything,” but on developing complex deconfliction protocols that allow for reconciling conflicting institutional goals.

IOL Models – breaking points

To diagnose where the IOL process breaks down in the security context, the 4I model by Crossan et al. (1999) is useful. This model describes learning as a dynamic, multi-level process of strategic renewal involving four linked processes: intuition – a process at the individual level (subconscious recognition of patterns and possibilities) (Serrat, 2017); interpretation – a process at the individual level (conscious explanation of intuition to oneself and others, making sense of it, and creating cognitive maps) (Lawrence et al., 2005); integration – a process at the group level (developing “shared understanding among individuals and taking coordinated actions”) (Lawrence et al., 2005); institutionalization – a process at the organizational level (embedding learning in the organization’s systems, structures, procedures, and routines) (Lawrence et al., 2005).

The 4I model allows for a precise diagnosis of where IOL fails in the European security architecture. As empirical analysis will show, the problem is often not a lack of intuition or interpretation at the national level (e.g., an analyst in one Member State identifies a threat). The process notoriously collapses at the integration stage – the inability to transform individual knowledge into “shared understanding” and “coordinated action” at the inter-organizational level. This happens due to trust barriers (Walsh, 2006) and “turf” conflicts (Boardman, 2006), which prevent the flow of knowledge from the individual level to the network level.

The second key analytical model is the concept of Absorptive Capacity (ACAP), defined by Cohen and Levinthal (1990) as an organization’s ability to “recognize the value of new information, assimilate it, and apply it” (Cohen & Levinthal, 1990). ACAP is not passive reception; it is an active capability critically dependent on prior related knowledge and existing communication and coordination paths (Farrell & Coburn, 2018). This model, though derived from firm innovation research, is successfully applied to analyze performance improvement in the public sector, including police forces (Harvey et al., 2010). In this context, ACAP is defined as a public organization’s ability to access new knowledge, assimilate it, and apply it to improve results (Harvey et al., 2010).

Applying the ACAP model allows for nuanced analysis of IOL failures in the EU. Suboptimal performance of information exchange systems, such as those managed by

Europol (Safjański, James, 2020), does not necessarily result solely from the sender's (Europol) failure. Equally often, it may be the receiver's (national police unit) failure. A Member State may receive high-quality intelligence data but lack the appropriate absorptive capacity – i.e., trained analysts (lack of *prior related knowledge*) or internal procedures (lack of *paths*) – to assimilate and operationally apply this data. This diagnosis shifts the burden of analysis from EU agencies alone to the critical interface between agencies and national bodies.

The architecture of knowledge exchange in the EU

Using the presented theoretical frameworks, it is possible to analyze the key EU security agencies – Europol, Frontex, and ENISA – as central nodes in the IOL network. A synthetic comparison of their mandates, mechanisms, and diagnosed barriers is presented below.

Table 1. Characteristics of key EU security agencies as learning organizations

Agency	Main mandate (related to IOL)	Key IOL platforms/mechanisms	Identified barriers to IOL (sources)
Europol	Central hub for criminal intelligence and analysis; supporting Member States (MS) investigations.	SIENA (Secure Information Exchange Network Application), EIS (Europol Information System), EPE (Europol Platform for Experts), J-CAT (Joint Cybercrime Action Taskforce).	Lack of Trust by MS leading to reluctance to share data (Safjański, James, 2020). Legal Fragmentation and data protection limits (European Data Protection Supervisor, EDPS) (Fotiadis et al., 2022). Bottlenecks in SIENA architecture (national units) (Statewatch, 2025).
Frontex	Promoting Integrated Border Management (IBM); developing a common professional culture.	Joint trainings (on-the-job, formal), e-learning (EU Learn platform), operations, risk analysis (EU-ROSUR).	Culture of Resistance to negative feedback (e.g., re: fundamental rights). Low Perception of value-add by MS (reporting seen as a „burden“) (Walsh, 2006). Insufficient transparency of complaint mechanisms.
ENISA (and CSIRT Network)	Building situational awareness; strengthening operational cooperation (CSIRT Network support).	CSIRT Network, common incident taxonomies, threat analysis, joint exercises.	Conflicting Mandates (CSIRT: mitigation vs. Law Enforcement (LE): prosecution) (ENISA, 2020). “Two fronts of trust” dilemma (CSIRTs must protect constituent trust, limiting data sharing with LE) (ENISA, 2020).

Source: Author's own elaboration.

Europol

Europol's mandate situates the agency as the center of European police cooperation, intended to serve as a criminal information hub (Europol, 2024) and analytical center supporting Member State investigations (Europol, n.d.-a). To this end, Europol manages key IOL platforms: the Europol Information System (EIS), the Platform for Experts (EPE), which hosts, among others, the SIRIUS project facilitating access to electronic evidence from service providers (Europol, n.d.-g), and primarily the Secure Information Exchange Network Application (SIENA) (Europol, n.d.-c).

Analysis of these platforms reveals, however, two fundamental paradoxes limiting Europol's IOL potential. The first is the SIENA Paradox, illustrating the gap between technological optimism and political realism. The official narrative describes SIENA as a "state-of-the-art" platform enabling "rapid and user-friendly exchange" of operational information (Europol, n.d.-f). However, evaluation reports point to a much more problematic picture: SIENA's functioning is often "constrained by limited access" of national bodies, and the multitude of available communication channels (bilateral, multilateral, via Interpol) creates "more difficulties than solutions" for practitioners (Disley et al., 2012). The cause of this dysfunction is not technical but architectural and political. As analyses indicate, the SIENA system was intentionally designed so that data must pass through National Contact Units (Statewatch, 2025). This architecture is a technical reflection of the sovereignty paradigm – Member States, instead of creating a true peer-to-peer knowledge exchange, imposed a "hub-and-spoke" model where national units act as gatekeepers. This intentionally built-in "bottleneck" institutionalizes the lack of trust (Walsh, 2006) in the technology itself, fundamentally limiting the potential for learning.

The second problem is the dilemma of learning vs. legality. For Europol to become a learning organization capable of detecting complex criminal patterns, especially in the era of Big Data and AI, it needs the capacity to analyze vast datasets (Statewatch, 2025). However, the unprecedented decision by the European Data Protection Supervisor (EDPS) in January 2022, ordering Europol to delete its "big data ark" (Fotiadis et al., 2022), demonstrates a fundamental conflict. The EDPS stated that Europol was illegally storing data on persons not directly linked to criminal activity, violating the principle of data minimization (Fotiadis et al., 2022). Europol is thus trapped in an unsolvable conflict: the logic of learning (more data = better patterns and analysis) stands in direct contradiction to the EU's legal logic (data protection and privacy) (Fotiadis et al., 2022). This means Europol, unlike agencies in the style of the American NSA (Fotiadis et al., 2022), is legally restrained from achieving its full data-driven IOL potential, constituting a key, externally imposed barrier.

Frontex

Frontex's mandate focuses on promoting Integrated Border Management (IBM) (Frontex, n.d.-a). A key IOL mechanism in this context is creating a "common European professional culture" for border guards (Frontex, n.d.-c). The agency invests heavily in various forms of knowledge transfer, including on-the-job training, formal courses (e.g., on fundamental rights, languages), and e-learning platforms (like "EU Learn") (Frontex, n.d.-a).

Analysis of Frontex's activity indicates a distinction between performative learning and critical learning. The agency demonstrates high proficiency in performative learning – teaching officers how to perform tasks according to specific procedures (Frontex, n.d.-c). This is "top-down" knowledge transfer. Simultaneously, Frontex exhibits strong resistance to critical learning – absorbing feedback about errors, failures, and systemic problems, particularly in the sensitive area of fundamental rights. Evidence of this dysfunction is clear. The Consultative Forum on Fundamental Rights (CFFR) stated it was "not consulted" on human rights issues, and its comments were "often ignored." Similarly, the Fundamental Rights Officer (FRO) faced allegations of a lack of independence, and complaint mechanisms proved insufficiently transparent and effective. Furthermore, relationships with Member States also indicate value perception problems. Some Member States perceived sharing information with Frontex as an "additional burden" rather than a process bringing "value added" (Walsh, 2006). This points to an organizational culture resistant to negative feedback. From the perspective of OL theory, an organization that systematically ignores feedback mechanisms is not a learning organization; it is an example of institutional unlearning, where the culture actively rejects knowledge contrary to its operational goals.

ENISA

ENISA plays a key role in the EU cybersecurity ecosystem, aiming to raise common situational awareness (ENISA, n.d.-a) and operationally supporting the CSIRT Network (ENISA, n.d.-b). Learning in this network occurs through information exchange on threats and incidents (ENISA, n.d.-a) and creating common frameworks, such as incident taxonomies (ENISA, 2020).

However, as signaled earlier, the main barrier here is the conflict of mandates (ENISA, 2020). This barrier leads to a more complex problem, which can be called the "two fronts of trust" dilemma. CSIRTs, especially national, academic, or sectoral ones, operate largely based on voluntary incident reporting by their constituents, e.g., private sector companies (ENISA, 2020). To maintain this key data flow, CSIRTs must guarantee confidentiality and act in the victim's best interest (e.g., quickly patching the system). At the same time, law enforcement (LE) demands access to the

same data for investigative and prosecutorial purposes (ENISA, 2020). CSIRTs are trapped in a dilemma. If they too willingly and automatically pass data to law enforcement, they risk losing the trust of their constituents.

As research indicates, victims of cybercrime “sometimes refuse to report incidents” to law enforcement for various reasons (ENISA, 2020). In such cases, CSIRTs are “discouraged from sharing information... because they fear losing the trust of their constituent” (ENISA, 2020). CSIRT networks must therefore manage trust on two fronts simultaneously: (1) towards their data providers (private sector) and (2) towards their partners (LE). The interests of these two groups are often contradictory. For this reason, simple technical solutions, such as promoting a “common platform” for data exchange (ENISA, 2019), will not solve the problem. The barrier is fundamentally relational, political, and rooted in the conflicting operational logics of different security ecosystem actors.

Learning from failures and successes

Theoretical and institutional analysis shows that IOL in the EU is a process burdened with structural barriers. This section verifies this thesis through case study analysis, contrasting strategic failure with operational successes.

The Paris (2015) and Brussels (2016) attacks

The coordinated terrorist attacks in Paris (November 2015) and Brussels (March 2016) constitute a tragic and textbook example of a catastrophic failure of inter-organizational learning. Post-mortem analyses revealed that the terrorist network (the so-called Zerkani network) executing the attacks was known to law enforcement and intelligence services in several Member States, including Belgium and France (Andreeva, 2025).

The failure was not a lack of data. It was a systemic inability to integrate distributed fragments of information into a coherent intelligence picture and transform it into “coordinated action,” which is the definition of failure at the Integration stage of the 4I model (Lawrence et al., 2005). Law enforcement and intelligence agencies from different states “failed to cooperate adequately,” leading to numerous “missed opportunities” to interrupt preparations for the attacks (Andreeva, 2025). This was a direct result of trust barriers (Walsh, 2006), differences in organizational cultures (Boardman, 2006), and the lack of effective intelligence exchange protocols.

However, OL theory also indicates that failure can be a powerful catalyst for learning. The 2015 and 2016 attacks provided a key insight: it was precisely as a result of these failures that a “European counter-terrorism and intelligence co-operation culture” began to develop (Andreeva, 2025). The shock caused by the scale of the attacks and the realization that they were preventable forced national

practitioners to understand that “cooperation is necessary” to meet threats (Andreeva, 2025).

This tragedy acted as a reactive learning mechanism, temporarily overcoming the sovereignty paradigm. The cost of not sharing information (mass casualties) suddenly proved higher than the perceived cost of sharing it. Many subsequent legislative initiatives and the strengthening of agency mandates (including Europol) can be seen as an attempt at institutionalization (the fourth stage of the 4I model) of the lessons learned from this failure.

Studies of success: Joint Investigation Teams (JITs) and Network Operations

In radical contrast to the strategic failures of central data exchange stand the successes of Joint Investigation Teams (JITs). JITs are recognized as “one of the most advanced tools” for international cooperation in criminal matters (European Union Agency for Criminal Justice Cooperation [Eurojust], n.d.). These are ad hoc teams created for a fixed period (usually 12-24 months) and a specific investigative purpose, consisting of prosecutors, judges, and law enforcement officers from two or more states (Eurojust, n.d.). Eurojust plays a key role in the legal, logistical, and financial support of JITs, similar to Europol in operational support (Eurojust, n.d.).

The success of JITs can be explained by analyzing them as incubators of trust and micro-spaces of effective IOL that directly address identified barriers:

1. overcoming the trust barrier: unlike anonymous data exchange via centralized platforms (like SIENA), JITs rely on intensive, daily, face-to-face cooperation (Nuño-Solinís & Urtaran-Laresgoiti, 2018). Trust here is not a prerequisite imposed from above, but a result of shared operational practice focused on solving a concrete, shared problem (e.g., dismantling a specific criminal group) (United Nations Office on Drugs and Crime, n.d.);
2. realizing the “Integration” process (4I): a JIT is by definition an integration mechanism (Lawrence et al., 2005). It forces participants from different legal and organizational systems (Block, 2008) to develop “shared understanding” and take “coordinated actions” in real-time;
3. maximizing Absorptive Capacity (ACAP): a JIT creates a temporary organizational unit with maximum absorptive capacity (Farrell & Coburn, 2018). By gathering experts with the required “prior related knowledge” (police, analysts, prosecutors) in one place, the JIT ensures that newly acquired knowledge (e.g., from a wiretap in Country A) is immediately understood, assimilated, and applied (e.g., to issue an arrest warrant in Country B) (Harvey et al., 2010), without delays resulting from bureaucratic “gatekeepers” (Statewatch, 2025).

The success of JITs proves that effective IOL in the European security sector is largely bottom-up, problem-oriented, and relationship-based, rather than top-down, centralized, and technology-based.

Further evidence of IOL evolution is provided by complex network operations that go beyond traditional state-to-state cooperation. An example is Operation European Money Mule Action (EMMA), which led to the arrest of 178 people in 2016 (Europol, 2016). The key to its success was not only cooperation between 16 states, Europol, Eurojust, and the FBI. It was the engagement of 106 banks and private partners (Europol, 2016).

Similarly, Operation EMMA95, which led to the dismantling of the encrypted communication network EncroChat, was the result of JIT actions (France, Netherlands) supported by Europol and Eurojust (Europol, 2020). This case illustrates that critical infrastructure used by criminals is in private hands.

These cases indicate the most important new trend: the evolution from public-public IOL to public-private IOL. State agencies no longer possess a monopoly on knowledge nor control over infrastructure (financial systems (Europol, 2016), encrypted communication services (Europol, 2020)). Effective crime fighting now requires the ability to learn *from* and *with* the private sector (tech companies, financial institutions).

Europol attempts to institutionalize this new reality through initiatives such as the SIRIUS project (facilitating cooperation with online service providers) (Europol, n.d.-g) or direct cooperation with tech companies (Statewatch, 2025). However, this raises new, complex challenges related to law, ethics, and trust.

Conclusion

The analysis conducted in this article demonstrated that inter-organizational learning (IOL) in the European security sector is a complex, highly politicized process burdened with fundamental contradictions. Its dynamics are defined by the constant tension between the functional necessity of cooperation, forced by the transnational character of threats, and the political and cultural imperative of protecting national sovereignty and secrecy – the sovereignty paradigm.

The main findings of the analysis indicate that the most serious obstacles to effective IOL lie not in the sphere of technology, but in organizational culture and politics. These include, above all, the lack of trust between Member States and agencies (Safjański, James, 2020), a culture of “knowledge hoarding” (need-to-know) rather than “need-to-share” (Boardman, 2006), and deep mandate conflicts (e.g., CSIRT vs. LE) (ENISA, 2020).

A further problem is the dysfunction of centralized models. Top-down, centralized IOL mechanisms based on technological platforms (like SIENA at Europol) are systematically weakened. This happens because their architecture is a political compromise reflecting the sovereignty paradigm (built-in bottlenecks)

(Statewatch, 2025), and their potential is further limited by rigorous European data protection frameworks (the Legality Dilemma) (Fotiadis et al., 2022).

Simultaneously, it is clear that effective IOL – understood as learning leading to behavioral change and improved operational results – occurs primarily in bottom-up, problem-oriented, and trust-based microsystems. Joint Investigation Teams (JITs) are the best example of this, acting as “incubators of trust” and realizing Integration processes (from the 4I model) and maximizing absorptive capacity (ACAP) (Eurojust, n.d.).

Undoubtedly, the current EU security architecture exhibits characteristics of reactive learning, adapting in response to catastrophic failures (Andreeva, 2025). It lacks the mechanisms and organizational culture necessary to implement proactive learning, characteristic of High Reliability Organizations (HRO).

Further progress in building the EU’s capacity for collective learning requires a strategic shift in resources and attention. Instead of concentrating solely on investments in further technological platforms, policymakers should equally invest in human platforms – mechanisms such as CEPOL, exchange programs, joint exercises, and facilitating the creation of JITs. Technological platforms can only transmit data; it is human platforms, building social capital, that are capable of generating the rarest and most important resource in the security ecosystem: trust.

The author is aware that a limitation of this analysis is its reliance on publicly available reports and literature. Undoubtedly, further research, particularly ethnographic studies on daily cooperation practices within JITs and deeper analysis of cultural barriers in implementing HRO principles in police forces, is necessary to fully understand the dynamics of learning in this critical sector for Europe.

As noted, the current IOL model in the EU is largely reactive – learning from spectacular failures like the 2015 and 2016 attacks (Andreeva, 2025). This is a costly and inefficient model. An alternative is offered by the concept of High Reliability Organizations (HRO), derived from research on extremely high-risk sectors like aviation, nuclear power, or aircraft carrier operations. HROs are characterized by a proactive approach to learning, based on two key principles: (1) a system perspective, which in case of error focuses on analyzing faulty processes rather than blaming individuals, and (2) *preoccupation with failure*, viewing minor errors and “near misses” as priceless opportunities for learning and system adaptation before they lead to disaster.

Implementing HRO thinking in the European security sector would require a fundamental cultural change. As analyses indicate, security organizations are often dominated by a “culture of punishment” for reporting errors, which prompts employees to hide them. The HRO model requires the opposite: a “culture of reward” or at least a “just culture” (Kanaan & Mayer, 2023) that actively encourages problem reporting. In practice, this would mean that a Frontex officer reporting

a fundamental rights violation or a Europol analyst pointing out a systemic flaw in SIENA data flow (Disley et al., 2012) would not be treated as a problem, but as a key source of learning.

Ultimately, the analysis of IOL barriers leads to the conclusion that the weakest link is not technology, but the human and relational factor (Birdi et al., 2020). Investments in expensive IT platforms (like SIENA) will not yield results if they are not accompanied by equivalent investments in human capital and social networks. The key barrier remains the lack of trust (Walsh, 2006). Trust is not a product of technology; it is built by people through repeated, positive interactions (Birdi et al., 2020). This highlights the key, though often underestimated, role of agencies like CEPOL (European Union Agency for Law Enforcement Training), whose mandate is precisely creating “human platforms” for IOL (European Commission, 2025). Joint trainings, officer exchange programs, and even informal social events (Birdi et al., 2020) build relationships and mutual cultural understanding, which are the foundation of trust. As research indicates, barriers as prosaic as the lack of a common language (Birdi et al., 2020) or misunderstanding of organizational differences (Birdi et al., 2020) are often a greater obstacle to information exchange than the lack of technical compatibility.

References

- Andreeva, C. (2025). The Zerkani Network and the 2015 Paris and 2016 Brussels Attacks: An Illustration of Counter-Terrorism Dysfunction in Europe. *Studies in Conflict & Terrorism*, 48(11), 1313–1341. <https://doi.org/10.1080/1057610X.2023.2178078>
- Birdi, K., Griffiths, K., Turgoose, C., ..., Vonaş, G. (2020). Factors influencing cross-border knowledge sharing by police organisations: An integration of ten European case studies. *Police Practice and Research*, 22(1), 3–22. <https://doi.org/10.1080/15614263.2020.1789462>
- Block, L. (2008). Combating organized crime in Europe: Practicalities of police cooperation. *Policing: A Journal of Policy and Practice*, 2(1), 74–81. <https://doi.org/10.1093/police/pan009>
- Boardman, Ch.H. (2006). *Organizational culture challenges to interagency and intelligence community communication and interaction*. Defense Technical Information Center. <https://apps.dtic.mil/sti/tr/pdf/ADA451234.pdf> [accessed: 30.10.2025].
- Cohen, W.M., & Levinthal, D.A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, 35(1), 128–152. <https://doi.org/10.2307/2393553>
- Crossan, M.M., Lane, H.W., & White, R.E. (1999). An organizational learning framework: From intuition to institution. *Academy of Management Review*, 24(3), 522–537. <https://doi.org/10.5465/amr.1999.2202135>
- Disley, E., Irving, B., Hughes, W., Patrui, B. (2012). *Evaluation of the implementation of the Europol Council Decision and of Europol's activities*. RAND Europe. https://www.europol.europa.eu/sites/default/files/documents/rand_evaluation_report.pdf [accessed: 30.10.2025].
- European Commission. (2025, June 23). Law enforcement cooperation. https://home-affairs.ec.europa.eu/policies/internal-security/law-enforcement-cooperation_en [accessed: 30.10.2025].
- European Union Agency for Cybersecurity (ENISA). (n.d.-a). *Cooperation mechanisms*. <https://www.enisa.europa.eu/topics/cyber-threats/situational-awareness> [accessed: 23.10.2025].

- European Union Agency for Cybersecurity (ENISA). (n.d.-b). *CSIRTs Network*. <https://csirtsnetwork.eu/> [accessed: 23.10.2025].
- European Union Agency for Cybersecurity (ENISA). (2019, July 24). *Sharing is caring: Technical cooperation across CSIRTs, LE and the judiciary*. <https://www.enisa.europa.eu/news/enisa-news/sharing-is-caring-technical-cooperation-across-csirts-le-and-the-judiciary> [accessed: 23.10.2025].
- European Union Agency for Cybersecurity (ENISA). (2020). *ENISA Report on CSIRT-LE Cooperation: A study of the roles and synergies among selected countries*. Publications Office of the European Union. <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20on%20CSIRT-LE%20Cooperation%20-%20A%20study%20of%20the%20roles%20and%20synergies%20among%20selected%20countries.pdf> [accessed: 29.10.2025].
- European Union Agency for Criminal Justice Cooperation (Eurojust). (n.d.). *Joint investigation teams (JITs)*. <https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams> [accessed: 23.10.2025].
- European Union Agency for Law Enforcement Cooperation (Europol). (n.d.-a). *About Europol*. <https://www.europol.europa.eu/about-europol> [accessed: 23.10.2025].
- European Union Agency for Law Enforcement Cooperation (Europol). (n.d.-c). *Information exchange*. <https://www.europol.europa.eu/how-we-work/services-support/information-exchange> [accessed: 23.10.2025].
- European Union Agency for Law Enforcement Cooperation (Europol). (n.d.-f). *Secure Information Exchange Network Application (SIENA)*. <https://www.europol.europa.eu/how-we-work/services-support/information-exchange/secure-information-exchange-network-application-siena> [accessed: 29.10.2025].
- European Union Agency for Law Enforcement Cooperation (Europol). (n.d.-g). *Sirius Project*. <https://www.europol.europa.eu/how-we-work/sirius-project> [accessed: 24.10.2025].
- European Union Agency for Law Enforcement Cooperation (Europol). (2016, November 22). *178 arrests in successful hit against money muling*. <https://www.europol.europa.eu/media-press/newsroom/news/178-arrests-in-successful-hit-against-money-muling> [accessed: 28.10.2025].
- European Union Agency for Law Enforcement Cooperation (Europol). (2020, July 2). *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*. <https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe> [accessed: 28.10.2025].
- European Union Agency for Law Enforcement Cooperation (Europol). (2024). *Decoding the EU's most threatening criminal networks*. Publications Office of the European Union. <https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20report%20on%20Decoding%20the%20EU-s%20most%20threatening%20criminal%20networks.pdf> [accessed: 30.10.2025].
- Farrell, C.C., & Coburn, C.E. (2017). Absorptive capacity: A conceptual framework for understanding district central office learning. *Journal of Educational Change*, 18, 135–159. <https://doi.org/10.1007/s10833-016-9291-7>
- Fotiadis, A., Stavinoha, L., Zandonini, G., Howden, D. (2022, January 10). A data black hole: Europol ordered to delete vast store of personal data. *The Guardian*. <https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data> [accessed 3.11.2025].
- Frontex. (n.d.-a). *Career development*. <https://www.frontex.europa.eu/careers/what-we-offer/career-development/> [accessed: 23.10.2025].
- Frontex. (n.d.-c). *Trainings at Frontex*. <https://www.frontex.europa.eu/training/trainings-at-frontex/> [accessed: 23.10.2025].

- Harvey, G., Jas, P., Walshe, K., Skelcher, C. (2010). Absorptive capacity: how organisations assimilate and apply knowledge to improve performance. In: K. Walshe, G. Harvey, P. Jas (Eds.), *Connecting Knowledge and Performance in Public Services: From Knowing to Doing* (pp. 226–250). Cambridge University Press.
- Kanaan N., & Mayer J.C. (2023). Revealing the spatiality of crises: Lessons from failures of boundary work in a cross-border crisis. *M@n@gement*, 26(4), 16–34. <https://doi.org/10.37725/mgmt.2023.8104>
- Lawrence, T.B., Mauws, M.K., Dyck, B., & Kleysen, R.F. (2005). The politics of organizational learning: Integrating politics and the 4I framework. *Academy of Management Review*, 30(1), 180–191. <https://doi.org/10.5465/AMR.2005.15281451>
- Nuño-Solinis, R. & Urtaran-Laresgoiti, M. (2018). Learning from integrated care top performers in Spain. *International Journal of Integrated Care*, 18(S2), Article 4. <https://doi.org/10.5334/ijic.s2004>
- Safański, T., James, A. (2020). Europol's Crime Analysis System – Practical Determinants of Its Success, *Policing: A Journal of Policy and Practice*, 14(2), 469–478. <https://doi.org/10.1093/police/pay021>
- Serrat, O. (2017). Knowledge as Culture. In: *Knowledge Solutions: Tools, Methods, and Approaches to Drive Organizational Performance* (pp. 523–557). Springer. https://doi.org/10.1007/978-981-10-0983-9_58
- Statewatch. (2025, February 27). *Behind closed doors: Europol's opaque relations with tech companies*. <https://www.statewatch.org/analyses/2025/behind-closed-doors-europol-s-opaque-relations-with-tech-companies/> [accessed: 3.11.2025].
- United Nations Office on Drugs and Crime (UNODC). (n.d.). *Case studies: Operation "Valter"*. <https://www.unodc.org/e4j/en/organized-crime/module-7/exercises/case-studies.html> [accessed: 4.11.2025].
- Walsh, J. I. (2006). Intelligence-sharing in the European Union: Institutions are not enough. *Journal of Common Market Studies*, 44(3), 625–643. <https://www.jamesigoewalsh.com/jcms.pdf> [accessed: 5.11.2025].

Key barriers to inter-organizational learning in the European security ecosystem

Abstract

This article analyzes the mechanisms and barriers to inter-organizational learning (IOL) in the European Union's security sector. The research aims to diagnose why effective IOL remains a systemic challenge despite significant institutional and technological investments. Using a targeted literature review and case study synthesis mapped against the 4I and Absorptive Capacity theoretical frameworks, the study identifies a fundamental tension termed the *sovereignty paradigm*. The analysis of key agencies (Europol, Frontex, ENISA) and specific operations (Paris and Brussels attacks, Joint Investigation Teams) reveals that the main obstacles are not technical. Rather, they are rooted in political and cultural barriers, specifically a chronic lack of trust, conflicting mandates, and cultures resistant to critical feedback. The article concludes that improving IOL requires a strategic shift from investing in centralized technological platforms to building bottom-up, relationship-based human networks capable of generating trust.

Keywords: inter-organizational learning (IOL), European security, European Union, Europol, Frontex, information sharing, trust, absorptive capacity

Author Contributions

Conceptualization: M.duV.

Methodology: M.duV.

Formal analysis: M.duV.

Investigation: M.duV.

Resources: M.duV.

Writing – original draft: M.duV.

Writing – review & editing: M.duV.

Supplementary Materials

Not applicable.

Funding

This research received no external funding.

Ethics Approval Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Data sharing is not applicable to this article as no new data were generated or analyzed in this study.

Declaration of Generative AI Use

No artificial intelligence tools were used in the preparation of this manuscript.

Acknowledgments

Not applicable.

Conflict of Interest

Marta du Vall joined the editorial team of *Security: Theory and Practice* as a thematic section editor in July 2026. The editorial and peer review processes for this manuscript were fully completed prior to this appointment. The article was submitted on November 17, 2025, and accepted on March 5, 2026. The author had no role in the editorial handling or decision-making process of this manuscript.

Postrzeganie bezpieczeństwa przez turystów przyjeżdżających do Zjednoczonych Emiratów Arabskich w kontekście usług hotelarskich segmentu premium

Izabela Kapera

dr hab., prof. UAFM, Wydział Zarządzania, Mediów i Technologii,
Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie (Faculty of Management,
Media and Technology, Andrzej Frycz Modrzewski Krakow University, Kraków, Poland)
<https://orcid.org/0000-0003-1691-5275>

Wprowadzenie

Bezpieczeństwo w usługach hotelarskich stanowi zagadnienie wielowymiarowe i jest powszechnie uznawane za jeden z kluczowych elementów jakości usług turystycznych, wpływający zarówno na komfort oraz zaufanie klientów, jak i na postrzeganie całości doświadczenia turystycznego. W literaturze przedmiotu problematyka bezpieczeństwa w hotelarstwie analizowana jest na wielu płaszczyznach – od aspektów technicznych i organizacyjnych, poprzez regulacyjne i prawne, aż po zachowania konsumentów oraz percepcję ryzyka. Zakres tych analiz obejmuje zarówno odpowiedzialność hotelarza oraz przestrzeganie obowiązujących przepisów, jak i identyfikację zagrożeń, a także wdrażanie rozwiązań organizacyjno-technicznych służących ich ograniczaniu.

W literaturze polskiej zagadnienia bezpieczeństwa w hotelarstwie były już podejmowane. Przykładem są analizy Kapery i Kapery (2014), którzy wskazują na szerokie spektrum zagrożeń występujących w obiektach hotelowych (obejmujących czynniki

wewnętrzne i zewnętrzne), odpowiedzialność hotelarza za bezpieczeństwo gości oraz konieczność systemowego podejścia do identyfikacji i minimalizacji ryzyka. Rozwijając perspektywę zarządczą, Podwysocka (2024) zwraca uwagę na znaczenie bezpieczeństwa jako integralnego elementu systemu zarządzania kryzysowego w branży hotelarskiej. Szersze ujęcie dotyczące zagadnień bezpieczeństwa prezentuje Chodyński (2021; 2024), analizując je w kontekście rezyliencji organizacyjnej. Autor wskazuje, że zdolność organizacji do utrzymania stabilności oraz adaptacji w warunkach kryzysowych stanowi fundament jej długofalowego funkcjonowania, a bezpieczeństwo jest tym ujęciu jednym z kluczowych filarów rezyliencji. Znaczenie zarządzania bezpieczeństwem w hotelarstwie podkreślają również Chodyński, Podwysocka, Wolak i Kapera (2024), wskazując, że skuteczne przeciwdziałanie sytuacjom kryzysowym wymaga uwzględnienia oczekiwań zarówno interesariuszy wewnętrznych, jak i zewnętrznych. Dla pełniejszego ujęcia problematyki zasadne jest odróżnienie bezpieczeństwa jako kategorii organizacyjnej od percepcji bezpieczeństwa jako kategorii poznawczej i społecznej. W naukach o zarządzaniu bezpieczeństwo bywa ujmowane przez pryzmat rozwiązań strukturalnych, procedur, nadzoru i kontroli ryzyka, natomiast percepcja bezpieczeństwa odnosi się do sposobu, w jaki uczestnicy organizacji lub odbiorcy usług interpretują poziom zagrożenia oraz skuteczność stosowanych zabezpieczeń. Problematyka ta znajduje szerokie odzwierciedlenie w literaturze międzynarodowej. W przeglądach dotyczących ryzyka w turystyce podkreśla się, że percepcja zagrożeń ma charakter wielowymiarowy i wpływa zarówno na wybory podróży, jak i na ocenę jakości doświadczenia turystycznego (Yang i Nair, 2014; Seabra, Dolnicar, Abrantes i Kastenholz, 2013). W odniesieniu do hotelarstwa badania Chan, Leung i Lo (2013) pokazują, że bezpieczeństwo i zabezpieczenia należą do istotnych kryteriów oceny obiektu, przy czym między perspektywą zarządzających a oczekiwaniami gości mogą występować wyraźne rozbieżności. Z kolei Berezina, Cobanoglu, Miller i Kwansa (2012) zwracają uwagę, że naruszenia bezpieczeństwa informacyjnego również oddziałują na postrzeganą jakość usług hotelowych i zaufanie klientów.

Jednocześnie w nowszych badaniach coraz większą uwagę poświęca się percepcji bezpieczeństwa z perspektywy odbiorców usług. Bezpieczeństwo nie jest wówczas rozumiane wyłącznie jako zbiór formalnych rozwiązań funkcjonalnych i organizacyjnych, lecz jako subiektywne poczucie gościa, kształtowane przez doświadczenia pobytu, kontakt z personelem oraz sposób organizacji przestrzeni hotelowej. Taki kierunek interpretacji pozostaje zbieżny z dorobkiem badań, który wskazuje na to, że recenzje internetowe traktowane są jako ważne źródło wiedzy o doświadczeniach konsumentów, redukcji postrzeganego ryzyka oraz procesach decyzyjnych w turystyce i hotelarstwie (Sparks i Browning, 2011; Marine-Roig i Huertas, 2020; Yadav, Verma i Chikhalkar, 2024). Zaproponowana w artykule analiza opinii gości publikowanych na platformach internetowych umożliwia uchwycenie tych aspektów bezpieczeństwa, które nie zawsze znajdują odzwierciedlenie w przepisach, projektowaniu czy procedurach dotyczących obiektów.

Pomimo rosnącej liczby publikacji poświęconych bezpieczeństwu w hotelarstwie, widoczna pozostaje luka badawcza odnosząca się do segmentu premium oraz do rynków pozaeuropejskich. Segment ten obejmuje obiekty i usługi o ponadstandardowej jakości, w których kluczową rolę odgrywają takie cechy jak wysoki poziom personalizacji, prywatność oraz rozbudowane mechanizmy kontroli procesów. Na łamach literatury naukowej sektor premium w turystyce jest najczęściej konceptualizowany poprzez pojęcia turystyki luksusowej oraz hotelarstwa w obiektach o wysokim standardzie. W badaniach dotyczących doświadczeń gości zauważa się, że poczucie i oczekiwania wobec bezpieczeństwa w tego typu miejscach rzadko są artykułowane wprost, lecz odnoszą się na przykład do sposobu organizacji przestrzeni czy zachowaniu personelu.

Zjednoczone Emiraty Arabskie postrzegane są jako jeden ze światowych liderów w zakresie turystyki luksusowej, a rynek hotelarski tego państwa charakteryzuje się dużą liczbą obiektów segmentu premium oraz szeroko rozwiniętą ofertą usługową. W tym kontekście problematyka bezpieczeństwa nabiera szczególnego znaczenia – zarówno jako element zarządzania w hotelarstwie, jak i jako istotna składowa wizerunku destynacji turystycznej.

W odpowiedzi na zidentyfikowaną lukę badawczą artykuł podejmuje problematykę percepcji bezpieczeństwa w doświadczeniach turystów korzystających z usług hotelarskich segmentu premium w Zjednoczonych Emiratach Arabskich. Analiza oparta została na materiałach źródłowych, obserwacjach własnych dokonanych podczas pobytu w badanej destynacji i wizytach w wybranych hotelach, a także na jakościowej analizie ponad 70 000 opinii internautów publikowanych w Internecie (Tripadvisor i Google Reviews). Szczególną uwagę poświęcono aspektom bezpieczeństwa zarówno artykułowanym wprost, jak i ujawniającym się pośrednio w narracjach gości. Celem artykułu jest zbadanie sposobów postrzegania kwestii bezpieczeństwa przez gości korzystających z usług hotelarskich segmentu premium w Zjednoczonych Emiratach Arabskich.

Metoda badawcza

W postępowaniu badawczym zastosowano: analizę materiałów źródłowych, obserwację własną oraz jakościową analizę opinii gości publikowanych na platformach internetowych.

Analiza materiałów źródłowych objęła literaturę przedmiotu, raporty branżowe oraz dokumenty dotyczące bezpieczeństwa w hotelarstwie. Obserwacja własna została przeprowadzona podczas pobytu w Zjednoczonych Emiratach Arabskich i obejmowała wizyty w wybranych obiektach hotelowych segmentu premium (Jumeirah Burj Al Arab w Dubaju, Emirates Palace Mandarin Oriental w Abu Zabi). Kluczowym elementem badania była jakościowa analiza treści opinii gości

publikowanych na platformach Tripadvisor i Google Reviews. Analizie poddano recenzje odnoszące się do pobytów w obu hotelach, przy czym szczególną uwagę zwrócono zarówno na bezpośrednie wzmianki dotyczące bezpieczeństwa, jak i na odniesienia pośrednie, takie jak kwestie prywatności, czystości, organizacji przestrzeni czy zachowania personelu. Bazowano na publicznie dostępnych opiniach dotyczących hoteli segmentu premium w Zjednoczonych Emiratach Arabskich i ze względu na bardzo dużą liczbę recenzji zastosowano projekt dwustopniowy. W celu identyfikacji opinii bezpośrednio odnoszących się do bezpieczeństwa przeprowadzono kwerendę treści z wykorzystaniem słów kluczowych: *safe, safety, secure, security* (oraz ich form negatywnych: *unsafe, insecure*). To pozwoliło wyodrębnić recenzje, w których kwestie bezpieczeństwa były artykułowane wprost. W celu zapewnienia jakości materiału badawczego przeprowadzono weryfikację treści opinii pod kątem ich kompletności oraz zgodności z przyjętym zakresem analizy. Wpisy niejednoznaczne klasyfikowano na podstawie analizy kontekstu całej wypowiedzi, a przypisanie do kategorii następowało według dominującego wątku znaczeniowego. Analizie poddano wyłącznie opinie sformułowane w języku angielskim, co zapewnia spójność semantyczną materiału empirycznego oraz porównywalność narracji gości pochodzących z różnych krajów, lecz zawęża reprezentację zróżnicowanej językowo grupy gości.

Przypisanie fragmentów opinii do kategorii analitycznych opierało się na identyfikacji słów i wyrażeń kluczowych, a w dalszym postępowaniu – ich interpretacji w kontekście całej wypowiedzi. W drugim etapie przeprowadzono także pogłębioną analizę jakościową opinii pośrednio związanych z bezpieczeństwem (tabela 1). Łącznie przeanalizowano 37 741 opinii dotyczących Jumeirah Burj Al Arab i 33 287 wypowiedzi na temat Emirates Palace Mandarin Oriental, Abu Dhabi (tabela 2). Zebrane opinie odzwierciedlają stan widoczny na platformach rezerwacyjnych na dzień 30 grudnia 2025 r., przy czym liczba publicznie dostępnych recenzji może ulegać zmianom w wyniku aktualizacji danych, moderacji treści oraz publikowania nowych opinii.

Tabela 1. Charakterystyka postępowania badawczego

Element opisu	Charakterystyka
Obszar badań	Zjednoczone Emiraty Arabskie (Dubaj, Abu Zabi)
Analizowane obiekty	Jumeirah Burj Al Arab; Emirates Palace Mandarin Oriental, Abu Dhabi
Segment hotelarski	Segment premium (luksusowy)
Źródła danych	Tripadvisor, Google Reviews
Etap I badania	Kwerenda tematyczna opinii zawierających słowa kluczowe odnoszące się do bezpieczeństwa
Etap II badania	Pogłębiona analiza jakościowa opinii

Źródło: opracowanie własne.

Tabela 2. Liczba opinii – Tripadvisor i Google Reviews – dotyczących wybranych hoteli (stan w dniu 30.12.2025)

Hotel	Tripadvisor – liczba opinii	Google Reviews – liczba opinii
Jumeirah Burj Al Arab (Dubaj)	7154	30 587
Emirates Palace Mandarin Oriental, Abu Dhabi	2196	31 091

Źródło: opracowanie własne na podstawie: *Emirates Palace Mandarin Oriental, Abu Dhabi*. Tripadvisor. https://www.tripadvisor.com/Hotel_Review-g294013-d507156-Reviews-Emirates_Palace_Mandarin_Oriental-Abu_Dhabi_Emirate_of_Abu_Dhabi.html [dostęp: 31.12.2025]; *Emirates Palace Mandarin Oriental, Abu Dhabi*. Google Maps – Reviews. <https://www.google.com/maps/place/Emirates+Palace+Mandarin+Oriental> [dostęp: 31.12.2025]; *Jumeirah Burj Al Arab*. Google Maps – Reviews. <https://www.google.com/maps/place/Jumeirah+Burj+Al+Arab> [dostęp: 31.12.2025]; *Jumeirah Burj Al Arab*. Tripadvisor. https://www.tripadvisor.com/Hotel_Review-g295424-d302457-Reviews-Burj_Al_Arab_Jumeirah-Dubai.html [dostęp: 31.12.2025].

Obszar badań

Obszar badań stanowiły Zjednoczone Emiraty Arabskie – kraj będący przykładem dynamicznie rozwijającego się rynku turystyki luksusowej.

Dane statystyczne pokazują, że w drugiej połowie ostatniej dekady ZEA osiągały wysokie poziomy przyjazdów turystycznych. W 2015 roku liczba międzynarodowych przyjazdów turystycznych w ZEA wyniosła ponad 19,3 mln, następnie systematycznie rosła i osiągnęła 25,3 mln w 2019 roku, co stanowiło rekordowy poziom przed pandemią COVID-19 (CEIC Data, 2025). W 2020 roku, w wyniku globalnych ograniczeń podróży związanych z pandemią, liczba przyjazdów spadła do niemal 8,1 mln – było to znaczące obniżenie w porównaniu z 2019 rokiem i jeden z najniższych wyników w analizowanym okresie (CEIC Data, 2025).

Po okresie spadków sektor turystyczny w ZEA zaczął się sukcesywnie odbudowywać. Na poziomie globalnym turystyka międzynarodowa zbliżyła się do wyników sprzed pandemii w 2023 i 2024 roku, co znajduje odzwierciedlenie także w statystykach dla ZEA. Generalnie przemysł turystyczny cechuje się wysokim poziomem rezyliencji i – z wyjątkiem długotrwałych konfliktów zbrojnych – jest zdolny do pełnej odbudowy po różnorodnych kryzysach (Mansfeld i Pizam, 2006). Szczegółowe dane z destynacji wskazują, że Dubaj, który był dominującym ośrodkiem turystycznym w ZEA, przyjął około 17,15 mln międzynarodowych turystów nocujących w 2023 roku, co stanowiło wzrost o ok. 19% w porównaniu z 2022 rokiem i przewyższyło wcześniejszy rekord z 2019 roku (Alrashdi, 2024). W 2024 roku liczba ta wzrosła do 18,72 mln (wzrost o około 9% rok do roku i nowy rekord odwiedzin) (Dubai Department of Economy and Tourism [DET], 2025; Global Media Insight 2025). Trend ten potwierdza szybką odbudowę sektora turystycznego w ZEA po okresie ograniczeń pandemicznych oraz silne przyciąganie kraju jako destynacji turystycznej. Według oficjalnych danych federalnych, w pierwszej

połowie 2024 roku w ZEA funkcjonowało ponad 213,7 tys. pokoi hotelowych we wszystkich emiratach (Ministry of Economy, 2024). Wcześniejsze dane ministerialne wskazują, że w 2022 roku w Zjednoczonych Emiratach Arabskich działało 1189 hoteli, oferujących około 203 tys. pokoi (Ministry of Economy, 2022). Największym i najważniejszym rynkiem hotelowym w ZEA pozostawał Dubaj, który koncentrował zdecydowaną większość krajowej podaży hotelowej. Zgodnie z danymi Dubai Department of Economy and Tourism, na koniec 2024 roku w Dubaju funkcjonowały 832 obiekty hotelowe, oferujące łącznie 154 016 pokoi (DET, 2024). Struktura tej podaży wskazuje na silną orientację emiratów na segment wysokiego standardu – około 35% pokoi hotelowych w Dubaju należało do hoteli pięciogwiazdkowych, a kolejne 28% – do hoteli czterogwiazdkowych (Emirates NBD Research, 2025).

Drugim pod względem wielkości rynkiem hotelowym była stolica kraju. Dane publikowane przez władze emiratu oraz materiały prasowe oparte na oficjalnych statystykach wskazują, że w 2024 roku w Abu Zabi funkcjonowało około 171 hoteli, oferujących ponad 34 tys. pokoi (Aletihad 2025). Struktura bazy hotelowej emiratu charakteryzowała się także znaczącym udziałem obiektów luksusowych. Istotną rolę w krajowej strukturze hotelowej odgrywała również Szardża, która w ostatnich latach systematycznie rozwijała ofertę noclegową. Według danych Sharjah Commerce and Tourism Development Authority, w 2024 roku w emiracie działało 101 hoteli (Sharjah Commerce and Tourism Development Authority, 2025). Mniejsze emiraty, takie jak Adżman, Ras al-Chajma czy Fudżajra, również rozwijały swoją bazę hotelową, choć na znacznie mniejszą skalę. Przykładowo, według danych branżowych w Adżmanie funkcjonowały w 2024 roku 52 hotele, oferujące około 4315 pokoi, co wskazuje na stopniowy rozwój infrastruktury noclegowej w emiratach o mniejszym natężeniu ruchu turystycznego (Connecting Travel, 2024). Analiza struktury bazy hotelowej w Zjednoczonych Emiratach Arabskich pokazuje wyraźną dominację segmentu luksusowego oraz wysoką koncentrację podaży w Dubaju i Abu Zabi. Jednocześnie obserwowany wzrost liczby hoteli w pozostałych emiratach świadczył o stopniowej dywersyfikacji przestrzennej oferty noclegowej i rosnącym znaczeniu turystyki jako czynnika rozwoju regionalnego w skali całego kraju.

Przeprowadzone badanie koncentruje się na wybranych obiektach hotelarskich segmentu premium zlokalizowanych w Dubaju i Abu Zabi, będących rozpoznawalnymi symbolami luksusu i wysokich standardów obsługi. Do badań wybrano następujące hotele: Jumeirah Burj Al Arab w Dubaju i Emirates Palace Mandarin Oriental w Abu Zabi. Przynależność obu obiektów do segmentu premium wynika z kumulacji cech charakterystycznych dla dóbr i usług luksusowych, obejmujących ekskluzywność, wysoki standard infrastruktury, intensywną personalizację świadczeń oraz symboliczny wymiar prestiżu.

Hotele te charakteryzują się wysoką rozpoznawalnością międzynarodową, dużą liczbą opinii publikowanych przez gości oraz zróżnicowaną ofertą usługową, co czyni je odpowiednim polem badawczym do analizy postrzegania bezpieczeństwa w hotelarstwie segmentu premium.

Jumeirah Burj Al Arab to jeden z najbardziej rozpoznawalnych symboli Dubaju i zarazem przykład hotelu, którego znaczenie wykracza poza funkcję noclegową – obiekt jest ikoną urbanistyki i swego rodzaju wizytówką destynacji oraz narzędziem budowania marki luksusu.

Bywa on wskazywany jako flagowy element architektury Dubaju oraz przykład obiektu, którego powstanie wpisywało się w proces transformacji miasta i wzmacniało przekonanie o możliwości realizacji ambitnych projektów wysokościowych w jego przestrzeni (Hammad, 2020). Jak zauważa Tawfik (2023), Burj Al Arab to modelowy przykład, jak estetyka luksusu materializuje się w formach przestrzennych, rozwiązaniach projektowych oraz symbolice architektury.

Drugi z wybranych obiektów, Emirates Palace Mandarin Oriental, Abu Dhabi, to także jeden z najbardziej reprezentacyjnych przykładów luksusowego hotelarstwa w Zjednoczonych Emiratach Arabskich. Poza istotną rolę w turystyce, obiekt ma również znaczenie symboliczne, kulturowe i gospodarcze dla stolicy kraju. Hotel został otwarty w 2005 roku jako Emirates Palace i od początku pełnił podwójną funkcję: ekskluzywnego obiektu hotelowego oraz miejsca oficjalnych wydarzeń państwowych, dyplomatycznych i międzynarodowych. W 2020 roku przeszedł pod zarządzanie sieci Mandarin Oriental, zachowując swoją architektoniczną i prestiżową tożsamość.

Wyniki i analiza badań

Przeprowadzona analiza opinii gości luksusowych hoteli w Zjednoczonych Emiratach Arabskich, opublikowanych na platformach Tripadvisor oraz Google Reviews, umożliwiła wielowymiarowe ujęcie zagadnień bezpieczeństwa w hotelarstwie segmentu premium. Badanie objęło łącznie ponad 71 tysięcy recenzji dotyczących dwóch obiektów o zbliżonym prestiżu rynkowym, lecz odmiennych strategiach organizacyjnych: Emirates Palace Mandarin Oriental, Abu Dhabi oraz Jumeirah Burj Al Arab.

Uzyskane wyniki pozwalają sformułować wnioski wykraczające poza prostą ocenę poziomu bezpieczeństwa i skoncentrować się na jego percepcji, narracyjnym ujawnianiu oraz roli w zarządzaniu doświadczeniem gościa.

Na poziomie ogólnym analiza wykazała wysoką spójność wyników niezależnie od platformy publikacji opinii. W obu hotelach bezpieczeństwo funkcjonuje przede wszystkim jako domyślny standard luksusu, a nie jako problem wymagający częstego werbalizowania. Marginalna obecność pojęć *unsafe* oraz *insecure* (tabela 3) w analizowanych zbiorach świadczy o wysokim poziomie zaufania gości do samych obiektów.

W tym sensie bezpieczeństwo przejawia się raczej w braku narracji o zagrożeniu niż w bezpośrednich deklaracjach dotyczących jego odczuwania. Jak wynika z przeprowadzonej analizy, pojęcia *safe* i *safety* odnoszą się do emocjonalnego komfortu, spokoju, poczucia opieki oraz rodzinnego charakteru pobytu. Są one wykorzystywane jako element pozytywnej oceny doświadczenia, rzadko natomiast jako narzędzie refleksji nad konkretnymi zagrożeniami czy procedurami ochronnymi. Z kolei termin *security* koncentruje się wokół sfery operacyjnej: personelu ochrony, kontroli dostępu, weryfikacji uprawnień oraz organizacji przestrzeni. To właśnie w odniesieniu do *security* pojawiają się najbardziej szczegółowe, a zarazem najbardziej krytyczne narracje.

Tabela 3. Porównanie częstości użycia słów związanych z bezpieczeństwem w opiniach gości hoteli Jumeirah Burj Al Arab i Emirates Palace Mandarin Oriental, Abu Dhabi na platformie Tripadvisor i Google Reviews

	<i>safe</i>	<i>safety</i>	<i>secure</i>	<i>security</i>	<i>unsafe</i>	<i>insecure</i>
Tripadvisor						
Jumeirah Burj Al Arab	30	10	19	197	1	0
Emirates Palace Mandarin Oriental, Abu Dhabi	11	6	2	28	1	1
Google Reviews						
Jumeirah Burj Al Arab	15	0	14	50	0	0
Emirates Palace Mandarin Oriental, Abu Dhabi	11	0	2	20	2	0

Źródło: opracowanie własne na podstawie danych z: *Emirates Palace Mandarin Oriental, Abu Dhabi*. Tripadvisor. https://www.tripadvisor.com/Hotel_Review-g294013-d507156-Reviews-Emirates_Palace_Mandarin_Oriental-Abu_Dhabi_Emirate_of_Abu_Dhabi.html [dostęp: 31.12.2025]; *Emirates Palace Mandarin Oriental, Abu Dhabi*. Google Maps – Reviews. <https://www.google.com/maps/place/Emirates+Palace+Mandarin+Oriental> [dostęp: 31.12.2025]; *Jumeirah Burj Al Arab*. Google Maps – Reviews. <https://www.google.com/maps/place/Jumeirah+Burj+Al+Arab> [dostęp: 31.12.2025]; *Jumeirah Burj Al Arab*. Tripadvisor. https://www.tripadvisor.com/Hotel_Review-g295424-d302457-Reviews-Burj_Al_Arab_Jumeirah-Dubai.html [dostęp: 31.12.2025].

Istotnym wnioskiem jest fakt, że krytyka obecna w opiniach gości nie dotyczy braku bezpieczeństwa jako takiego, lecz stylu jego realizacji. Negatywne wypowiedzi odnoszą się przede wszystkim do sposobu komunikacji personelu ochrony, proporcjonalności kontroli, elastyczności procedur oraz pojedynczych uchybień operacyjnych. Nawet incydentalne użycia pojęcia *unsafe* mają charakter punktowy i odnoszą się do konkretnych problemów infrastrukturalnych, nie podważając ogólnego poczucia bezpieczeństwa w obiekcie. Brak narracji o trwałym zagrożeniu potwierdza, że bezpieczeństwo w badanym segmencie hotelarstwa jest postrzegane jako norma, a nie jako wartość wyróżniająca.

Na tym tle szczególnie wyraźnie ujawniają się różnice pomiędzy analizowanymi hotelami, które dotyczą nie poziomu ochrony, lecz modelu zarządzania bezpieczeństwem i sposobu jego doświadczania przez gości. Emirates Palace Mandarin

Oriental, Abu Dhabi reprezentuje model bezpieczeństwa wbudowanego w kulturę organizacyjną, styl obsługi oraz relacje z gośćmi. Ochrona działa dyskretnie, pozostając w tle codziennego doświadczenia pobytu. W narracjach gości bezpieczeństwo wzmacnia poczucie spokoju, komfortu psychicznego oraz rodzinnej swobody, szczególnie w kontekście dzieci, infrastruktury rekreacyjnej i rozległej przestrzeni obiektu. Język opinii sugeruje, że bezpieczeństwo jest tu zarządzane poprzez zaufanie, empatię i obecność wspierającą, a nie poprzez restrykcję czy nadmierną kontrolę.

W przypadku Jumeirah Burj Al Arab bezpieczeństwo stanowi wyraźny element struktury organizacyjnej oraz narracji marki. Goście mają silną świadomość obecności ochrony, punktów kontrolnych i zasad dostępu, które pełnią nie tylko funkcję zabezpieczającą, lecz także selekcyjną i symboliczną. Bezpieczeństwo jest tu integralnym składnikiem ekskluzywności i prestiżu, ale jednocześnie bywa doświadczane ambiwalentnie. W ocenach pojawia się napięcie pomiędzy logiką ochrony a logiką gościnności – bezpieczeństwo może wzmacniać poczucie wyjątkowości, lecz w niektórych sytuacjach generować dyskomfort, poczucie nadmiernej kontroli lub ograniczenia swobody.

Porównanie opinii publikowanych na obu platformach pozwala stwierdzić, że postrzeganie bezpieczeństwa jest zasadniczo zbieżne, choć ujawnia się poprzez różne akcenty znaczeniowe. Z perspektywy praktyki zarządzania oznacza to potrzebę takiego projektowania rozwiązań ochronnych, aby były one skuteczne, ale zarazem możliwie dyskretne, proporcjonalne i spójne z doświadczeniem pobytu w obiekcie premium. Szczególnego znaczenia nabiera komunikacja personelu z gośćmi, ponieważ sposób wyjaśniania procedur, styl interakcji oraz kultura obsługi współdecydują o tym, czy środki bezpieczeństwa są odbierane jako element troski, czy jako źródło dystansu i dyskomfortu. Wnioski te wskazują również, że w hotelarstwie premium bezpieczeństwo powinno być uwzględniane nie tylko w procedurach ochrony, lecz także w projektowaniu przestrzeni, organizacji ruchu gości oraz standardach kontaktu personelu z klientem.

Podsumowanie

Przeprowadzone badanie miało na celu analizę postrzegania bezpieczeństwa przez turystów korzystających z hoteli segmentu premium w Zjednoczonych Emiratach Arabskich na podstawie opinii publikowanych na dwóch wiodących platformach turystycznych – Tripadvisor oraz Google. Zastosowane metody pozwoliły uchwycić bezpieczeństwo nie tylko jako techniczny element funkcjonowania obiektów hotelowych, lecz przede wszystkim jako istotny komponent doświadczenia turystycznego oraz narzędzie zarządzania relacjami z gośćmi.

Uzyskane wyniki wskazują, że w narracjach gości bezpieczeństwo rzadko jest artykułowane wprost. Może to świadczyć o jego postrzeganiu jako elementu oczywistego

i domyślnego w hotelarstwie luksusowym oraz o wysokim poziomie zaufania do funkcjonujących rozwiązań ochronnych. Skuteczność systemów bezpieczeństwa ujawnia się zatem głównie w braku narracji o zagrożeniu, a nie w częstym deklarowaniu poczucia bezpieczeństwa. Jednocześnie kwestie te pojawiają się pośrednio poprzez odniesienia do komfortu psychicznego, spokoju, prywatności, czystości obiektu oraz profesjonalizmu personelu, co podkreśla ich znaczenie dla całościowego odbioru jakości pobytu. W przypadku Zjednoczonych Emiratów Arabskich, a zwłaszcza hoteli segmentu premium, bezpieczeństwo jest oczekiwane, lecz niewidoczne, dopóki nie zostanie naruszone.

Porównanie dwóch hoteli o zbliżonym poziomie prestiżu, lecz odmiennych strategiach organizacyjnych, pozwoliło zidentyfikować różne modele realizacji bezpieczeństwa w hotelarstwie segmentu premium. W jednym przypadku bezpieczeństwo przyjmuje formę relacyjną i dyskretną, opartą na zaufaniu oraz braku ostentacyjności działań ochronnych, co wzmacnia poczucie spokoju i swobody gości. W drugim modelu bezpieczeństwo ma charakter bardziej proceduralny i widoczny, co podkreśla ekskluzywność i selektywność dostępu, lecz jednocześnie tworzy ambiwalentne doświadczenia gości. Oba podejścia okazują się funkcjonalnie skuteczne, jednak prowadzą do odmiennych narracji w opiniach internetowych.

Wyniki badania wpisują się w ustalenia literatury dotyczącej zarządzania bezpieczeństwem i rezyliencji organizacyjnej, potwierdzając, że skuteczne systemy ochrony w hotelarstwie luksusowym cechują się wysoką efektywnością przy jednoczesnej niskiej widoczności dla klienta. Szczególne znaczenie ma w tym kontekście bezpieczeństwo rozumiane nie tylko jako ochrona przed zagrożeniami, lecz także jako element doświadczenia gościa, obejmujący poczucie komfortu, sprawczości i zaufania. Tak ujmowane bezpieczeństwo istotnie wpływa na postrzeganie jakości usług oraz satysfakcję gości.

Przeprowadzone badanie potwierdza również zasadność wykorzystania analizy opinii internetowych w badaniach nad bezpieczeństwem w turystyce. Metoda ta umożliwia identyfikację subtelnych mechanizmów percepcyjnych i narracyjnych, trudnych do uchwycenia za pomocą klasycznych metod ilościowych, a jednocześnie dostarcza wiedzy istotnej zarówno z perspektywy teoretycznej, jak i praktyki zarządzania w hotelarstwie segmentu premium.

Ograniczenia badania

Przedstawione badanie ma pewne ograniczenia, które należy uwzględnić przy interpretacji uzyskanych wyników. Przede wszystkim trzeba zaznaczyć, że ocena poziomu bezpieczeństwa w hotelarstwie ZEA wymaga uwzględnienia zmieniających się uwarunkowań regionalnych i geopolitycznych, które mogą okresowo wpływać na percepcję bezpieczeństwa oraz funkcjonowanie sektora turystycznego. Po drugie analiza

opiera się na opiniach gości publikowanych na platformach Tripadvisor i Google Reviews, które odzwierciedlają indywidualne doświadczenia oraz sposoby narracyjnego ujmowania kwestii bezpieczeństwa, a nie pełny obraz rozwiązań organizacyjnych stosowanych w badanych obiektach. Dodatkowo badanie koncentruje się wyłącznie na hotelach segmentu premium, co ogranicza możliwość generalizacji wyników na inne segmenty rynku hotelarskiego oraz odmienne konteksty kulturowe i destynacje turystyczne.

Pomimo wskazanych ograniczeń przyjęte podejście pozwala na identyfikację sposobów, w jakie zagadnienia bezpieczeństwa ujawniają się w narracjach gości luksusowych hoteli, oraz potwierdza użyteczność opinii internetowych jako źródła wiedzy wspierającej zarządzanie bezpieczeństwem i doświadczeniem gościa w hotelarstwie segmentu premium.

Bibliografia

- Abu Dhabi Media Office. (2024). *Department of Culture and Tourism – Abu Dhabi records 4.8m hotel visitors received in emirate in 2024*. Abu Dhabi Government Media Office. <https://www.mediaoffice.abudhabi/en/tourism/department-of-culture-and-tourism-abu-dhabi-records-4m-hotel-visitors-received-in-emirate-in-2024/> [dostęp: 30.12.2025].
- Aletihad. (2025, January 15). *Abu Dhabi hotel sector booms with 5.8 million guests in 2024*. <https://en.aletihad.ae/news/business/4579524/abu-dhabi-hotel-sector-booms-with-5-8-million-guests-in-2024> [dostęp: 30.12.2025].
- Alrashdi, M. (2024, 26 lutego). *Dubai Tourism: Record visitors numbers in 2023*, Emirates NBD Research, <https://www.emiratesnbdresearch.com/en/articles/dubai-tourism-2023> [dostęp: 30.12.2025].
- Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions, and word-of-mouth. *International Journal of Contemporary Hospitality Management*, 24(7), 991–1010. <https://doi.org/10.1108/09596111211258883>
- CEIC Data. (2025). *United Arab Emirates AE: International tourism: Number of arrivals*. World Bank. <https://www.ceicdata.com/en/united-arab-emirates/tourism-statistics> [dostęp: 30.12.2025].
- Chan, E. S. W., & Lam, D. (2013). Hotel safety and security systems: Bridging the gap between managers and guests. *International Journal of Hospitality Management*, 32, 202–216. <https://doi.org/10.1016/j.ijhm.2012.05.010>
- Chodyński, A. (2021). *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*. Oficyna Wydawnicza KAAFM.
- Chodyński, A. (2024). Zarządzanie technologiami wodorowymi. Aspekty bezpieczeństwa ekologiczno-energetycznego. *Bezpieczeństwo. Teoria i Praktyka*, 4, 29–44. <https://doi.org/10.48269/2451-0718-btip-2024-4-002>
- Chodyński, A., Podwysocka, B., Wolak, G., & Kapera, I. (2024). Przeciwdziałanie sytuacjom kryzysowym – rozmowa i prezentacja poglądów na temat zarządzania bezpieczeństwem w hotelarstwie. *Bezpieczeństwo. Teoria i Praktyka*, 1, 13–20. <https://doi.org/10.48269/2451-0718-btip-2024-1-00W>

- Connecting Travel. (2024, May 22). *Ajman sees 9% upsurge in visitor numbers in Q1 2024*. <https://connectingtravel.com/news/ajman-sees-9-upsurge-in-visitor-numbers-in-q1-2024-ct> [dostęp: 30.12.2025].
- Dubai Department of Economy and Tourism. (2024). *DET annual visitor report 2024*. <https://www.dubaidet.gov.ae/en/research-and-insights/-/media/files/faqs/annual-visitor-report-2024/det-annual-visitor-report-2024.pdf> [dostęp: 30.12.2025].
- Dubai Department of Economy and Tourism. (2025, February 9). *Dubai welcomes 18.72 million international visitors in 2024 (+9% YoY)*. <https://dmo.dof.gov.ae/en/news-and-publications/latest-press-releases/dubai-welcomes-1872-million-international-visitors-in-2024-plus9-yoy/> [dostęp: 30.12.2025].
- Emirates NBD Research. (2024, February 26). *Dubai tourism sector hits new record in 2023*. <https://www.emiratesnbdresearch.com/en/articles/dubai-tourism-2023> [dostęp: 30.12.2025].
- Emirates NBD Research. (2025). *Dubai hotel market update*. <https://www.emiratesnbdresearch.com/-/media/research/emirates-nbd-dubai-hotel-market-update.pdf> [dostęp: 30.12.2025].
- Emirates Palace Mandarin Oriental, Abu Dhabi. (n.d.). *Google Maps reviews*. <https://www.google.com/maps/place/Emirates+Palace+Mandarin+Oriental> [dostęp: 30.12.2025].
- Emirates Palace Mandarin Oriental, Abu Dhabi. (n.d.). *Tripadvisor*. https://www.Tripadvisor.com/Hotel_Review-g294013-d507156-Reviews-Emirates_Palace_Mandarin_Oriental-Abu_Dhabi_Emirate_of_Abu_Dhabi.html [dostęp: 30.12.2025].
- Global Media Insight. (2025, June 4). *Dubai tourism statistics 2025*. <https://www.globalmediain-sight.com/blog/dubai-tourism-statistics/> [dostęp: 30.12.2025].
- Hammad, A. A. R. (2020). Tall buildings in Dubai – Converting architecture into reality. *Urban Studies and Public Administration*, 3(2), 99–116. <https://doi.org/10.22158/uspav3n2p99>
- Jumeirah Burj Al Arab. (n.d.). *Google Maps reviews*. <https://www.google.com/maps/place/Jumeirah+Burj+Al+Arab> [dostęp: 30.12.2025].
- Jumeirah Burj Al Arab. (n.d.). *Tripadvisor*. https://www.Tripadvisor.com/Hotel_Review-g295424-d302457-Reviews-Burj_Al_Arab_Jumeirah-Dubai.html [dostęp: 30.12.2025].
- Kapera, I., & Kapera, J. (2014). Bezpieczeństwo w hotelarstwie polskim. *Bezpieczeństwo. Teoria i Praktyka*, 3, 69–79. <https://repozytorium.uafm.edu.pl/server/api/core/bitstreams/09f145a9-e5a3-44fe-96db-944ce14c6de2/content> [dostęp: 30.12.2025].
- Mansfeld, Y., & Pizam, A. (Eds.). (2006). *Tourism, Security and Safety: From Theory to Practice*. Butterworth-Heinemann.
- Marine-Roig, E., & Huertas, A. (2020). How safety affects destination image projected through online travel reviews. *Journal of Destination Marketing & Management*, 18, article 100469, <https://doi.org/10.1016/j.jdmm.2020.100469>
- Ministry of Economy. (2022). *Tourism sector indicators in the UAE 2022*. Ministry of Economy – United Arab Emirates. <https://www.moet.gov.ae/en/-/tourism-sector-indicators-in-2022> [dostęp: 30.12.2025].
- Ministry of Economy. (2024). *UAE tourism sector witnesses steady growth with hotel establishment revenues increasing by 7 per cent to reach AED 24.6 billion in H1 2024*. Ministry of Economy – United Arab Emirates. <https://www.moet.gov.ae/en/-/ministry-of-economy-uae-tourism-sector-witnesses-steady-growth-with-hotel-establishment-revenues-increasing-by-7-per-cent-to-reach-aed-24.6-billion-in-h1-2024> [dostęp: 30.12.2025].
- Podwojska, B. (2024). Determinanty funkcjonowania systemu zarządzania kryzysowego w branży hotelarskiej. In D. Fatuła & A. Balamut (Eds.), *Spoleczne aspekty zarządzania organizacjami wobec zmienności otoczenia* (pp. 143–159). Oficyna Wydawnicza AFM. <https://doi.org/10.48269/978-83-67491-42-6-C>

- Seabra, C., Dolnicar, S., Abrantes, J. L., & Kastenholtz, E. (2013). Heterogeneity in risk and safety perceptions of international tourists. *Tourism Management*, 36, 502–510. <https://doi.org/10.1016/j.tourman.2012.09.008>
- Sharjah Commerce and Tourism Development Authority. (2025). *Sharjah Hospitality Statistics Report, Year 2024*. <https://www.sharjahtourism.ae/wp-content/uploads/2025/03/Statistics-Report-Yr-2024.pdf> [dostęp: 30.12.2025].
- Sparks, B. A., & Browning, V. (2011). The impact of online reviews on hotel booking intentions and perception of trust. *Tourism Management*, 32(6), 1310–1323. <https://doi.org/10.1016/j.tourman.2010.12.011>
- Tawfik, M. J., & Faris, J. M. (2023). Technical work and its design Image in the interior space: (as a case study of the Burj Al Arab hotel as a model). *Journal of Techniques*, 5(1), 260–266. <https://doi.org/10.51173/jt.v5i1.586>
- Yadav, N., Verma, S., & Chikhalkar, R. (2024). Online reviews towards reducing risk. *Journal of Tourism Futures*, 10(2), 299–316, <https://doi.org/10.1108/JTF-01-2022-0016>
- Yang, E. C. L., & Nair, V. (2014). Tourism at risk: A review of risk and perceived risk in tourism. *Asia-Pacific Journal of Innovation in Hospitality and Tourism*, 3(2), 239–259. <https://doi.org/10.7603/s40930-014-0013-z>

Postrzeganie bezpieczeństwa przez turystów przyjeżdżających do Zjednoczonych Emiratów Arabskich w kontekście usług hotelarskich segmentu premium

Streszczenie

Artykuł podejmuje problematykę obecności i znaczenia zagadnień bezpieczeństwa w doświadczeniach turystów korzystających z luksusowych obiektów hotelowych w Zjednoczonych Emiratach Arabskich. Postępowanie badawcze oparto na analizie materiałów źródłowych, obserwacji własnej przeprowadzonej podczas pobytu w badanej destynacji oraz wizyt w hotelach: Jumeirah Burj Al Arab i Emirates Palace Mandarin Oriental, Abu Dhabi. Istotnym uzupełnieniem badań była jakościowa analiza ponad 70 tys. opinii gości publikowanych na platformach Tripadvisor i Google Reviews, ze szczególnym uwzględnieniem odniesień do kwestii bezpieczeństwa. Uzyskane wyniki wskazują, że zagadnienia bezpieczeństwa rzadko są artykułowane wprost w narracjach gości hotelowych, co może świadczyć o postrzeganiu bezpieczeństwa jako immanentnego elementu oferty segmentu premium lub o wysokim poziomie zaufania do funkcjonujących rozwiązań. Jednocześnie bezpieczeństwo ujawnia się pośrednio poprzez opisy dotyczące kontroli dostępu, prywatności, czystości oraz zachowania personelu. Przeprowadzona analiza potwierdza, że opinie gości mogą stanowić istotne źródło wiedzy wspierające doskonalenie zarządzania bezpieczeństwem oraz wzmacnianie rezyliencji organizacyjnej w hotelarstwie segmentu premium.

Słowa kluczowe: zarządzanie, bezpieczeństwo, hotelarstwo, turystyka, Zjednoczone Emiraty Arabskie

Perception of safety by tourists visiting the United Arab Emirates in the context of premium hospitality services

Abstract

The article addresses the presence and significance of safety-related issues in the experiences of tourists using luxury hotel facilities in the United Arab Emirates. The research procedure was based on an analysis of source materials, the author's own observations conducted during stays in the studied destination, and visits to the hotels: Jumeirah Burj Al Arab in Dubai and Emirates Palace Mandarin Oriental, Abu Dhabi. An important complement to the research was a qualitative analysis of guest reviews (over 70, 000) published on online platforms Tripadvisor and Google Reviews, with particular attention paid to references related to safety.

The findings indicate that safety issues are rarely articulated explicitly in hotel guests' narratives, which may suggest that safety is perceived as an inherent component of the premium hospitality offering or reflects a high level of trust in existing protective measures. At the same time, safety emerges indirectly through narratives concerning access control, privacy, cleanliness, and staff behaviour. The analysis demonstrates that guest reviews can constitute a valuable source of knowledge supporting the improvement of safety management and the strengthening of organisational resilience in the premium hospitality sector.

Keywords: management, safety, hospitality, tourism, United Arab Emirates

Wkład autorów / Author Contributions

Konceptualizacja / Conceptualization: I.K.

Metodologia / Methodology: I.K.

Analiza formalna / Formal analysis: I.K.

Badania / Investigation: I.K.

Zasoby / Resources: I.K.

Przygotowanie wersji wstępnej / Writing – original draft: I.K.

Recenzja i edycja / Writing – review & editing: I.K.

Materiały dodatkowe / Supplementary Materials

Nie dotyczy / Not applicable.

Finansowanie / Funding

Badania nie otrzymały żadnego zewnętrznego finansowania. / This research received no external funding.

Oświadczenie o zatwierdzeniu etycznym / Ethics Approval Statement

Nie dotyczy / Not applicable.

Oświadczenie o świadomej zgodzie / Informed Consent Statement

Nie dotyczy / Not applicable.

Oświadczenie o dostępności danych / Data Availability Statement

Dane analizowane w niniejszym badaniu pochodziły z publicznie dostępnych opinii użytkowników Tripadvisor i Google Reviews. Przetworzone dane powstałe w toku badania są dostępne u autora na uzasadnioną prośbę. / The data analyzed in this study came from

publicly available user reviews on Tripadvisor and Google Reviews. The processed data generated during the study are available from the author upon request.

Declaration of Generative AI Use

No artificial intelligence tools were used in the preparation of this manuscript.

Podziękowania / Acknowledgments

Nie dotyczy / Not applicable.

Konflikt interesów / Conflict of Interest

Izabela Kapera dołączyła do zespołu redakcyjnego czasopisma „Bezpieczeństwo. Teoria i Praktyka” jako redaktorka sekcji tematycznej w lipcu 2026 roku. Proces redakcyjny i recenzje niniejszego artykułu zostały w pełni zakończone przed objęciem stanowiska. Artykuł został złożony 30 grudnia 2025 roku i przyjęty 9 marca 2026 roku. Autorka nie brała udziału w procesie redakcyjnym ani decyzyjnym dotyczącym niniejszego manuskryptu. / Izabela Kapera joined the editorial team of Security: Theory and Practice as a thematic section editor in July 2026. The editorial and peer review processes for this manuscript were fully completed prior to this appointment. The article was submitted on December 30, 2025, and accepted on March 9, 2026. The author had no role in the editorial handling or decision-making process of this manuscript.

Świadomość interesariuszy odnośnie do zagrożeń a przywództwo w modelach organizacji rezylientnej

Andrzej Chodyński

prof. dr hab., Wydział Zarządzania, Mediów i Technologii, Uniwersytet Andrzeja
Frycza Modrzewskiego w Krakowie (Faculty of Management, Media and Technology,
Andrzej Frycz Modrzewski Krakow University, Kraków, Poland)
<https://orcid.org/0000-0003-4962-5143>

Wprowadzenie

Współczesna organizacja funkcjonuje w świecie VUCA (Ziarko, 2024), co wymaga przyjęcia założeń organizacji rezylientnej. Wiąże się to z uwzględnieniem potencjalnych i rzeczywistych zagrożeń, które mogą wywołać kryzys w organizacji. Zagrożenia wojenne, pandemiczne, ataki terrorystyczne, awarie czy katastrofy naturalne mogą wywołać kryzys pozaekonomiczny (Chodyński, 2022: 17). W niniejszej publikacji katalog zagrożeń poszerzono o zagrożenia klimatyczne, związane m.in. ze skutkami globalnego ocieplenia i koniecznością odchodzenia od paliw kopalnych jako źródeł i nośników energii (Chodyński, 2025). Prezentowane są poglądy odnośnie do rezyliencji modeli biznesowych organizacji, wykorzystujące m.in. doświadczenia z pandemią COVID-19. Radic i in. (2022) zidentyfikowali 13 czynników wpływających na rezyliencję modelu biznesowego: zarządzanie kryzysowe, kulturę korporacyjną, nastawienie na klienta, digitalizację, współpracę zewnętrzną, finanse, zasoby ludzkie, innowacyjność, przywództwo, nastawienie na produkt, strategię, łańcuchy dostaw

i propozycję wartości dla klientów. Istotną rolę w zapobieganiu i przeciwdziałaniu tym kryzysom odgrywa przywództwo i zaangażowanie interesariuszy. Teorie przywództwa stanowią znaczący wkład w dorobek nauk o zarządzaniu i jakości. Przywództwo jest rozpatrywane w ramach koncepcji doskonałości organizacyjnej („Europejska nagroda jakości”, b.d.). Ewolucja podejścia do przywództwa wiąże się z przejściem od teorii cech, poprzez teorie sytuacyjne aż po podejście organiczne. Współcześnie w szczególności podnosi się znaczenie przywództwa jako oddziaływania (wpływu) na zachowania osób/grup, a także wywoływania pożądanego zachowania lub inspirowania innych na rzecz dobrowolnego angażowania się oraz wnoszenia wkładu w realizację celów organizacji; opisano typy przywództwa (Hilarowicz, 2017). Problematykę przywództwa podnoszono m.in. w monografiach A. Chodyńskiego: *Kreowanie odpowiedzialnego biznesu* (2016: 192–197) (przywództwo związane z umiejętnościami wyznaczania kierunków działania, komunikowania wizji i misji przedsiębiorstwa oraz motywowaniem pracowników; etyczne i nieetyczne przywództwo, uwarunkowania kulturowe, przywództwo transformacyjne, odpowiedzialne przywództwo, przywództwo transgresyjne i sensualne); *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo* (2021: 162–163) (odpowiedzialne przywództwo w modelach biznesu, oburęczne przywództwo w innowacjach oraz przywódca a menadżer). J. Kalejta (2022: 38–39) prezentuje teorie przywództwa: wielki człowiek, poprzez cechy, zachowanie, przypadkowość, sytuacyjne, autorytarny, ścieżka do celu, transakcyjny, transformacyjny, charyzmatyczny, służebny, leseferyczny, pełny zasięg przywództwa oraz adaptacyjny.

Przywództwo (w tym rola przywództwa w zarządzaniu interesariuszami) powinno być uwzględnione w budowie modeli organizacji rezyliентnych. Zachowania rezyliентne wymagają wsparcia ze strony wszystkich interesariuszy oraz budowy legitymizacji organizacji rezyliентnej (w tym z uwzględnieniem działań przywódczych) wobec tych interesariuszy (Chodyński, 2025).

Agata Austen (2010) zwraca uwagę na fakt relatywnie małego dorobku związanego z łączeniem przywództwa z teorią interesariuszy. W modelu przywództwa opartego na relacjach z interesariuszami autorstwa Marguerite Schneider (2002) uwzględniono z jednej strony charakterystykę przywódcy, a z drugiej – charakterystykę otoczenia zarówno zewnętrznego, jak i wewnętrznego organizacji. W modelu tym interesariusze dokonują oceny efektywności przywództwa w odniesieniu do spełnienia ich oczekiwań. Przywództwo i interesariusze odgrywają istotną rolę w kreowaniu kapitału ludzkiego w ramach kapitału społecznego organizacji (Nair i Radhakrishnan, 2019).

W rozważaniach o interesariuszach wskazuje się na fakt zróżnicowania ich oczekiwań wobec przedsiębiorstwa. Jednak wobec występujących lub możliwych zagrożeń, budując organizację rezyliентną, należy rozważyć konieczność skupienia oczekiwań interesariuszy na celu głównym, jakim jest przetrwanie lub/i dostosowanie

organizacji do otoczenia w kontekście tych zagrożeń. Warunkiem realizacji tego zadania jest uświadomienie sobie przez kierownictwo i interesariuszy możliwości wystąpienia tych zagrożeń oraz wykorzystanie działań synergicznych interesariuszy do przeciwdziałania tym zagrożeniom. Świadomość sytuacyjna jest w tym przypadku czynnikiem synergicznym w działaniach interesariuszy. Warto zwrócić uwagę, że jako czynniki synergiczne wskazywano zagrożenia klimatyczne, związane z emisją gazów cieplarnianych, a także fakt synergicznego oddziaływania Unii Europejskiej jako interesariusza poprzez wykorzystanie mechanizmów solidarnościowych (Chodyński, 2025). Zmiany klimatyczne wpływają na rozwój tematyki rezyliencji organizacyjnej (Chen i in., 2023).

W badaniach taksonomii modeli pomiaru odporności (rezyliencji) przedsiębiorstw w oparciu o dane z lat 2010–2023 zestawiono, porównano i oceniono 39 elementów. Wśród nich występuje świadomość sytuacyjna (w dwóch przypadkach) a także przywództwo (w jednym przypadku). W badaniach nie wyodrębniono aspektu interesariuszy (Bąk i Jedynak, 2025). Prowadzono badania sześciu wysoko odpornych (rezyliентnych) podmiotów gospodarczych: Southwest Airlines, Apple, Microsoft, Starbucks, Kyocera oraz Lego. Wyniki badań wskazują że rezyliencia organizacyjna obejmuje pięć wymiarów: kapitałowy, strategiczny, kulturowy, relacyjny (odnoszony do interesariuszy) oraz uczenia się (Chen i in., 2021). W modelu Harvard Business Review określono cechy organizacji rezyliентnej: bycie przygotowanym, elastyczność, oparcie się na współpracy (co można odnieść do interesariuszy), bycie godnym zaufania oraz bycie odpowiedzialnym (Deloitte, 2021).

Problematyka rezyliencji i roli przywództwa odnosi się także do firm małych i średnich, w tym wobec doświadczeń pandemii COVID-19. Rozpatrywany był wpływ następujących czynników na rezyliencję organizacyjną: przywództwo i zwinność w podejmowaniu decyzji, kultura organizacyjna i zarządzanie wiedzą, zasoby strategiczne i stabilność finansowa, technologia i przystosowanie cyfrowe, łańcuch dostaw a adaptacyjność do środowiska, kapitał ludzki i zwinność w zakresie siły roboczej (w aspekcie zaangażowania interesariuszy) (Kalubowila i in., 2025).

Cel pracy: wskazanie możliwości wykorzystania synergii interesariuszy opartej na świadomości (sytuacyjnej) zagrożeń w działaniach organizacji rezyliентnej i roli przywództwa w tworzeniu tej synergii.

Problem badawczy odnosi się do możliwości wykorzystania mechanizmów wspierających synergię między interesariuszami.

Pytanie badawcze: na ile świadomość sytuacyjna stanowiąca czynnik synergiczny wobec interesariuszy może być wykorzystana w działaniach przywódczych w sytuacji zagrożeń?

Metody badawcze: analiza działań wobec groźby kryzysu jako podstawa tworzenia mechanizmów na rzecz rezyliencji w oparciu o świadomość sytuacyjną interesariuszy i liderów z wykorzystaniem krytycznego przeglądu literatury.

Tak sformułowany cel pracy, problem badawczy i pytanie badawcze powinny służyć wypełnieniu luki badawczej wynikającej z niedostatecznego powiązania problematyki przywództwa i roli interesariuszy dla zapewnienia rezyliencji organizacyjnej, w sytuacji gdy każdy z tych elementów oddzielnie (przywództwo, interesariusze, rezyliencja) został już dosyć szeroko opracowany w literaturze przedmiotu.

Przywództwo a świadomość sytuacyjna w modelach rezyliencji

Występujące zagrożenia mogą prowadzić do sytuacji kryzysowych w organizacjach. W literaturze przedmiotu analizowano przywództwo w ramach zagrożenia, jakim była pandemia COVID-19, wobec zmian w organizacjach, w tym w przedsiębiorstwach. Wskazuje się rekomendacje działań z zakresu przywództwa z uwzględnieniem komunikacji w czasie kryzysu. Podkreśla się znaczenie budowy zaufania, dążenie do osiągnięcia stanu świadomości sytuacyjnej z uwzględnieniem oceny prawdopodobieństwa oraz potencjalnych konsekwencji i zagrożeń (Grzybowska, 2021). Zdaniem autora niniejszego artykułu przywództwo kryzysowe ma swoje odniesienie do przywództwa sytuacyjnego. W literaturze przedmiotu opisywane są style przywództwa w obszarze bezpieczeństwa (Ta i in., 2022).

Pojęcie przywództwa występuje w modelach rezyliencji organizacyjnej. W modelu S. McManus i współpracowników, w oparciu o badania z roku 2007 zaproponowano trzy elementy tego modelu: świadomość sytuacyjną, zarządzanie podatnością na zagrożenia oraz zdolność adaptacyjną (McManus i in., 2008). Rozwój tego modelu opierał się na wprowadzeniu elementu (czynnika) kultury rezyliencji (*resilience ethos*) (Lee i in., 2013), uwzględniającego w ramach zdolności adaptacyjnej przywództwo i zarządzanie, akcentującego znaczenie podejmowania decyzji oraz ciągłej oceny strategii i programów. McManus przywództwo rozpatruje w kontekście zarządzania organizacją, mając na uwadze podejmowanie decyzji, komunikowanie awaryjne, a także dostępność menadżerów oraz transparentność i odpowiedzialność (McManus, 2007).

W późniejszym w stosunku do propozycji S. McManus modelu A. Stephenson (2010) zawarto także obszar przywództwa. Propozycje ujęcia roli interesariuszy w tym modelu wraz ze wskazaniem ich roli w odniesieniu do przywództwa zawarto w artykule A. Chodyńskiego (2025). W modelu A. Stephenson przywództwo odnoszone jest do podejmowania decyzji w czasie kryzysu, bez prowadzenia rozbudowanych konsultacji z pracownikami i przy ich akceptacji dla takiego sposobu postępowania. Podkreśla się znaczenie roli działania strategicznego wyższego kierownictwa. W ramach rozważań o przywództwie kierownicy wyższego szczebla są postrzegani jako profesjonaliści, od których można się uczyć. C. Gibson i M. Tarrant (2010) podkreślają, że problematyka przywództwa, obok wartości organizacyjnych, jest podnoszona w ramach modeli atrybutowych rezyliencji, związanych z dynamicznymi cechami organizacji. Wartości i przywództwo odnoszą się do kultury organizacji. W literaturze

przedmiotu rozpatruje się powiązania kultury rezyliencji z przywództwem (Knapp, 2016). Podobny pogląd prezentują A.Y.P. Santos i R.G. Spers (2023), którzy do obszaru „przywództwo i kultura” zaliczają zakresy: przywództwo, zaangażowanie personelu, podejmowanie decyzji oraz innowacyjność i kreatywność. Analizowana jest rola przywództwa organizacji rezydentnej w ramach działań w cyklu PDCA (Planuj/Plan – Wykonaj/Do – Sprawdź/Check – Działaj/Act), wykorzystujących uczenie się, antycypowanie przyszłości, interpretację i reagowanie wobec stanu aktualnego oraz monitorowanie i przegląd minionych wydarzeń wraz z określaniem zmian. Rezyliencja organizacji odnosi się do optymalizacji wyników, kontroli zapobiegawczej, świadomego działania, a także adaptacyjnych innowacji (Denyer, 2017: 5, 10, 20, 24).

Warto podkreślić, że zarówno w modelu S. McManus, jak i A. Stephenson występuje pojęcie świadomości sytuacyjnej, odnoszonej do wiedzy o środowisku, w którym funkcjonuje organizacja (w tym – wiedzy o zagrożeniach). W pierwszym modelu świadomość sytuacyjna odnosi się m.in. do zrozumienia zagrożeń, obowiązków i odpowiedzialności, monitorowania i raportowania, świadomości powiązań, ale i ubezpieczeń, priorytetów odbudowy, a także podejmowania decyzji. W drugim modelu podkreślane jest zdobywanie wiedzy o otoczeniu i rola przepływu informacji. W późniejszych badaniach potwierdzono istotną korelację między postawą proaktywną, świadomością sytuacyjną a potencjałem odporności organizacyjnej (Ewertowski i in., 2025).

M.R. Endsley (2015) wskazuje na trzy poziomy świadomości sytuacyjnej: od percepcji związanej z identyfikacją elementów otoczenia (1), poprzez zrozumienie w oparciu o percepcję w odniesieniu do informacji, z uwzględnieniem celów organizacji (2), do projekcji stanu przyszłego (3). Interakcja między poziomami ma charakter dynamiczny w układzie góra–dół oraz dół–góra (Endsley, 2000).

Działania w ramach przywództwa służące zwiększeniu świadomości sytuacyjnej pracowników odnoszą się do percepcji w środowisku wewnętrznym, a dalej obejmują identyfikację i rozwiązywanie problemów oraz pojmowanie związane ze zrozumieniem zagrożeń zewnętrznych. Obejmuje ono percepcję rzeczywistości przy akceptacji sytuacji oraz zaufanie – odnoszone do zapewnienia poczucia bezpieczeństwa. Ważną rolę odgrywa transparentność związana z zaangażowaniem pracowników. Podnoszenie świadomości w ramach percepcji w środowisku wewnętrznym obejmuje: 1. empatię, odnoszoną do odczuwania przez innych oraz ich sytuacji, 2. wsłuchiwanie się, a następnie zrozumienie doświadczeń innych, oraz 3. rozpoznanie potrzeb. Podano praktyki dotyczące zwiększenia świadomości (m.in. wywiady z pracownikami, spotkania informacyjne, dyskusje w grupach, anonimowe ankiety). W zakresie pojmowania określono procesy zapewniające odbiór przez pracowników odpowiednich i właściwych informacji (w tym m.in. odnoszone do planowania zasobów, koordynację interakcji, zachęcanie do generowania pytań, a także oceny wpływu i oceny konsekwencji) (Ramašauskienė i in., 2025).

Świadomość sytuacyjną można rozważać wobec złożoności koncepcyjnego modelu rezyliencji organizacyjnej, uwarunkowanej dynamiką zmian w otoczeniu, w szczególności w obszarze technologii i innowacji (Manzini i in., 2025).

Przywództwo i świadomość sytuacyjna są wymieniane wśród 13 elementów rezyliencji organizacyjnej i opisywane wraz ze studiami przypadków, w tym w odniesieniu do bezpieczeństwa infrastruktury krytycznej (Australian Government, 2024).

Rozważa się wpływ przywództwa przedsiębiorczego (odnoszonego do kognitywnego *ambidexterity*, kreowania wartości społeczno-ekonomicznych oraz samoświadomości) na rezyliencję organizacyjną, a także późniejsze koncepcje, wiążące przywództwo z nastawieniem na interesariuszy na zewnątrz i wewnątrz organizacji (Koswate i in., 2025).

W odniesieniu do prezentowanych poglądów należy podkreślić znaczenie roli przywództwa w kształtowaniu świadomości sytuacyjnej interesariuszy, zarówno wewnętrznych, jak i zewnętrznych.

Wykorzystanie synergii interesariuszy i mechanizmów rezyliencji

Propozycję wykorzystania synergii interesariuszy w ramach modelu dojrzałości zarządzania interesariuszami zawarto w publikacji Chodyńskiego i in. (2024). Proponuje się traktować interesariuszy jako zasób przedsiębiorstwa. Wskazuje się, że czynnikiem synergicznym dla interesariuszy są zagrożenia klimatyczne, zaś Unia Europejska jest wskazywana jako aktywny interesariusz, wspierający oddziaływania synergiczne, wpływający głównie na rozwiązania legislacyjne (Chodyński, 2025). Warto jednak zwrócić uwagę na rolę przywództwa w budowaniu i wykorzystaniu synergii i przywołać poglądy odnośnie do synergii w procesie zarządzania strategicznego zasobami niematerialnymi w przedsiębiorstwie (Murawska, 2008). Aktywność interesariuszy jest związana zarówno z oddziaływaniem czynników interpersonalnych, jak i czynników zewnętrznych, przy czym na proces ten ma wpływ jakość przywództwa oraz zdolności interesariuszy. Należy brać pod uwagę powiązania sieciowe interesariuszy, ich sposób myślenia, jakość oraz dostępność informacji, uwarunkowania oraz realizację priorytetów (Waligo i in., 2014).

W szczególności w aspekcie sieciowych powiązań między interesariuszami oraz w układzie firma–interesariusze istotną rolę odgrywa zakorzenienie oraz bliskość (Chodyński, 2021: 216–222). Bliskość może być atrybutem interesariusza (Driscoll i Starik, 2004). Może ona przyjmować postać bliskości geograficznej, poznawczej, społecznej czy instytucjonalnej (Boschma, 2005). Prezentowany jest podział mówiący o bliskości geograficznej (odnosi się nie tylko do przestrzeni geograficznej, ale też wymiaru społecznego), przemysłowej (z występującym podobieństwem i/lub komplementarnością technologiczną), kulturowej (odnoszonej do podobieństwa wartości, postaw i norm), organizacyjnej (dotyczącej podobieństwa zasad

koordynacji działań) oraz instytucjonalnej. W ramach tej ostatniej obserwuje się podobieństwo tych samych reguł postępowania przez uczestników wspólnoty. Mowa jest także o bliskości relacyjnej – na podstawie liczby, częstotliwości i jakości występujących relacji (Klimas, 2011). Zdaniem autora niniejszej publikacji bliskość może być czynnikiem synergicznym, skłaniającym interesariuszy do formułowania wspólnych celów na rzecz rezyliencji, w szczególności wobec zagrożeń o charakterze lokalnym. Rolą lidera jest tworzenie mechanizmów wykorzystujących bliskość dla zarządzania interesariuszami.

Należy podkreślić rolę przywództwa w kształtowaniu mechanizmów rezyliencji (odporności) organizacji. A. Karman (2019: 139) wymienia cztery mechanizmy odporności: władzy (w tym określanie ról w czasie kryzysu, tworzenie zespołów kryzysowych, a także tworzenie planów awaryjnych), komunikowania się (w tym budowanie świadomości odnośnie do podatności organizacyjnej), koordynowania (obejmuje dysponowanie zasobami i samoorganizację) oraz uczenia się (m.in. przez obserwację, tworzenie scenariuszy, ćwiczenia na wypadek awarii, z dokumentacji, z analizy przeszłych zdarzeń, a także otoczenia).

Mechanizm rezyliencji w kontekście roli przywództwa powinien odnosić się do koordynacji działań, w tym w zarządzaniu wiedzą i organizacyjnym uczeniem się, a także do mechanizmów dostosowawczych, odnoszonych do tworzenia nowych warunków równowagi w aspekcie zachowań rezyliencyjnych. Z kolei mechanizm innowacyjny, oparty na brikolażu, może być wykorzystany jako brikolaz kryzysowy, w tym dla zwiększenia rezyliencji organizacyjnej. Mechanizmy te, z podkreśleniem synergii działań interesariuszy, wykorzystano w modelu odpowiedzialnych zachowań innowacyjnych organizacji wobec turbulencji otoczenia, wraz z opisem modeli cząstkowych i wskazaniem roli interesariuszy (Chodyński, 2021: 169–173, 182–186, 208–211).

Przywództwo w odniesieniu do interesariuszy powinno wykorzystywać świadomość interesariuszy w kwestii zagrożeń, a szczególne znaczenie ma możliwość budowy synergii pomiędzy interesariuszami o najwyższej świadomości. Przydatne może być narzędzie stanowiące propozycję autora niniejszej publikacji – pozwalające na identyfikację grup interesariuszy o określonych poziomach świadomości zagrożeń wraz ze wskazaniem mechanizmów budowy synergii. Analiza (tabela 1) może obejmować: 1. typ interesariusza – ocenę przez interesariusza stopnia zagrożenia powodowanego przyczynami wewnętrznymi i zewnętrznymi według typów kryzysów (np. w skali 1–5), oraz 2. wydzielenie interesariuszy o najwyższej świadomości (o najwyższej sumie punktów) jako grupy, dla której wysoka świadomość określonych zagrożeń stanowi czynnik synergiczny. Liderzy powinni proponować mechanizmy zarządzania na rzecz synergii. Zdaniem autora niniejszej publikacji wykorzystać można działania liderów w budowie przywództwa w oparciu o wzajemne zaufanie. Uwzględniają one m.in. wykorzystanie wiedzy, zarządzanie ryzykiem, podejmowanie decyzji na czas, przyzwolenie na błędy, przejrzystość w komunikowaniu decyzji, pracę zespołową,

tworzenie warunków dla rozwoju kompetencji pracowniczych, a także budowę kultury organizacyjnej wykorzystującej uczenie się. W zakresie komunikacji podkreśla się m.in. znaczenie jej natężenia, a także tworzenie nowego stylu komunikacji (Grzybowska, 2021). Rekomendacje dla działań praktycznych zawarto w podsumowaniu dla każdej kolumny w tabeli.

Tabela 1. Świadomość zagrożeń przez interesariuszy (ocena) i propozycja mechanizmów budowy synergii interesariuszy

Rodzaj (typ interesariusza) i ich udział w ocenie świadomości zagrożeń	Typ zagrożeń w ramach kryzysów pozaekonomicznych, ich ocena przez interesariuszy i kierownictwo	Ocena postrzegania poszczególnych zagrożeń przez interesariuszy	Uwagi/ proponowane mechanizmy dla budowy synergii
Interesariusze wewnętrzni: pracownicy, zarząd, inwestorzy; przywództwo w praktyce często jest kojarzone z działaniami zarządu (najwyższego kierownictwa)	Katastrofy naturalne; pandemie; cyberataki, akty terroru; niepokoje społeczne; wojny; nowe regulacje prawne; fałszywe informacje; działania naruszające reputację; o podłożu społecznym (np. strajki); o podłożu kryminalnym (np. kradzieże, akty wandalizmu); o podłożu technologicznym (np. wielkie awarie, katastrofy przemysłowe), a ponadto: brak źródeł i dostaw nośników „czystej energii” (wskazane ograniczenie emisji gazów cieplarnianych pochodzących ze spalania paliw kopalnych, powodujących zagrożenia klimatyczne), kryzys wywołany aspektami prawnymi lub kosztami uniemożliwiającymi funkcjonowanie organizacji (Chodyński, 2022: 17; 2024: 29–44). Niektóre zjawiska, jak np. pożary lasów zagrażające funkcjonowaniu podmiotów gospodarczych (np. hoteli w ośrodkach turystycznych), mogą być wywołane zarówno przez akty terroru (piroterroryzm) (Kaczmarowski, 2017), jak i przez ocieplenie klimatu, powodujące wzrost ryzyka wystąpienia pożarów ekstremalnych (Wernicki, 2024).	Ocena punktowa, skala od 1 do 5 Oceny: 1 – minimalne zagrożenie, 2 – małe zagrożenie, 3 – średnie zagrożenie, 4 – duże zagrożenie, 5 – bardzo duże zagrożenie	Budowa zaufania, wykorzystanie wiedzy, przejrzystość komunikacji, w tym dla budowa świadomości sytuacji, podejmowanie decyzji na czas, brykół kryzysowy, bliskość interesariuszy, ewakuacja z wykorzystaniem środków technicznych
Interesariusze zewnętrzni: klienci, konkurenci, społeczność lokalna, organizacje non profit, media, inni	Jak wyżej	Jak wyżej	Jak wyżej
Podsumowanie: ocena świadomości zagrożeń przez poszczególnych interesariuszy	Podsumowanie: ocena punktowa poszczególnych zagrożeń przez kolejnych interesariuszy; porównanie tych wyników do wyników dla liderów (najwyższego kierownictwa)	Podsumowanie: suma punktów dla poszczególnych zagrożeń w odniesieniu do poszczególnych interesariuszy	Podsumowanie: wskazanie mechanizmów synergii dla interesariuszy o najwyższej sumie punktów

Źródło: opracowanie własne z wykorzystaniem podanej literatury.

Propozycje autora niniejszej publikacji zawarte w tabeli można rozpatrywać w odniesieniu do prezentowanych w publikacji M.R. Endsley (2015) poglądów dotyczących świadomości sytuacyjnej. W szczególności należy podkreślić znaczenie budowy zaufania, wykorzystania wiedzy i przejrzystości komunikacji, które wspierają percepcję elementów otoczenia. Z kolei oparte na percepcji zrozumienie dotyczące informacji pozwala na podejmowanie decyzji na czas i wykorzystanie brikolażu kryzysowego. Czynnikiem wspierającym realizację kolejnych etapów budowy świadomości sytuacyjnej jest wykorzystanie synergii interesariuszy i jej mechanizmów (proponowanych w tabeli 1). Synergia między interesariuszami sprzyja także projekcji stanu przyszłego, z podkreśleniem roli przywódców organizacji w jej kształtowaniu.

Zakończenie

Aleksandra Spik (2025), wykorzystując przede wszystkim opracowanie M. Reevesa i K. Whitakera (2022), zaproponowała elementy organizacji o wysokiej rezyliencji, mianowicie:

1. Funkcjonalna redundancja związana z duplikowaniem elementów systemu,
2. różnicowanie reakcji na kryzys w oparciu o zróżnicowane zasoby organizacji,
3. modułowość związana z zapewnieniem funkcjonowania systemu nawet w przypadku zaburzenia funkcjonowania jednego z jego elementów,
4. adaptacyjność, obejmująca próby i możliwość popełniania błędów, dla budowy organizacji elastycznej i uczącej się,
5. przezorność, związana z wprowadzaniem środków ograniczania ryzyka zdarzeń niekorzystnych,
6. osadzenie (ang. *embeddedness*) oparte głównie na dopasowaniu organizacji do celów i wymogów społecznych, w tym w odniesieniu do szerszego ekosystemu biznesowego.

Jednak warunkiem budowy organizacji o wysokiej rezyliencji jest wysoka świadomość sytuacyjna zarówno liderów, jak i interesariuszy. Punktem wyjścia jest ocena stanu tej świadomości. Dla interesariuszy o określonym poziomie świadomości możliwe są działania synergiczne, inicjowane przez liderów.

Zarówno dla podnoszenia świadomości, jak i realizacji działań synergicznych w sytuacji realnych zagrożeń możliwe jest wykorzystanie określonych mechanizmów. W odniesieniu do organizacji o wysokiej rezyliencji zaproponowano mechanizm wykorzystujący zaufanie, a w odniesieniu do dysponowania zasobami w sytuacji krańcowej turbulencji otoczenia – mechanizm brikolażu. Wskazano na mechanizm uczenia się (wykorzystanie wiedzy). Osadzenie, w powiązaniu z odpowiednim mechanizmem na rzecz synergii interesariuszy, jest odnoszone do pojęcia bliskości. Mechanizmy te można wykorzystać w praktycznej realizacji założeń modeli rezyliencji organizacyjnej.

Bibliografia

- Austen, A. (2010). Efektywność przywództwa w organizacji publicznej. *Organizacja i Zarządzanie*, 4, 25–42.
- Australian Government. (2024). *Organisational Resilience: Good Practice Guide*. <https://www.cisc.gov.au/resources-subsite/Documents/org-res-good-practice-guide.pdf> [dostęp: 5.09.2025].
- Bąk, S., Jedynak, P. (2025). Enterprise resilience assessment – an overview of models. *Organization and Management*, 1, 7–21.
- Boschma, R. (2005). Proximity and innovation: A critical assessment. *Regional Studies*, 39(1), 61–74.
- Chen, C., Li, J., Zhao, Y., Goerlandt F., Reniers, G., Yiliu, L. (2023). Resilience assessment and management: A review on contributions on process safety and environmental protection. *Process Safety and Environmental Protection*, 170, 1039–1051. <https://doi.org/10.1016/j.psep.2022.12.072>
- Chen, R., Xie, Y., Liu, Y. (2021). Defining, conceptualizing, and measuring organizational resilience: A multiple case study. *Sustainability*, 13(5), artykuł 2517. <https://doi.org/10.3390/su13052517>
- Chodyński, A. (2016). *Kreowanie odpowiedzialnego biznesu*. Oficyna Wydawnicza AFM.
- Chodyński, A. (2021). *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*. Oficyna Wydawnicza KAAFM.
- Chodyński, A. (2022). Kryzys pozaekonomiczny przedsiębiorstwa – ekologiczny aspekt rezylencji organizacyjnej. [W:] A. Chodyński, D. Fatuła, M. Leśniewski (red.). *Zrównoważony rozwój, systemy informacyjne i zarządzanie bezpieczeństwem w perspektywie długoterminowej przedsiębiorstw* (s. 11–31). Oficyna Wydawnicza AFM.
- Chodyński, A. (2024). *Zarządzanie technologiami wodorowymi. Aspekty bezpieczeństwa ekologiczno-energetycznego*. *Bezpieczeństwo. Teoria i Praktyka*, 4, 29–44, <https://doi.org/10.48269/2451-0718-btip-2024-4-002>
- Chodyński, A. (2025). Interesariusze w modelu rezylencji organizacyjnej wobec zagrożeń ekologiczno-energetycznych. *Bezpieczeństwo. Teoria i Praktyka*, 1, 23–38, <https://doi.org/10.48269/2451-0718-btip-2025-1-001>
- Chodyński, A., Huszлак, W., Rosa, K. (2024). Audyt zarządzania interesariuszami organizacji wobec zagrożeń ekologiczno-energetycznych. *Bezpieczeństwo. Teoria i Praktyka*, 4, 89–104, <https://doi.org/10.48269/2451-0718-btip-2024-4-006>
- Deloitte. (2021, 12 marca). *5 Traits of Resilient Organizations*. Harvard Business Review. <https://hbr.org/sponsored/2021/03/5-traits-of-resilient-organizations> [dostęp: 26.10.2025].
- Denyer, D. (2017). *Organizational resilience: A summary of academic evidence, business insights and new thinking*. BSI and Cranfield University. <https://cranfieldsombrochures.cld.bz/Organisational-Report/2> [dostęp: 11.08.2025].
- Driscoll, C., Starik, M. (2004). *The primordial stakeholder: Advancing the conceptual consideration of stakeholder status for the natural environment*. *Journal of Business Ethics*, 49(1), 55–73.
- Endsley, M.R. (2000). Theoretical underpinnings of situation awareness: a critical review. [W:] M.R. Endsley, D.J. Garland (red.). *Situation awareness analysis and measurement*. Lawrence Erlbaum Associates. https://www.researchgate.net/publication/292771806_Situation_awareness_analysis_and_measurement_chapter_theoretical_underpinnings_of_situation_awareness [dostęp: 11.08.2025].

- Endsley, M.R. (2015). Situation awareness misconceptions and misunderstandings. *Journal of Cognitive Engineering and Decision Making*, 9(1), 4–32. <https://doi.org/10.1177/1555343415572631>
- Europejska nagroda jakości. (b.d.). [W:] *Encyklopedia Zarządzania*. https://mfiles.pl/pl/index.php/Europejska_nagrada_jako%C5%9Bci [dostęp: 11.08.2025].
- Ewertowski, T., Sadłowska-Wrzesińska, J., Racek, E., Woźna, D. (2025). Optimizing organizational resilience potential based on predefined attributes: A case study of the Polish foundry industry during the COVID-19 pandemic. *Organizacja i Kierowanie*, 197, 39–58.
- Gibson, C., Tarrant, M. (2010). A 'conceptual models' approach to organisational resilience. *The Australian Journal of Emergency Management*, 25(2), 8–14.
- Grzybowska W. (2021), Rola przywództwa w procesie zarządzania zmianą. *Academy of Management*, 5(2), s. 70–86.
- Hilarowicz, A. (2017). Inteligentne specjalizacje – problematyka przywództwa. *Zeszyty Naukowe Politechniki Śląskiej, Seria: Organizacja i Zarządzanie*, 105, 85–96.
- Kaczmarowski, J. (2017). Lasy – zasoby podatne na zagrożenia terrorystyczne. [W:] P. Guzowski (red.). *Dochodzenia pożarowe – nauka i technika* (t. 1, s. 37–58). Polskie Towarzystwo Ekspertów Dochodzeń Pożarowych.
- Kalejta, J. (2022). *Style przewodzenia a skuteczność realizacji celów turystycznych organizacji pozarządowych* [Rozprawa doktorska, Politechnika Białostocka. Wydział Inżynierii Zarządzania].
- Kalubowila, P. S., Nuwan A. N., Bandara, H. G. K. N., Heenkenda, S., Damayanthi, B.W.R., Bulankulama S. W. G. K. (2025). Unpacking organizational resilience in SMEs in Sri Lanka. *International Journal of Research and Innovation in Social Science*, 9(8), 2726–2742. <https://dx.doi.org/10.47772/IJRIS.2025.908000223>
- Karman, A. (2019). *Odporność organizacji na ekstrema pogodowe*. Wydawnictwo UMCS.
- Klimas, P. (2011). Wymiary bliskości w sieciach innowacji. *Przegląd Organizacji*, 4, 16–20.
- Knapp, H.P. (2016). Designing and implementing an interdependent resilience culture. *Journal of Business Continuity & Emergency Planning*, 10(1), 76–83.
- Koswatte, I., Joseph, S., Yatawara, T., Iyampillai, K., Kaushalya Vidanalage A. (2025). Entrepreneurial resilience through leadership transformation: Evidence from Sri Lanka. [W:] C. Harrison (red.). *Leadership and leadership development* (s. 109–132), Routledge. <https://doi.org/10.4324/9781032624976-7>
- Lee A.V., Vargo J., Seville E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural Hazards Review*, 14(1), 29–41.
- Manzini D., Oosthuizen R., Chikwanda H. (2025). Enhancing organisational resilience through systems thinking. *Social Sciences & Humanities Open*, 12, artykuł 101783. <https://doi.org/10.1016/j.ssaho.2025.101783>
- McManus, S. (2007). *Organisational resilience in New Zealand* [Doctoral thesis, University of Canterbury]. <https://ir.canterbury.ac.nz/items/11a41130-acdc-4eb2-9ebb-57d1a0cd4b04> [dostęp: 11.08.2025].
- McManus, S., Seville, E., Vargo, J., Brundson D. (2008). Facilitated process for improving organizational resilience. *Natural Hazards Review*, 9(2), 81–90.
- Murawska, M. (2008). *Zarządzanie strategiczne niematerialnymi zasobami przedsiębiorstwa*. Fundacja Promocji i Akredytacji Kierunków Ekonomicznych. https://www.fundacja.edu.pl/pliki/monika_murawska_zarzadzanie_strategiczne.pdf [dostęp: 7.09.2025].
- Nair K. S., Radhakrishnan, L. (2019). Role of leadership and stakeholder engagement in creating human capital. *International Journal of Scientific & Technology Research*, 8(12), 3855–3899.

- Radic, M., Herrmann, P., Haberland, P., & Riese, C.R. (2022). Development of a business model resilience framework for managers and strategic decision-makers. *Schmalenbach Journal of Business Research*, 74(4), 575–601. <https://doi.org/10.1007/s41471-022-00135-x>
- Ramašauskienė, V., Župerkienė, E., Šimanskienė, L. (2025). Situational awareness in leadership: Application of methods in business organisations. *Administrative Sciences*, 15(6), artykuł 210. <https://doi.org/10.3390/admsci15060210>
- Reeves, M., Whitaker, K. (2022). A guide to building a more resilient business. *Harvard Business Review Special Issues*, Summer 2022, 60–64, <https://www.zinio.com/article/harvard-business-review-special-issues/summer-2022-i547481/1-a-guide-to-building-a-more-resilient-business-a18> [dostęp: 11.08.2025].
- Santos A.Y.P., Spers R.G. (2023). How to measure organizational resilience? Validating a simplified model. *RAM. Revista de Administração Mackenzie*, 24(6), 1–32. <https://doi.org/10.1590/1678-6971/eRAMD230007.en>
- Schneider, M. (2002). A stakeholder model of organizational leadership. *Organization Science*, 13(2), 209–220.
- Spik, A. (2025). Rezyliencja: panaceum, moda czy oszustwo? Znaczenie i zastosowanie pojęcia w zarządzaniu organizacjami. *Studia i Materiały (Wydział Zarządzania. Uniwersytet Warszawski)*, 1, 75–90. <https://doi.org/10.7172/1733-9758.2025.42.7>
- Stephenson, A. (2010). *Benchmarking the resilience of organisations* [Doctoral thesis, University of Canterbury]. https://ir.canterbury.ac.nz/bitstream/handle/10092/5303/THESIS_BENCHMARKINGTHERESILIENCEOFORGANISATIONS.pdf?sequence=1&isAllowed=y [dostęp: 27.11.2025].
- Ta, M. T. D., Kim, T., Gausdal A. H. (2022). Leadership styles and safety performance in high-risk industries: A systematic review. *Safety and Reliability*, 41(1), 10–44. <https://doi.org/10.1080/09617353.2022.2035627>
- Waligo, V.M., Clarke, J., Hawkins, R. (2014). The Leadership–stakeholder involvement capacity’ nexus in stakeholder management. *Journal of Business Research*, 67(7), 1342–1352.
- Wernicki, P. (2024, 17 sierpnia). *Zmiany klimatyczne zwiększyły prawdopodobieństwo pożarów lasów*. Nauka w Polsce. <https://naukawpolsce.pl/aktualnosci/news%2C104066%2Czmiany-klimatyczne-zwiczyszy-prawdopodobienstwo-pozarow-lasow.html> [dostęp: 7.09.2025].
- Ziarko, J. (2024). Uwarunkowania zarządzania problemami bezpieczeństwa w świecie VUCA. *Bezpieczeństwo. Teoria i Praktyka*, 1, 23–41. <https://doi.org/10.48269/2451-0718-btip-2024-1-001>

Świadomość interesariuszy odnośnie do zagrożeń a przywództwo w modelach organizacji rezyliencyjnej

Streszczenie

Opisano znaczenie świadomości sytuacyjnej interesariuszy na rzecz rezyliencji organizacyjnej. Wskazano rolę przywództwa w kształtowaniu tej świadomości. Określono miejsce świadomości i przywództwa w modelach rezyliencji przedsiębiorstw. Zaproponowano wykorzystanie synergii interesariuszy i określonych mechanizmów na rzecz budowy rezyliencji organizacyjnej. Wskazano na czynniki synergiczne dla interesariuszy, w tym zagrożenia klimatyczne oraz bliskość interesariuszy. Zaproponowano narzędzie pozwalające na identyfikację grup interesariuszy o określonych poziomach świadomości zagrożeń wraz ze wskazaniem mechanizmów budowy synergii. Pozwala ono na wykorzystanie w ramach przywództwa synergii pomiędzy interesariuszami o najwyższej świadomości dla budowy rezyliencji organizacyjnej.

Słowa kluczowe: świadomość sytuacyjna interesariuszy wobec zagrożeń, przywództwo, mechanizmy wspierające synergię między interesariuszami, modele rezyliencji organizacyjnej

Stakeholder awareness of threats and leadership in resilient organization models

Abstract

The importance of stakeholder situational awareness for organizational resilience is described. The role of leadership in shaping this awareness is highlighted. The place of awareness and leadership in business resilience models is defined. The use of stakeholder synergies and specific mechanisms to build organizational resilience is proposed. Synergistic factors for stakeholders are identified, including climate threats and stakeholder proximity. A tool was proposed to identify stakeholder groups with specific levels of threats awareness, along with mechanisms for building synergy. It allows leadership to leverage synergy between stakeholders with the highest awareness to build organizational resilience.

Keywords: stakeholders' situational awareness of threats, leadership, mechanisms supporting synergy between stakeholders, models of organizational resilience

Wkład autorów / Author Contributions

Konceptualizacja / Conceptualization: A.Ch.

Metodologia / Methodology: A.Ch.

Analiza formalna / Formal analysis: A.Ch.

Badania / Investigation: A.Ch.

Zasoby / Resources: A.Ch.

Przygotowanie wersji wstępnej / Writing – original draft: A.Ch.

Recenzja i edycja / Writing – review & editing: A.Ch.

Materiały dodatkowe / Supplementary Materials

Nie dotyczy / Not applicable.

Finansowanie / Funding

Badania nie otrzymały żadnego zewnętrznego finansowania. / This research received no external funding.

Oświadczenie o zatwierdzeniu etycznym / Ethics Approval Statement

Nie dotyczy / Not applicable.

Oświadczenie o świadomej zgodzie / Informed Consent Statement

Nie dotyczy / Not applicable.

Oświadczenie o dostępności danych / Data Availability Statement

Udostępnianie danych nie ma zastosowania do tego artykułu, ponieważ w ramach badania nie wygenerowano ani nie analizowano żadnych nowych danych. / Data sharing is not applicable to this article as no new data were generated or analyzed in this study.

**Deklaracja dotycząca wykorzystania generatywnej sztucznej inteligencji /
Declaration of Generative AI Use**

Autorzy oświadczają, że podczas przygotowywania niniejszego manuskryptu nie korzystali z generatywnej sztucznej inteligencji ani technologii wspomaganych przez sztuczną inteligencję. / The authors declare that no generative artificial intelligence or AI-assisted technologies were used in the preparation of this manuscript.

Podziękowania / Acknowledgments

Nie dotyczy / Not applicable.

Konflikt interesów / Conflict of Interest

Andrzej Chodyński pełni funkcję redaktora naczelnego czasopisma „Bezpieczeństwo. Teoria i Praktyka”. Zgodnie z polityką redakcyjną czasopisma i wytycznymi COPE dotyczącymi możliwego konfliktu interesów, Andrzej Chodyński po nadesłaniu zgłoszenia nie uczestniczył w kolejnych etapach prac. Tekst został skierowany do publikacji na podstawie anonimowych opinii dwóch niezależnych recenzentów, spoza jednostki reprezentowanej przez autora (double-blind review). Proces recenzji nadzorował i korespondencję z recenzentami prowadził niezależny członek Redakcji. / Andrzej Chodyński serves as Editor-in-Chief of the journal *Bezpieczeństwo. Teoria i Praktyka* / *Security: Theory and Practice*. In accordance with the journal's editorial policy and COPE guidelines regarding potential conflicts of interest, Andrzej Chodyński did not participate in subsequent stages of the work after submitting the submission. The manuscript was accepted for publication based on the anonymous opinions of two independent reviewers from outside the author's institution (double-blind review process). The review process was overseen, and all correspondence with the reviewers was conducted, by an independent member of the Editorial Office.

Leveraging the intellectual capital of a resilient organization in crisis threat situations (case studies)

Andrzej Chodyński

Prof., PhD, DSc, Eng., Faculty of Management, Media and Technology,
Andrzej Frycz Modrzewski Krakow University, Kraków, Poland
<https://orcid.org/0000-0003-4962-5143>

Vladyslava Kornilova

MA, Faculty of Management, Media and Technology,
Andrzej Frycz Modrzewski Krakow University, Kraków, Poland
<https://orcid.org/0009-0005-8676-6342>

Introduction

The development of an organization (including the economic entity) can be disrupted by a crisis situation. The reaction of an economic entity to an emerging threat may depend on its intellectual capital. In the literature on the subject, much attention is paid to the place of intellectual capital in organizational management. Intellectual capital was included in the proposal for the company development management process (Chodyński, 2005). The possibilities of using different models of intellectual capital for knowledge management in an organization are considered (Chodyński, 2004, 2007). Intellectual capital influences business security architecture (Chodyński, 2024). It is indicated that the elements of intellectual capital (human, relational and organizational capital) support the company's capacity to be resilient and maintain its

results in situations of threats (disasters) (Ahmed i in., 2020; Agostini i Nosella 2023). The impact of intellectual capital on, among others, the functioning of banks (Elenwo i Tolofari, 2024) and its use in the IT sector are considered (Tunio, 2024). The role of intellectual capital in supporting supply chain resilience is discussed (Pettit i in., 2019; Mubarik i in., 2022). For logistics companies, the impact of individual elements of intellectual capital (human, structural, relational) on their resilience capabilities was determined. These capabilities were related to the relationship between intellectual capital, human resource management (HR) practices, and the use of artificial intelligence. The relationship between the quality of logistics services, logistics companies' resilience, and their performance was addressed (Abdalati i Yamin, 2025).

In this article, the division of intellectual capital into: human capital and structural capital (Walecka, 2016) as well as the division into: human capital, structural (organizational) capital and relational capital related to contacts with the environment was adopted for consideration (Sokołowski, 2018) (Sokołowski treats structural and organizational capital as identical, assuming that it refers to management structures, processes, organizational knowledge, innovation and internal relations in the organization).

The aim of this study is to determine the impact of an organization's intellectual capital on its resilient behaviors. A resilient organization is capable of anticipating threats and, when they do occur, adopting behaviors that enable survival in crisis conditions and further organizational development. Particular attention is paid to the potential of intellectual capital in relation to A. Stephenson's model of organizational resilience. Stephenson's model contains 13 elements: minimizing tunnel thinking ("Minimisation of Silo Mentality"), internal resources ("Capability & Capacity of Internal Resources"), employee engagement ("Staff Engagement & Involvement"), knowledge utilization ("Information & Knowledge"), leadership ("Leadership, Management & Governance Structures"), innovation and creativity ("Innovation & Creativity"), efficient decision-making ("Devolved & Responsive Decision Making"), situation awareness ("Internal & External Situation Monitoring & Reporting"), strategy planning ("Planning Strategies"), emergency plans and exercises ("Participation in Exercises"), proactive attitude ("Proactive Posture"), effective partnership ("Capability & Capacity of External Resources") and awareness of goals and priorities ("Recovery Priorities") (Stephenson, 2010; Chodyński, 2025; Rzegocki, 2021, p. 73). The importance of innovative behavior was emphasized.

The research question is: to what extent does Stephenson's organizational resilience model incorporate elements of intellectual capital, particularly in terms of innovative behavior? To what extent are these behaviors influenced by organizational stakeholders?

Research methods: a critical literature review and analysis of case studies of companies affected by threats. In the literature, a case study is presented as a detailed

description, usually of a real economic phenomenon, e.g., an organization, a management process, its components, or its environment, in order to draw conclusions about its causes and outcomes. In the literature, we can distinguish three purposes of case studies: theory-generating, theory-testing, and practical (Grzegorzczuk, 2015). A case study can be considered from a narrow or broad perspective. The narrow approach focuses on why specific decisions or groups of decisions were made, how they were implemented, and what their consequences are. The broad approach encompasses the logic of designing and selecting strategies as a response to a specific research problem when the number of variables exceeds the capacity to collect specific data. It is used to develop new theories. The term “case study” refers to both the research process and the research outcome. Types of case studies include autotelic, instrumental, and collective case studies. An autotelic study examines a specific case that is not treated as representative of a broader phenomenon. An instrumental case study serves to deepen understanding of a broader phenomenon or allows for the drawing of more general conclusions. A collective case study is an instrumental study that encompasses several similar or diverse cases (Chodyński, 2016, pp. 247–259).

This article presents three case studies stemming from threats of different nature: a pandemic, war, and a natural disaster.

Intellectual capital and organizational resilience in the A. Stephenson model

The literature on the subject points to the link between intellectual capital and organizational resilience. The special role of human capital in building organizational resilience is emphasized (Kwiecień, 2023; Shela i in., 2021). In A. Walecka's (2016) considerations regarding the elements of intellectual capital, human capital includes knowledge, experience of employees, their education, refers to the sources of creativity and innovation, as well as the improvement and acquisition of new skills. In this approach, it is considered in Stephenson's model primarily in the areas of employee engagement, innovation, and creativity. Internal structural capital (organizational capital), relating to processes, procedures, databases, and communication and information infrastructure, is primarily related to the area of efficient decision-making in Stephenson's model. In turn, external structural capital (relational capital), relating to relationships with the environment, can refer to building networks with external partners and is primarily associated with the area of effective partnership in Stephenson's model, emphasizing the key role of stakeholders.

The analysis of intellectual capital and the components of the presented model of organizational resilience led to the conclusion that the analyzed model of resilience by Stephenson includes elements that are directly related to individual areas of intellectual capital.

The role of innovation

The literature on the subject highlights the importance of relational capital (both internal and external) as an element of intellectual capital in crisis management. It is emphasized that a company's relational capital determines its resilience to crisis. Walecka (2019) treats a crisis situation as a set of circumstances that led to a crisis as a turning point in the course of events, although she emphasizes that there are also views that a crisis precedes a crisis situation. In turn, the Crisis Management Act defines a crisis as a situation that negatively impacts the safety of people, property, or the environment, which is associated with a significant limitation in the actions of the relevant authorities due to the inadequacy of available resources. The concept of a crisis is not defined in the Act (Crisis Management Act, 2007). With relational capital in mind, it's worth emphasizing the potential for leveraging scientific research to expand the existing description of network dimensions (flexibility or dynamics, cohesion, coordination, scale of operations) to include the exchange of knowledge as a resource (including collaboration between inter-organizational teams in times of threats). This also applies to considering the time factor, considering changes in partners' intellectual capital over time, as well as the construction of *ad hoc* networks (Chodyński, 2021, p. 216, Table 9). Referring to Stephenson's model, the extended approach to network dimensioning can be linked primarily to the areas of "effective partnership" and "proactive attitude".

The components of intellectual capital are the source of innovation, and knowledge is the foundation for creating intellectual capital. In terms of structural capital, knowledge is formalized, relating to management structures and methods (organizational documentation), descriptions of processes and technologies, and organizational culture (records regarding, among other things, the company's vision and mission) (Sokołowski, 2018). In A. Stephenson's model, two independent areas were distinguished: "innovation and creativity" and the area of "use of knowledge".

The literature on the subject draws attention to the role of intellectual capital in an enterprise in the context of its innovation and innovation absorption, as well as entrepreneurship (Różycka, 2021). The role of innovation management mechanisms in companies and organizational networks, using intellectual capital, is emphasized (Chodyński, 2021, pp. 175–176, Table 5). The impact of individual components of intellectual capital on the innovative capacity of enterprises is presented (Danielak, 2024). At the same time, the impact of intellectual capital and organizational resilience on innovation potential and the creation of competitive advantage is emphasized (Iqbal i in., 2025). The impact of intellectual capital and organizational resilience on individual sectors is presented, including in relation to the issue of innovation, including for business activities in tourism (Alnasser i in., 2024).

Leveraging intellectual capital in situations where organizational security is threatened, including through entrepreneurial and innovative activities, is particularly important, as described in A. Chodyński's monograph (2021). These proposals were presented within the framework of partial models of the model of responsible innovative behavior in the face of environmental turbulence. Among other things, the importance of entrepreneurial bricolage within *ad hoc* innovation is emphasized (Chodyński, 2021, pp. 208–215, esp. Figure 1, Table 8), which on the one hand can be associated with human capital within the framework of intellectual capital, and on the other hand – can be related to the area of “efficient decision-making” within the framework of A. Stephenson's model.

The presented analysis indicates that innovative behaviors are related, on the one hand, to the intellectual capital possessed, and, on the other hand, they significantly influence organizational resilience, in particular in the face of extreme environmental turbulence.

Case studies of the behavior of resilient companies

Case studies were presented relating to the response of economic entities to COVID-19, disruption of supply chains due to the war in Ukraine and natural disasters.

The case studies were selected based on well-described examples in the literature relating to these three threat groups. Therefore, the previously discussed approach of an autotelic, case-specific study was utilized.

Case study I. The COVID-19 pandemic and technological company CISCO

From the very beginning of the pandemic, CISCO was recognized as a key provider of critical infrastructure services. Priority was given to orders from emergency services and essential services, and the rapidly evolving needs of healthcare facilities were supported. The COVID-19 lockdown resulted in a threefold increase in the number of people using the market-leading Webex videoconferencing platform within a month.

Rules applied:

1) Employees are the company: With the right technology, a distributed workforce can be more resilient, effective, and diverse. Even before the pandemic, CISCO already had significant experience implementing this so-called hybrid work model. Employees spent an average of about two days a week at home.

2) Resilience through leadership, empathy, and emotional intelligence.

Flexibility and trust are key factors in resilience. Empathetic management of remote workers is gaining importance. Online remote management tools allow employees to maintain close contact with their managers. Videoconferencing technology is important for maintaining organizational culture in a distributed workforce.

Company management has increased the frequency of video calls with employees, ensuring each employee feels recognized and cared for.

3) Resilience through smarter security

Employee education plays a crucial role in threat prevention. CISCO offered its employees cybersecurity training and periodically sent them fraudulent (phishing) emails (CISCO, 2021).

Stakeholder support included:

1) Customers

A series of free offers and trials for Webex and security technologies, along with \$2.5 billion in funding, were launched to help businesses maintain operations. The Business Resiliency Program, offered by Cisco Capital, included a 90-day payment freeze and allowed customers to defer 95% of the cost of a new product or solution until 2021. Healthcare customers were provided with essential technology for remote connectivity and telemedicine; customized solutions were developed to support the rapid deployment of intensive care units, temporary clinics, and COVID-19 testing sites. Medical device integration and remote access to medical data were enabled. Customers managing factories, distribution warehouses, and other facilities requiring on-site personnel were provided with solutions that helped ensure employee safety and privacy while maintaining productivity.

2) Suppliers

In collaboration with suppliers, a new order prioritization process was developed, enabling the fulfilment of over 2,500 critical customer requests for emergency infrastructure.

3) Employees

Although many CISCO employees were already prepared to work remotely, capacity was expanded sevenfold to support 140,000 remote workers and contractors in just 10 days. This required increasing VPN capacity, providing employees with essential equipment, and expanding global IT support. During regular virtual meetings, the leadership team, along with medical and mental health experts and special guests, shared the latest business news, medical advice, perspectives, and inspiration. Employees also received several additional paid days off to spend time with family or to rest and recharge.

4) Communities, Governments, Businesses, International Organizations

Non-profit organizations serving vulnerable populations have seen a decline in volunteers and financial support, and have also experienced challenges in adhering to social distancing guidelines. CISCO has stepped up to help organizations around the world, donating \$53 million in cash and personal protective equipment to various organizations.

As part of CISCO's contribution to COVID-19 relief efforts, \$7 million went to the United Nations Foundation's COVID-19 Solidarity Response Fund, supporting the World Health Organization's (WHO) global efforts to prevent, detect, and manage the spread of the virus. The Country Digital Acceleration (CDA) program provided funding to countries, government agencies, and businesses to rapidly implement COVID-19 technology solutions. Webex collaboration technology also enabled institutions like the G20 and the U.S. Congress to transition to secure virtual meetings. Teleconferencing equipment at CISCO offices was donated to local hospitals. Stanford Children's Health, one of the hospitals that received the system as a donation, was able to increase the number of virtual visits per day from 30 to 700. CISCO donated 5.3 million KN95 masks and over 750,000 surgical masks and face shields, some of which were 3D printed by CISCO volunteers around the world (Boynton, 2021).

The company has developed processes to coordinate responses to pandemics like COVID-19, including Global Business Resilience (GBR) and Supply Chain Incident Management (SCIM) (Garrett, 2020).

Case Study II. The war in Ukraine and car manufacturers VW and BMW

The Russian invasion of Ukraine has significantly increased risk and uncertainty in the global economy, particularly in Eastern Europe. Consequences for automakers include sourcing from Russia and Ukraine and the ability to produce or sell vehicles in these countries. Sanctions imposed by the EU, the United States, and/or other countries on Russia, as well as sanctions on Russian banks, companies, and individuals, have impacted the operations of automotive companies (BMW Group, 2023).

Two German car manufacturers, BMW and Volkswagen, have stated that Russia's invasion of Ukraine has caused shortages of key components, forcing them to curtail vehicle production in Europe. The war is negatively impacting supply chains in the automotive industry. In BMW's case, the problems stem, among other things, from the fact that its main suppliers of electrical wiring harnesses are located in western Ukraine. Volkswagen has supported its Ukrainian suppliers of wiring harnesses. The company sources them from as many as 11 plants in Ukraine, nine of which are operating at reduced capacity. To address the problem, the carmakers are seeking suppliers outside Ukraine. Furthermore, some European car production is being relocated to other regions, including China and South America. BMW and Volkswagen halted car production in Russia and exports to the country following the outbreak of the war ("BMW, VW warn", 2022). Russia is the eighth largest automotive market in the world.

Volkswagen Group donates €1m (£833,690) to the UNO-Flüchtlingshilfe charity in response to the Russian invasion of Ukraine ("Car industry reacts", 2022).

Case Study III. Natural disaster and theme park Walt Disney World Resort in Florida

A comprehensive business continuity strategy for an organization includes, among other things, developing a business continuity plan following a natural disaster (e.g., floods, storms, or fires).

It describes in detail procedures ranging from securing facilities and creating data backups to activating alternative work locations and managing communications in the event of infrastructure failure.

Preparing for hurricanes at Walt Disney World Resort focuses on ensuring operational readiness. Developed protocols allow for the closure of the entire resort, securing resources, and communicating with thousands of employees and guests in less than 12 hours. The plan includes pre-established supply chains, the creation of local *ad hoc* teams, and detailed action lists. The importance of extensive training is emphasized.

Disney World has faced several hurricanes over the past few years, including Hurricane Milton in 2024. During these storms, Disney closed its theme parks and other attractions, requiring guests to stay put. During Hurricane Milton, Disney provided guests with discounts on rooms, meals, and hurricane kits, as well as children’s entertainment. While Disney ensures all guests on property are cared for during the storm, there are hotels that are better suited for staying put.

Disney’s official policy is as follows: “If the National Hurricane Center issues a hurricane warning for the Orlando area – or your area of residence – you may change or cancel Walt Disney Travel Company Disney Resort hotel packages and most room-only reservations (made directly with Disney) within 7 days of your planned arrival date at no additional charge. Most room-only packages and vacation packages can be modified or canceled online, including changes to travel dates” (Delpozo, 2025).

Possibilities of practical use of intellectual capital elements in reference to A. Stephenson’s model

The table 1 below presents the relationship between the elements of intellectual capital and the individual elements of Stephenson’s model, resulting from a critical review of the literature, in the light of the analysis of three different case studies, facing various threats.

The first stage identified the characteristics of individual elements of intellectual capital in relation to specific areas of Stephenson’s organizational resilience model. The second stage, using specific company examples, identified anti-crisis solutions that utilized these characteristics, depending on the threats faced.

Table 1. Linking the elements of intellectual capital with the individual elements of A. Stephenson’s model based on case studies

Elements of intellectual capital/areas of the A. Stephenson model	Characteristics	Companies	Anti-crisis solutions
Human capital/ the area of employee engagement, innovation and creativity, and the area of “knowledge utilization”	Innovation, creativity, knowledge, employee engagement, organizational culture	CISCO	Leveraging previous hybrid work model experiences to build human capital. A new type of leadership. Educating employees on cybersecurity.
		BMW, VW	Efforts to maintain continuity of supplies from Ukrainian companies, taking into account the commitment and creativity of employees.
		Walt Disney World Resort	The role of training in emergency situations.
Structural internal (organizational) capital/ referring mainly to the area of efficient decision-making	Procedures and processes within the organization, organizational communication, decision-making	CISCO	New forms of collaboration with employees. Coordination of activities supported by innovative technical solutions.
		BMW, VW	Decisions to suspend production in Russia.
		Walt Disney World Resort	Business continuity plan and procedures.
Structural external (relational) capital / is primarily associated with the area of effective partnership, emphasizing the key role of stakeholders. Aspects of network dimensioning can be linked primarily to the areas of “effective partnership” and “proactive attitude”	Relations with the environment, external partners, stakeholders, network building, including ad hoc	CISCO	New forms of cooperation and support for external stakeholders.
		BMW, VW	Relocating production to other countries. Support for non-profit organizations.
		Walt Disney World Resort	Ensuring guest safety in the event of an emergency. Flexible hotel cancellation policy.

Source: authors’ own work

Conclusions

Case studies confirm the use of general principles related to ensuring organizational resilience:

- 1) Creating remote work opportunities using innovative solutions, both technical and work organization (based on the experience of the COVID-19 pandemic).

- 2) Ensuring diversification of operations and supplies in the case of manufacturing companies (example: the war in Ukraine).
- 3) In the event of natural disaster threats, it is important to develop a business continuity plan that includes:
 - establishing detailed evacuation protocols: create and regularly practice clear, site-specific evacuation plans.
 - implementing off-site data replication: critical business data should not only be backed up but also actively replicated to a secure, dedicated location. This requires moving beyond cloud storage and includes disaster recovery solutions.
 - preparing emergency kits; these include first aid kits, water, long-life food, flashlights, and communication devices such as satellite phones or two-way radios that are not dependent on local cellular networks. A flexible approach to pricing and payment for customers is emphasized in the event of a natural disaster that threatens not only business operations but also human life and health.

In summary, the following can be stated:

For three different cases, the use of individual elements of intellectual capital by economic entities in resilient behavior was analyzed in situations of completely different threats;

In the area of human capital, the effectiveness of actions was based on employee experience, commitment, and training. Structural organizational capital leveraged coordination of activities, decision-making, and ensuring business continuity. Structural relational capital was leveraged through collaboration with stakeholders, international decision-making, and ongoing security actions.

Given diverse threats, depending on the type of economic entity and its situation, the use of intellectual capital elements in support of resilient behavior encompasses various anti-crisis solutions.

The article demonstrates that both the theoretical foundations of resilient companies with specific intellectual capital, as well as practical experience and the general principles of ensuring organizational resilience, can be applied to specific areas of Stephenson's model. The research questions were answered, and the work's objective was achieved.

References

- Abdalati, O.A.A., Yamin, M.A.Y. (2025). Does intellectual capital boost firm resilience capability? Conceptualizing logistic service quality as a moderating factor between resilience capability and firm performance. *Sustainability*, 17(17), Article 7948. <https://doi.org/10.3390/su17177948>.

- Agostini, L., Nosella, A. (2023). Intellectual capital and resilience: Evidence from two cases of SMEs. *Knowledge Management Research and Practice*, 21(5), 929–942. <https://doi.org/10.1080/14778238.2022.2103047>.
- Ahmed, S. S., Guozhu, J., Mubarik, S., Khan, M., Khan, E. (2020). Intellectual capital and business performance: The role of dimensions of absorptive capacity. *Journal of Intellectual Capital*, 21(1), 23–39. <https://doi.org/10.1108/JIC-11-2018-0199>.
- Alnasser, E. M., Alkhazaim, S. M., Alshiha, A. A., Al-Romeedy, B. S. (2024). Intellectual capital and organizational resilience in tourism and hotel businesses: Do organizational agility and innovation matter? *Current Issues in Tourism*, 28(16), 2649–2669. <https://doi.org/10.1080/13683500.2024.2378970>.
- BMW Group. (2023, May 10), *EUR 50,000,000,000 Euro medium term note programme*. BMW Group, https://www.bmwgroup.com/content/dam/grpw/websites/bmwgroup_com/ir/downloads/en/2023/emtn/01.00-Prospectus.pdf [accessed: 17.11.2025].
- BMW, VW warn of shortages from part suppliers in Ukraine. (2022, March 16). *The Independent*. <https://www.independent.co.uk/news/ap-volkswagen-bmw-russia-europe-b2037352.html> [accessed: 17.11.2025].
- Boynton, J. (2021, March 22). Connecting in a time of crisis: Cisco's response to COVID-19. *CISCO Blogs*. <https://blogs.cisco.com/csr/connecting-in-a-time-of-crisis-ciscos-response-to-covid-19> [accessed: 17.11.2025].
- Car industry reacts to Russian invasion of Ukraine (2022, March 4). *Motors.md*. <https://motors.md/en/news/car-industry-reacts-to-russian-invasion-of-ukraine-20220304.html> [accessed: 12.11.2025].
- Chodyński, A. (2004). Dynamika organizacji opartej o wiedzę. *Zeszyty Naukowe Wyższej Szkoły Zarządzania i Marketingu w Sosnowcu. Seria Zarządzanie i Marketing*, 1, 25–29.
- Chodyński, A. (2005). Ocena szans rozwojowych firm na globalnym rynku a zarządzanie wiedzą. *Zeszyty Naukowe Wyższej Szkoły Zarządzania i Marketingu w Sosnowcu. Seria Zarządzanie i Marketing*, 2, 23–28.
- Chodyński, A. (2007). *Wiedza i kompetencje ekologiczne w strategiach rozwoju przedsiębiorstw*, Difin, Warszawa.
- Chodyński, A. (2016). *Kreowanie odpowiedzialnego biznesu*. Oficyna Wydawnicza AFM.
- Chodyński, A. (2021). *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach: Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*. Oficyna Wydawnicza KAAFM.
- Chodyński, A. (2024). Wpływ koncepcji zarządzania na architekturę bezpieczeństwa biznesu – programy zapobiegania awariom przemysłowym. *Bezpieczeństwo. Teoria i Praktyka*, 1, 77–91.
- Chodyński, A. (2025). Interesariusze w modelu rezyliencji organizacyjnej wobec zagrożeń ekologiczno-energetycznych. *Bezpieczeństwo. Teoria i Praktyka*, 1, 23–38. <https://doi.org/10.48269/2451-0718-btip-2025-1-001>.
- CISCO (2021). *Building Resilience in the New Paradigm*. <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/building-resilience-paradigm-wp.pdf> [accessed: 17.11.2025].
- Crisis Management Act of April 26, 2007 [Ustawa o zarządzaniu kryzysowym], Dz. U. 2023, item 122 (Poland).
- Danielak, W. (2024). Wpływ kapitału intelektualnego na zdolności innowacyjne małych przedsiębiorstw. *Zeszyty Naukowe Akademii Górnośląskiej*, 4, 16–25. <https://doi.org/10.53259/2024.04.02>.
- Delpozo, B. (2025, June 15). The best hurricane-ready hotels in Disney World. *The Disney Food Blog*. <https://www.disneyfoodblog.com/2025/06/14/the-best-hurricane-ready-hotels-in-disney-world-2/> [accessed: 17.11.2025].

- Elenwo, A. M., Tolofari, D. T. (2024). Intellectual capital development and organizational resilience of commercial banks in Nigeria, *International Journal of Economics and Business Management*, 10(3), 108–124. <https://doi.org/10.56201/ijebm.v10.no3.2024.pg108.124>.
- Garrett, M. (2020, April 9). *Companies Like CISCO have a pandemic response plan – do you?* TGG. <https://tgg-accounting.com/companies-like-cisco-have-a-pandemic-response-plan-do-you/> [accessed: 17.11.2025].
- Grzegorzczak, W. (2015). Studium przypadku jako metoda badawcza i dydaktyczna w naukach o zarządzaniu. In W. Grzegorzczak (Ed.), *Wybrane problemy zarządzania i finansów. Studia przypadków* (pp. 9–16). Wydawnictwo Uniwersytetu Łódzkiego.
- Iqbal, Y., Ur Rehman, S., Akram, I., Abdulmuhsin, A.A., Afzal, M.A. (2025). Uncovering the relationship between intellectual capital, organizational resilience, innovation capacity, risk-taking tolerance and competitive advantage in manufacturing context. *Business Process Management Journal*. Advance online publication. <https://doi.org/10.1108/BPMJ-03-2025-0264>.
- Kwiecień, A. (2023). The importance of human capital for organizational resilience. *Scientific Papers of Silesian University of Technology, Organization and Management Series*, 177, 363–375. <http://dx.doi.org/10.29119/1641-3466.2023.177.21>
- Mubarik, M. S., Bontis, N., Mubarik, M., Mahmood, T. (2022). Intellectual capital and supply chain resilience. *Journal of Intellectual Capital*, 23(3), 713–738 <https://doi.org/10.1108/JIC-06-2020-0206>.
- Pettit, T. J., Croxton, K. L., Fiksel, J. (2019). The evolution of resilience in supply chain management: A retrospective on ensuring supply chain resilience. *Journal of Business Logistics*, 40(1), 56–65. <https://doi.org/10.1111/jbl.12202>.
- Różycka, A. (2021). *Rola kapitału intelektualnego w absorpcji innowacji w przedsiębiorstwie*, Archae-Graph Wydawnictwo Naukowe.
- Rzegocki, M.M. (2021). *Prężność organizacyjna jako kluczowy zasób dla odporności organizacji na kryzys. Czym jest i jak mierzyć prężność organizacyjną?* Oficyna Wydawnicza ASPRA.
- Shela, V., Ramayah, T., & Ahmad, N. H. (2023). Human capital and organisational resilience in the context of manufacturing: A systematic literature review. *Journal of Intellectual Capital*, 24(2), 535–559. <https://doi.org/10.1108/JIC-09-2021-0234>
- Sokołowski, J. (2018). Kapitał intelektualny a innowacyjność przedsiębiorstwa. *Zarządzanie Innowacyjne w Gospodarce i Biznesie*, 2, 21–32. https://doi.org/10.25312/2391-5129.27/2018_02js.
- Stephenson, A. (2010). *Benchmarking the resilience of organisations* [A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in the Civil and Natural Resources Engineering Department at the University of Canterbury]. <http://dx.doi.org/10.26021/2859>.
- Top 8 business continuity plan examples for UK firms 2025* (2025, August 8). SES Computers. <https://www.sescomputers.com/news/business-continuity-plan-examples> [accessed: 2.11.2025].
- Tunio, S. (2024). *Intellectual capital and organizational resilience: The role of dynamic capability – evidence from Karachi IT sector*. IBA SBS International Conference. <https://ir.iba.edu.pk/sbsic/2024/program/56> [accessed: 18.11.2025].
- Walecka, A. (2016). Kapitał relacyjny przedsiębiorstw w kryzysie. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, 422, 158–170.
- Walecka, A. (2019). Kapitał relacyjny a odporność przedsiębiorstwa na zjawiska kryzysowe. Wydawnictwo Politechniki Łódzkiej, Łódź.

Leveraging the intellectual capital of a resilient organization in crisis threat situations (case studies)

Abstract

The impact of an organization's intellectual capital on resilient behavior was determined. The links between intellectual capital elements and specific areas of A. Stephenson's organizational resilience model were discussed. It was emphasized that a resilient organization is not only capable of anticipating potential threats but, should they occur, of implementing behaviors that enable survival in crisis conditions. It should also enable the organization's further development. Based on the analysis of case studies of three companies from different sectors, exposed to various types of threats (COVID-19, war, hurricanes), practical possibilities for utilizing individual elements of intellectual capital were identified: human, organizational, and relational. The importance of innovative activities was emphasized. The particular importance of the Stephenson model's areas was demonstrated, such as employee engagement, innovation and creativity, knowledge utilization, efficient decision-making, proactive attitude, and effective partnership, with the key role of stakeholders emphasized.

Key words: organizational resilience, intellectual capital, innovative behavior, crisis management, A. Stephenson's resilience model, case studies

Author Contributions

Conceptualization: A.Ch.

Methodology: A.Ch, V.K.

Formal analysis: A.Ch, V.K.

Investigation: A.Ch, V.K.

Resources: A.Ch.,V.K.

Writing – original draft: A.Ch, V.K

Writing – review & editing: A.Ch, V.K.

Supplementary Materials

Not applicable.

Funding

This research received no external funding.

Ethics Approval Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Data sharing is not applicable to this article as no new data were generated or analyzed in this study.

Declaration of Generative AI Use

No artificial intelligence tools were used in the preparation of this manuscript.

Acknowledgments

Not applicable.

Conflict of Interest

Andrzej Chodyński serves as Editor-in-Chief of the journal *Bezpieczeństwo. Teoria i Praktyka* / Security: Theory and Practice. In accordance with the journal's editorial policy and COPE guidelines regarding potential conflicts of interest, Andrzej Chodyński did not participate in subsequent stages of the work after submitting the submission. The manuscript was accepted for publication based on the anonymous opinions of two independent reviewers from outside the author's institution (double-blind review process). The review process was overseen, and all correspondence with the reviewers was conducted, by an independent member of the Editorial Office.

Vladyslava Kornilova declares no conflict of interest.

Managing organisational resilience in the onshore wind energy sector in Poland

Anna Bałamut

PhD, Faculty of Computer Science, AGH University of Krakow

<https://orcid.org/0000-0001-7300-7367>

Michał Przygoda

PhD, Faculty of Social and Applied Sciences, Academy of Applied Sciences of the Common Knowledge Society in Szczecin

<https://orcid.org/0000-0002-2627-2886>

Introduction

Onshore wind energy is one of the key pillars of Poland's energy transition process today. In the light of the EU's climate and energy targets, such as reducing greenhouse gas emissions by 55% by 2030 ("Fit for 55" package) and increasing the share of renewable energy sources (RES) to at least 42.5% in the energy mix, Poland has committed to the dynamic development of the RES sector. According to the updated *Energy Policy of Poland until 2040* (Ministry of Climate and Environment, 2021), the installed capacity of onshore wind farms is expected to be approx. 14 GW by 2030 and reach up to 20 GW in 2040. This is a significant leap compared to the approximately 9.6 GW at the end of 2023, confirming that the development of this RES segment is among the fastest advancing. As of 2024, wind power was already the largest renewable energy source in the Polish electricity system, accounting for approximately 14.7% of total installed capacity (Ministry of Climate and Environment, 2021).

The increase in power also translates into an increasing share of electricity production from wind. In 2022, onshore wind farms produced almost 19 TWh of energy, accounting for 10.8% of national generation. In 2023, this figure rises to 22.12 TWh, or 14.6% of total production. Importantly, the combined share of wind and solar energy exceeded 20% of total national production for the first time, and the share of all renewable energy sources in the energy mix reached 27%. These figures indicate that Poland is getting closer to meeting the EU's climate targets and, according to the *National Energy and Climate Plan* (Ministry of Climate and Environment, 2025), the share of RES could reach up to 50% by 2030. However, such growth requires not only investment in new sources but also ensuring their stable functioning.

Despite the dynamic growth of the sector, wind farm operations are exposed to numerous risks that can disrupt their operational continuity. Although wind turbines are high-tech installations, they are prone to failure – including damage to gearboxes, rotor blades or control systems. The operation of wind farms is also affected by weather conditions: icing of the blades leads to downtime and loss of production, and lightning and fires can cause serious damage to the infrastructure. Grid constraints are also becoming an increasingly serious problem – the transmission and distribution infrastructure, which is not adapted to the scale of RES development, forces temporary restrictions on wind farm generation, especially during peak production periods. Transmission system operators are increasingly forced to issue orders to reduce turbine operation to avoid overloading the grid, resulting in operational losses and a lack of utilisation of available generation potential.

In the onshore wind sector, this relationship emerges particularly clearly in situations of grid constraints. Even high technical resistance of turbines does not eliminate operational losses if the farm operator's organisation does not have procedures for quick response to generation reduction commands, communication mechanisms with the system operator and flexible production management models. In such cases, it is not a technical failure but rather insufficient organisational resilience that determines the scale of the disruption.

All these factors show that the further development of wind energy cannot be based solely on the expansion of generation capacity. It is essential to strengthen simultaneously the functional resilience of wind farms, i.e. their ability to respond to unforeseen situations and maintain operational stability. The traditional approach has mainly focused on technical aspects – improving turbine design, developing condition monitoring systems or improving network balancing methods. Meanwhile, today's approach to operational security requires a much broader perspective – encompassing not only technology, but also how organisations manage disruption and adapt to changing conditions.

In this context, there is more and more talk about the need to implement the concept of organisational resilience, understood as the ability of an organisation to

prepare for disruptions, respond effectively to crisis situations and quickly regain operational capacity after their occurrence. A resilient organisation is not only one that has reliable technologies, but also one that can anticipate risks, learn from mistakes and adapt structures and procedures in a flexible way.

For the onshore wind sector, this means the need to seek out and implement organisational solutions that support business continuity – such as risk management systems, Business Continuity Planning, rapid response structures or an organisational culture that promotes learning and resilience. Managing organisational resilience thus becomes a key element in ensuring not only operational security, but also the long-term sustainability of the sector.

This article undertakes an analysis of this very issue – asking how organisations operating in the Polish onshore wind energy sector manage organisational resilience in the face of increasing technical, environmental and systemic challenges. The article proposes a look beyond technical snapshots, focusing on the managerial and organisational mechanisms that can underpin the building of operational resilience of wind farms. The aim is to identify practices that enable you not only to survive disruptive incidents, but also to recover quickly to full capacity and to learn in order to reduce the impact of similar incidents in the future. This approach puts forward a hypothesis that resilience management is not an addition to the functioning of the organisation, but one of the conditions for its durability and responsibility towards the power system and society.

It should be noted that the conducted analysis has certain limitations. The study does not include empirical research, and the conclusions are based on the desk research method, involving a systematic review of the literature and the analysis of secondary data. The literature review covered scientific publications (articles and monographs) indexed in selected academic databases, as well as reports from public institutions and industry organisations. The analysis of national conditions was carried out on the basis of strategic documents, legal acts, and statistical reports concerning the analyzed area in Poland. The selection of materials was purposeful and aimed at identifying key institutional, legal, and socio-economic factors influencing the phenomenon under study.

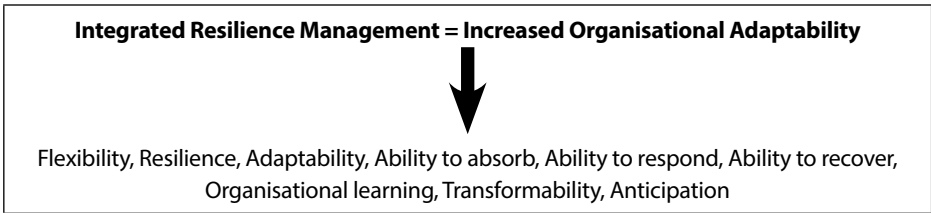
Organisational resilience as management category

The concept and evolution of the organisational resilience

Organisational resilience is understood as the ability of an organisation to absorb disruptions, adapt to changing conditions, and maintain or quickly recover key operational functions in the face of crises (Davidson, 2025). International standards emphasise that it is the ability of an organisation to withstand disruptions and

continuously achieve its goals and even grow despite adversity. For example, the ISO 22316 standard defines organisational resilience as the ability to “absorb” the impact of change and adapt to it, so that the organisation can continue to achieve its goals, survive disruption and evolve. Resilience is therefore treated as a strategic competence of the organisation – not a static state, but a continuous result of good management and adaptability (DesJardine et al., 2019). Unlike traditional risk management (focused mainly on avoiding threats), the concept of resilience emphasizes active learning from difficult experiences and the use of crises as development opportunities (Davidson, 2025). In other words, a resilient organisation not only protects itself from threats, but is able to emerge from them strengthened, building competitive advantages thanks to the experience gained (Figure 1).

Figure 1. Resilience definition approach



Source: authors’ own elaboration.

The concept of resilience originated in the natural sciences and psychology but was adapted in management science in the early 21st century in response to the need to better understand why some organisations handle crises more effectively than others. The literature indicates that organisational resilience manifests two complementary behavioural dimensions: stability (the ability to maintain continuity of core functions despite shocks) and flexibility (the ability to adapt and change in response to disruption) (Chodyński, 2025). Stability involves the preservation of an organisation’s key features and identity even during extreme turbulence in the environment (e.g. wars, disasters, terrorist attacks), which is particularly important for entities providing uninterrupted services such as critical infrastructure (Chodyński, 2021).

Flexibility, on the other hand, manifests itself in adapting the organisation to new conditions – enhancing its ability to adapt and innovate in response to change. As part of the concept of resilience, both these perspectives complement each other: the organisation must be resilient to shocks to some extent, but at the same time malleable and capable of transformation to meet unpredictable challenges (Chodyński, 2025).

The development of the concept of organisational resilience has been fostered by numerous empirical studies conducted in the aftermath of disasters and economic

crises. For example, the experience after the devastating tornado in New Zealand in 2005 initiated pioneering work on business resilience models (Chodyński, 2021).

In her doctoral dissertation, Amy Stephenson (2010) proposed a model for benchmarking organisational resilience, identifying two pillars: (1) strategic and operational planning (including strategy planning, contingency plans and exercises, proactive attitudes, partnerships with stakeholders, and clarity of objectives) and (2) adaptive capacity (including avoiding “tunnel vision,” effective use of internal resources, employee engagement, a learning culture, flexible leadership, innovation, and efficient decision-making). Similar resilience models emphasized that organisations capable of surviving and developing despite shocks are characterised by both solid plans and resources for the crisis and a culture conducive to continuous adaptation and improvement (Stephenson, 2010).

In the following years, organisational resilience gained in importance as an element of management standards. The British standard BS 65000 (2014) and the international standard ISO 22316 (2017) systematised the approach to resilience by presenting sets of principles and attributes of resilient organisations. Resilience has come to be seen as an umbrella strategic concept that integrates different areas of risk management, business continuity, security and innovation. This means that instead of treating resilience as a single programme (e.g. business continuity planning only), organisations are learning to shape it holistically – through leadership, organisational culture, process improvement and the ability to learn from mistakes. This trend particularly intensified during and after the COVID-19 pandemic, when many businesses were painfully affected by the disruption and began to look for ways to increase their resilience to future crises (Skrzypek, Skrzypek, 2023).

Despite the growing popularity of the concept of organisational resilience, there is still no single consistent definition in the literature that is universally accepted as superior. Different authors emphasise different aspects – from approaches focusing on “rebounding” after a crisis, to perspectives on dynamic adaptability, to treating resilience as a result of the organisation’s various competences. Research efforts are underway to develop a well-established theory of organisational resilience with high application values. Numerous case studies in recent years (e.g. during pandemics) have provided data on the drivers of corporate resilience and the tools for building it in practice. However, there are still noticeable research gaps that need to be deepened, for example in the links between the level of resilience and long-term organisational effectiveness and maturity. There is a lack of comprehensive research showing how resilience translates into business results, innovation or sustainable development of the organisation. This points to the need for further, systematic research into measuring organisational resilience and the integration of this concept with other areas of management (e.g. business continuity, process improvement) (Skrzypek & Skrzypek, 2023).

In summary, organisational resilience is still an evolving management category – it already has a well-established theoretical basis and examples of application but needs further conceptualisation and a standardised approach to realise its full practical potential.

It is worth noting that although the concept of organisational resilience has mainly developed in the context of industrial companies, the financial sector and classic critical infrastructure, its application in the onshore wind sector faces specific considerations. Indeed, wind farms operate under conditions of high environmental variability, dependence on weather factors and strong integration with the electricity system, which makes the adaptability of the operator’s organisation particularly important (Table 1).

Table 1. Resilience as an integrated management component

Area	Traditional approach	Resilience-based approach
Role	Management as an additional component of the management process	Integrated management as a core component of the management process
Nature of activities	After the event – reactive	Proactive and adaptive
Capacity of the organisation	Procedures	Flexible response to changes
Response to disturbances	Post-event recovery	Acquisition of adaptability
Supply Chain	Sensitive to changes	Resistant to disturbances

Source: authors’ own elaboration.

Resilience versus technical resilience: A comparative approach

When analysing organisational resilience, it is useful to distinguish between its “soft” (human, organisational) and “hard” (technical) aspects. The literature highlights that the terms organisational resilience and organisational resilience are sometimes used interchangeably, although they do not always mean exactly the same thing (Pytel, 2025). Resilience accentuates an organisation’s dynamic ability to recover, learn and adapt in a changing environment. Organisational resistance, on the other hand, is sometimes interpreted more broadly – as the overall ability to survive and maintain business continuity despite disruption. Resilience can thus be said to be a specific dimension of resilience: it is an adaptive and process-oriented component, whereas resilience (in technical or structural terms) is more often associated with the resilience and stability of a system (Pytel, 2025). In practice, effective crisis management requires both – both robust technical safeguards and organisational flexibility.

Technical resilience refers to the longevity and ability to quickly restore the performance of physical systems and infrastructure after a disruption. This includes the resilience of the infrastructure and the ability of engineered systems to operate

under fault conditions or to recover efficiently. For example, in the context of infrastructure networks, technical resilience can be measured by the number of critical components that have failed following an incident (e.g. the number of transformer substations shut down or percentage of pipelines damaged) and the time taken to repair them (Zhao et al., 2015).

Organisational resilience, on the other hand, is concerned with the human and process dimensions of system functioning – that is, the ability of an organisation's management structure to respond effectively to crisis situations, maintain continuity of key services and adapt in the face of new circumstances (Moteff et al., 2003). In practice, a measure of organisational resilience could be, for example, the percentage of users or areas that lost access to a service due to a failure: the smaller the scale of the service disruption (thanks to the organisation's efficient response), the higher the assessment of the organisational resilience of that structure (Zhao et al., 2015). In other words, technical resilience answers the question of how well equipment and systems can withstand an impact (e.g. a natural disaster) and how quickly it can be repaired, while organisational resilience answers the question of how well people and procedures can respond to minimise the effects of a disruption on the continued operation of the overall system.

A comparison between organisational resilience and technical resilience reveals both their distinct and complementary nature. Technical resilience tends to be more tangible and quantifiable – it depends on factors such as hardware redundancy, quality of materials, system architecture, planning for spare capacity, etc. It focuses on the prevention of physical failures and the rapid repair of damage. Organisational resilience, on the other hand, is based on soft factors: an organisational culture that promotes readiness for change, employee competencies (e.g. the ability to improvise, cooperate under pressure), an efficient crisis communication system, flexible procedures and leadership able to make decisions under conditions of uncertainty (Davidson, 2025). Technical resilience can ensure that the 'hard' infrastructure survives a hit (e.g. thanks to spare servers, the IT system will not go down with a single failure), but without resilient organisation, even the best infrastructure can be misused – for example, if action plans are missing or staff cannot respond to an alarm, the impact of a failure will still be severe. Conversely, a well-trained crisis team will do little if key equipment has no safeguards and is completely destroyed.

The risk management literature emphasises that the two dimensions – technical and organisational – must go hand in hand to achieve a truly high level of resilience (Rehak, 2020). Critical infrastructure research has even shown that resilience needs to be considered in a multidimensional perspective. For example, Bruneau et al. (2003) and Chang and Shinozuka (2004) proposed four interrelated dimensions for assessing the resilience of infrastructure systems: technical, organisational, social and economic. Importantly, they found that the technical and organisational

dimensions are key to maintaining the functionality of the infrastructure itself, while the social and economic aspects reveal themselves more at the level of the resilience of the whole community or market environment. It is clear from this that omitting any of these key dimensions (technical or organisational) impoverishes the picture of resilience. Indeed, previous studies have often focused solely on technical indicators (e.g. equipment reliability) or only on organisational aspects, leading to incomplete and sometimes contradictory conclusions on the actual level of system resilience. Zhao et al. (2015) note that it is difficult to fully assess resilience by analysing only one dimension – therefore, it is necessary to develop integrated metrics that take into account both technical and organisational perspectives to get a holistic view and avoid erroneous conclusions. In other words, future research work should focus on the links between technical resilience and organisational resilience – how one affects the other – and the creation of tools to diagnose and improve resilience in a comprehensive manner. This integration of approaches will allow organisations to develop a balance between investing in infrastructure reliability and developing an organisational culture of resilience, maximising the overall ability to survive and thrive under uncertainty.

Organisational resilience in the context of critical infrastructure

The concept of organisational resilience takes on particular relevance in relation to critical infrastructure – that is, systems and facilities whose disruption could threaten the security of the state, the lives of citizens or seriously disrupt essential services (such as energy supply, water supply, communications, transport or health-care). Critical infrastructure forms the lifeblood of modern society, hence its ability to withstand a variety of threats is crucial. Traditionally, there has been a strong emphasis on the technical security of such systems – i.e. physical security, equipment redundancy, contingency planning, etc. However, the current state-of-the-art approach also takes into account the organisational resilience of critical infrastructure managers. Operators and owners of critical infrastructures are required to maintain not only a high level of technical reliability of their systems, but also a high level of organisational resilience of their companies (Rehak, 2020). Only then will continuity of operation of these systems be ensured even in the face of major disruption.

Although onshore wind farms are not always formally classified as critical infrastructure in the legal sense, from a functional perspective – their increasing share of the power balance and their importance for energy security – they are increasingly acting as *de facto* critical infrastructure, which justifies the application of advanced organisational resilience management concepts to them.

Organisational resilience in the critical infrastructure sector manifests itself on many levels. Firstly, operational and emergency preparedness is key – organisations

responsible for infrastructure must constantly monitor risk factors, train staff in emergency procedures and update business continuity plans. Research indicates that organisational resilience is an important determinant of the ability of critical infrastructure elements to adapt in the face of disruption (Rehak, 2020). In other words, even the most technically advanced system may not be very resilient if the organisation managing it cannot make accurate decisions quickly in a crisis situation or lacks coordination and situational awareness. Critical infrastructure management therefore emphasises the development of characteristics such as situational awareness of management and staff, a culture of safety and continuous learning, effective internal and external communication during emergency events, and the ability to cooperate with other actors (e.g. emergency services, suppliers, public administration) under time pressure. All these elements make up the organisational resilience of the infrastructure operator.

In the context of critical infrastructure, it has proved very useful to frame resilience through these four dimensions: technical, organisational, social and economic (Zhao et al., 2015). This approach means that when assessing the resilience of, for example, an electricity system, one should consider not only the efficiency of the equipment (technical dimension), but also the preparedness of the managing organisation (organisational dimension), the impact of a potential failure on society (social dimension, e.g., the consequences of power outages for the population), and the ability to minimise financial losses and achieve a rapid economic recovery (economic dimension). Chang and Shinozuka's (2004) research on lifeline networks (water, power) showed that the first two dimensions, technical and organisational, are key to keeping the critical infrastructure itself functioning. This means that the organisation operating the infrastructure is integral to its resilience – it cannot be assumed that a strong equipment design alone will suffice if the human and organisational factor is neglected (Zhao et al., 2015).

Examples from recent years have vividly demonstrated the importance of organisational resilience for critical infrastructure. The 2021 Texas energy crisis (caused by extreme cold weather) revealed that some energy companies were only focused on surviving without power, while others were able to use the crisis as an impetus for growth – winning new customers and investing in strengthening their systems (Davidson, 2025). This difference was largely due to different organisational attitudes: the more resilient companies had a culture of responding proactively to disruption, so that at the moment of trial they were able not only to secure basic operations but even to improve their position in the market (Davidson, 2025). This case showed that managing critical infrastructure requires thinking beyond simply restoring the status quo after a disaster – it is necessary to learn from crises and make changes that will increase resilience for the future (e.g. diversifying supplies, modernising procedures, investing in intelligent control systems).

In response to such challenges, organisations in critical infrastructure sectors are increasingly implementing comprehensive resilience strengthening programmes. These include, *inter alia*, regular assessments of organisational resilience-identifying weaknesses in the management structure, safety culture, supply chain, etc. – so that corrective action can be taken in advance (Rehak, 2020). An example is the ASOR (Assessing and Strengthening Organisational Resilience) method developed for the infrastructure sector to systematically assess the determinants of organisational resilience and identify areas for improvement. In addition, governance standards recommend that resilience issues should be integrated into existing business continuity, risk and security management systems. A holistic approach is recommended, in which emergency planning, risk management, infrastructure maintenance and organisational improvement are coordinated within an overarching resilience strategy. Such an integrated system avoids a siloed approach to security issues – every relevant business process is also assessed for its impact on resilience, and strategic decisions take into account the risks and opportunities associated with potential disruptions.

In summary, in the context of critical infrastructure, organisational resilience is an integral component of system security. It is the people, decision-making structures and organisational culture that determine whether even a perfectly designed infrastructure survives a crisis without a breakdown in function. Current challenges (e.g. climate change generating extreme weather events, cyber threats, global pandemics) confirm that investing in hard defences alone is not enough – it is also necessary to develop resilience on a “soft” level. The literature points to the need to further systematise knowledge on best practices for building organisational resilience in critical infrastructure and measuring its effects. An open research question remains, for example, the quantification of the impact of high organisational resilience on the reduction of the consequences of failure (in socio-economic terms) or on the speed of recovery of full system functionality. There are also gaps in understanding the long-term economic benefits of investing in organisational resilience – do more resilient organisations achieve better financial performance and innovation over stable periods due to their adaptability? These questions point to directions for further research. However, it is already clear that organisational resilience is a critical success factor in critical infrastructure management and should be treated on a par with technical resilience in strategies to ensure security and business continuity of essential public services.

Table 2. Technical and organisational resistance and the impact of resilience on critical infrastructure

Area	Technical resistance	Organisational resistance	Resilience	Impact of resilience on the management of critical infrastructure
Elements	Technology	Structures, procedures, competences	A systemic approach, taking into account the period before and after the event	Cooperation in technology, organisational resilience and systems approach
Purpose	Resistance to technical incidents	Resilience to organisational events	System restoration after an event	Ensuring continuity of management
Response to disturbances	Yes	Yes	Yes – adaptation, learning	The ability of critical infrastructure elements to adapt in the face of disruption
Recovery	Yes	Yes	The ability of the organisation's management structure to respond effectively to crisis situations, maintain continuity of key services and adapt	Speed of recovery of full system functionality
Risk management approach	Process-oriented approach	Organisational and process-oriented approach	A systemic approach	Management consistency; learning from crises and implementing changes that increase future resilience

Source: authors' own elaboration.

The failure of wind turbines results from various technical and environmental factors. In Poland, there have been cases of mechanical damage, such as turbines collapsing under strong winds, like in Korzkwy, or fires in the nacelles. Abroad, lightning often damages the blades, as seen at Vineyard Wind in the USA or Lal Lal Wind Farm in Australia. Mechanical problems, such as gearbox or brake failures, have caused partial collapses of turbines in Denmark and the USA. Extreme weather conditions, including hurricane-force winds, also pose a threat to the structures, as shown in Germany. All these events highlight the importance of monitoring, predictive maintenance, and designing resilient wind energy systems.

Summary

The analysis carried out allows us to conclude that under conditions of the increasing share of onshore wind power in the national power balance and the increasing integration of these sources into the transmission and distribution grid, organisational

resilience is becoming a management category of comparable importance to the technical reliability of the installation. Wind farms operate in an environment characterised by high variability of operating conditions and interdependence with the electricity system, which means that the scale and persistence of operational disturbances depends not only on the technical parameters of the equipment, but also on the maturity of decision-making structures, coordination capabilities, the quality of crisis communication and the adaptive skills of the operator’s organisation. Consequently, the management of organisational resilience should be considered as a strategic element, determining the sector’s ability to maintain business continuity and reduce vulnerability to systemic disruptions.

The article demonstrates that resilience in the onshore wind sector is hybrid: it results from the integration of “hard” (technical) solutions with “soft” (organisational) mechanisms, including risk management, business continuity planning, competence development and the development of a safety and learning culture. Of particular importance here is the organisation’s ability to rapidly transition from routine to disruptive operations mode and then to effectively rebuild operational capability, while minimising the impact on system stakeholders – including network operators, customers and the regulatory environment. This means that the organisational resilience of wind farm operators should be developed in a systemic rather than incidental way as a permanent element of corporate governance.

At the same time, the results of the analysis point to the need for further standardisation of approaches and tools to diagnose and improve organisational resilience in the RES sector. This concerns, in particular: (1) the development of sectoral organisational resilience metrics to benchmark organisational maturity and monitor the effects of improvement actions; (2) the integration of resilience management processes with compliance, cyber security and energy market participant requirements; (3) the development of models of cooperation between wind farm operators and electricity system operators that would limit the effects of grid disruptions and foster the coordination of actions in emergency situations. The empirical verification of the relationship between the level of organisational resilience and the reduction of operational losses and the ability to recover quickly from technical and system disruptions remains a particularly important research direction (Table 3).

Table 3. Technical and organisational resilience in the onshore wind sector

Technical resilience	Organisational resilience
reliability and durability of wind turbines	risk management and business continuity planning
technical monitoring and diagnostic systems (e.g., turbine condition monitoring)	procedures for responding to failures and emergency situations
redundancy of key components and control systems	competencies and training of technical personnel

Technical resilience	Organisational resilience
infrastructure resilience to weather conditions and extreme weather events	cooperation with grid operators and regulatory institutions
protection systems and automatic turbine shutdown mechanisms	safety and quality management systems
regular maintenance and servicing of technical infrastructure	organisational flexibility and the ability to adapt to regulatory and market changes
digital systems for wind farm operation management (SCADA)	supply chain management for spare parts and maintenance services
cybersecurity of control and communication systems	communication and coordination between wind farm operators, service teams, and power system operators

Source: authors' own elaboration.

In summary, effective management of organisational resilience in the onshore wind energy sector should be considered as one of the key conditions for the stable functioning of this RES segment and the strengthening of energy security in Poland. Resilience should not be seen as an “add-on” to infrastructure operation, but as an integrated management component that – through the development of an organisation’s adaptive capacity – makes it possible to reduce the effects of disruptions, improve supply reliability and increase the resilience of the electricity system in the reality of the ongoing energy transition. The conclusions obtained confirm the hypothesis formulated at the outset. The article is introductory and provides a starting point for further in-depth research into the issue under consideration.

References

- Bruneau, M. et al. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*, 19(4), 733–752. <https://doi.org/10.1193/1.1623497>
- Chang, S. E., Shinozuka, M. (2004). Measuring improvements in the disaster resilience of communities. *Earthquake Spectra*, 20(3), 739–755. <https://doi.org/10.1193/1.1775796>
- Chodyński, A. (2022). Kryzys pozaekonomiczny przedsiębiorstwa – ekologiczny aspekt rezylencji organizacyjnej [The non-economic crisis of the enterprise – the ecological aspect of organisational resilience]. In A. Chodyński, D. Fatuła, M. Leśniewski (Eds.). *Zrównoważony rozwój, systemy informacyjne i zarządzanie bezpieczeństwem w perspektywie długoterminowej przedsiębiorstw* [Sustainable development, information systems and security management in the long-term perspective of enterprises] (pp. 11–31). Oficyna Wydawnicza AFM.
- Chodyński, A. (2025). Interesariusze w modelu rezylencji organizacyjnej wobec zagrożeń ekologiczno-energetycznych [Stakeholders in the model of organizational resiliency in the face of environmental and energy threats]. *Bezpieczeństwo. Teoria i Praktyka*, 1, 23–38. <https://doi.org/10.48269/2451-0718-btjp-2025-1-001>
- Chodyński, A., Huszлак, W., Rosa, K. (2024). Audyt zarządzania interesariuszami organizacji wobec zagrożeń ekologiczno-energetycznych [Audit of the organization’s stakeholder

- management in the face of ecological and energy threats]. *Bezpieczeństwo. Teoria i Praktyka*, 4, 89–104. <https://doi.org/10.48269/2451-0718-btip-2024-4-006>
- Davidson, R. (2025, October 17). Jak przestać się tylko bronić i zacząć wygrywać. Nowe myślenie o odporności organizacyjnej zmienia sektor energetyczny [How to stop just defending and start winning: New thinking on organisational resilience is changing the energy sector]. *Nowa Energia*, 4, <https://nowa-energia.com.pl/2025/10/17/jak-przestac-sie-tylko-bronic-i-zaczac-wygrywac-nowe-myslenie-o-odpornosci-organizacyjnej-zmienia-sektor-energetyczny/> [accessed: 2.01.2025].
- Desjardine, M., Bansal, P., & Yang, Y. (2019). Bouncing back: building resilience through social and environmental practices in the context of the 2008 global financial crisis. *Journal of Management*, 45(4), 1434–1460.
- Ministry of Climate and Environment. (2021). *Energy Policy of Poland until 2040* [Polityka energetyczna Polski do 2040 r.]. <https://www.gov.pl/web/climate/energy-policy-of-poland-until-2040-cpp2040>
- Ministry of Climate and Environment. (2025). *Krajowy Plan w dziedzinie Energii i Klimatu do 2030 r. z perspektywą do 2040 r.* [National Energy and Climate Plan until 2030 with a perspective until 2040]. <https://www.gov.pl/web/klimat/projekt-krajowego-planu-w-dziedzinie-energii-i-klimatu-do-2030-r-z-perspektywa-do-2040-r-wersja-przekazana-do-dalszego-procedowania-na-poziomie-rady-ministrow>
- Moteff, J.D., Copeland, C., Fischer, J.W. (2003). *Critical Infrastructures: What Makes an Infrastructure Critical?* Report for Congress (CRS) RL31556, Congressional Research Service, The Library of Congress, <https://digital.library.unt.edu/ark:/67531/metacrs5039/>
- Pytel, D. (2025). *Model budowania odporności organizacyjnej jako strategia zarządzania siecią kin* [A model for building organizational resilience as a cinema chain management strategy] [Doctoral dissertation, WSB University, Dąbrowa Górnicza]. https://wsb.edu.pl/files/pages/1608/autoreferat_d_pytel.pdf [accessed 12.12.2025].
- Rehak, D. (2020). Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic. *Safety Science*, 123, Article 104573. <https://doi.org/10.1016/j.ssci.2019.104573>
- Skrzypek, E., & Skrzypek, A. (2023). Odporność organizacji i jej wyznaczniki [Organisational resilience and its determinants]. *Problemy Jakości*, 2, 2–11, <https://doi.org/10.15199/46.2023.2.1>
- Stephenson, A. (2010). *Benchmarking the resilience of organisations* [Doctoral thesis, University of Canterbury]. https://ir.canterbury.ac.nz/bitstream/handle/10092/5303/THESIS_BENCHMARKINGTHERESILIENCEOFORGANISATIONS.pdf?sequence=1&isAllowed=y [accessed: 12.12.2025].
- Zhao, X., Chen, Z., & Gong, H. (2015). Effects comparison of different resilience enhancing strategies for municipal water distribution network: A multidimensional approach. *Mathematical Problems in Engineering*, Article 438063. <https://doi.org/10.1155/2015/438063>

Managing organisational resilience in the onshore wind energy sector in Poland **Abstract**

The dynamic development of onshore wind energy in Poland increases its importance for the national electricity system and creates new challenges related to technical failures, system disruptions and continuity of energy supply. The article analyses organisational resilience management mechanisms in the Polish onshore wind sector, understood as practices, procedures and competences supporting business continuity, disruption

mitigation and rapid recovery. The analysis, based on literature and national conditions, highlights the managerial dimension of resilience, including decision-making structures, risk management, business continuity planning and cooperation with power system operators. The findings indicate that effective resilience management can reduce wind farm vulnerability to disruptions and requires integrating technical solutions with mature organisational mechanisms and a safety culture. The article also identifies areas for further standardisation and research.

Keywords: organisational resilience management, wind energy, energy security, business continuity, critical infrastructure

Author Contributions

Conceptualization: A.B., M.P.

Methodology: A.B., M.P.

Formal analysis: A.B., M.P.

Investigation: A.B., M.P.

Resources: A.B., M.P.

Writing – original draft: A.B., M.P.

Writing – review & editing: A.B., M.P.

Supplementary Materials

Not applicable.

Funding

This research received no external funding.

Ethics Approval Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Data sharing is not applicable to this article as no new data were generated or analyzed in this study.

Declaration of Generative AI Use

No artificial intelligence tools were used in the preparation of this manuscript.

Acknowledgments

Not applicable.

Conflict of Interest

Both authors declare no conflict of interest.

Bezpieczeństwo i analiza ryzyka we wdrażaniu sztucznej inteligencji w bankowości detalicznej

Dariusz Fatuła

dr hab., prof. UAFM, Wydział Zarządzania, Mediów i Technologii, Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie (Faculty of Management, Media and Technology, Andrzej Frycz Modrzewski Krakow University, Kraków, Poland)
<https://orcid.org/0000-0002-6704-2585>

Wprowadzenie

Sztuczna inteligencja (AI) od wielu lat stanowi jeden z najbardziej dynamicznie rozwijających się obszarów technologii, które wywierają istotny wpływ na sektor bankowości detalicznej. Pierwsze zastosowania AI w bankach, sięgające lat 80. i 90. XX wieku, obejmowały systemy eksperckie i proste modele predykcyjne wspierające analizę ryzyka, ocenę zdolności kredytowej oraz wykrywanie prób oszustw (Baesens i in., 2016). Dzięki postępowi w dziedzinie uczenia maszynowego, przetwarzania dużych zbiorów danych oraz rosnącej dostępności mocy obliczeniowej, systemy te zostały znacznie rozbudowane i obecnie stanowią podstawę wielu procesów decyzyjnych w bankowości detalicznej. Sztuczna inteligencja w bankowości detalicznej przestaje być eksperymentem technologicznym, a staje się infrastrukturą decyzyjną o znaczeniu systemowym. W polskiej i międzynarodowej literaturze opisuje się już szerokie spektrum zastosowań – od automatyzacji procesów operacyjnych, przez ocenę zdolności kredytowej, wykrywanie nadużyć i personalizację ofert, po wsparcie nadzoru zgodności regulacyjnej. Równolegle podkreśla się, że każdy z tych obszarów generuje nowe typy ryzyka oraz wzmacnia istniejące ekspozycje sektora finansowego

(Szostek i in. 2022; Ziółkowska 2023; Shi i in. 2022; Noriega i in. 2023). W analizach dotyczących wpływu sztucznej inteligencji na rynek finansowy akcentuje się dualny charakter tej technologii: z jednej strony poprawia ona efektywność, dokładność predykcji i dostępność usług, z drugiej – zwiększa złożoność systemu, tworzy zależność od dostawców zewnętrznych (w tym Big Tech), pogłębia koncentrację rynku i rodzi trudne do oszacowania ryzyka dla stabilności finansowej (Financial Stability Board, 2024). W polskich opracowaniach kierowanych do sektora bankowego zwraca się uwagę, że instytucje finansowe stają wobec równoległego wymogu budowania przewagi konkurencyjnej dzięki AI oraz wdrożenia rygorystycznych mechanizmów kontroli, aby uniknąć naruszeń praw konsumentów, kar finansowych i utraty reputacji (Centrum Procesów Bankowych i Informacji, 2024).

Celem artykułu jest przegląd literatury oraz raportów z badań w celu pogrupowania i usystematyzowania wspomnianych zagadnień ryzyka wdrażania AI w bankowości detalicznej w obszarach łączących perspektywę zarządzania, prawa i technologii. Podjęto też próbę identyfikacji najważniejszych luk pomiędzy teorią a praktyką oraz zaproponowano ramy koncepcyjne ich wypełnienia.

Najważniejsze zastosowania AI w bankowości detalicznej

AI znajduje coraz szersze zastosowanie w bankowości detalicznej, transformując praktycznie wszystkie aspekty usług bankowych oferowanych klientom indywidualnym. Jednym z najstarszych i najbardziej zaawansowanych zastosowań AI w bankowości detalicznej jest automatyczna ocena kredytowa (*credit scoring*) i oceny ryzyka klienta (*underwriting*), gdzie systemy AI wykorzystują uczenie maszynowe do analizy historii kredytowej, zachowań finansowych, danych transakcyjnych oraz alternatywnych źródeł danych (takich jak np. historia płatności za media lub zakupy w sieci) w celu ustalenia zdolności kredytowej klienta (Sachan i in. 2020; Nimma-gadda, 2022).

Chatboty oparte na AI oraz wirtualni asystenci stanowią transformacyjną technologię w obsłudze klientów banków detalicznych. Banki wdrażają zaawansowane systemy konwersacyjne, które mogą obsługiwać miliony zapytań klientów. Wirtualni asystenci wykorzystują przetwarzanie języka naturalnego (*natural language processing*, NLP) do wyjaśniania warunków usług finansowych, pomagania w inicjowaniu transakcji, oferowania spersonalizowanych produktów oraz wspierania w zarządzaniu kontem.

AI znacznie podnosi jakość personalizacji usług bankowych poprzez analizę historii transakcji, zachowań wydatkowych oraz preferencji klientów. Systemy rekomendacyjne mogą automatycznie identyfikować momenty, w których klient jest gotów do przejścia na wyższą kategorię karty kredytowej, zaciągnięcia pożyczki czy otwarcia rachunku oszczędnościowego. AI służy też prognozowaniu, którzy klienci

mogą opuścić bank (*customer churn*), na podstawie analizy wzorców aktywności, zmian w wydatkach oraz interakcji z bankiem. Pozwala to bankom na proaktywne podejmowanie działań zapobiegawczych (retencyjnych). Modele predykcyjne segmentują również klientów, przewidują odejścia, analizują lojalność oraz generują wartościowe spostrzeżenia (*insighty*) na potrzeby marketingu i zarządzania portfelem produktów.

Systemy AI do wykrywania oszustów znacznie ograniczają koszty związane wyłudzeniami, oszustwami i innymi bezprawnymi działaniami w bankowości (Uddin 2025). Algorytmy uczenia maszynowego analizują w czasie rzeczywistym miliony transakcji, identyfikując anomalie i podejrzane wzorce, które mogą wskazywać na oszustwa lub nieautoryzowany dostęp. Banki wdrażają zaawansowane systemy AI, które zmniejszają liczbę fałszywych alarmów (*false positives*), jednocześnie poprawiając detekcję rzeczywistych zagrożeń. Aplikacje wykorzystują zaawansowane modele statystyczne i generatywne do aktywnej identyfikacji podejrzanych płatności oraz wczesnego ostrzegania o zagrożeniach.

Przestrzeganie zgodności z szybko zmieniającymi się przepisami prawa (*compliance*) w bankowości ewoluuje dzięki sztucznej inteligencji. Skomplikowane regulacje jak AI Act czy Basel IV wymagają aktualizacji bądź zmiany wewnętrznych przepisów i procedur bankowych. AI szybciej niż prawnicy wyłapuje niezgodności w wielu skomplikowanych dokumentach, opisach, materiałach marketingowych i proponuje odpowiednie zmiany.

AI przetwarza ogromne zbiory danych w czasie rzeczywistym, identyfikując ryzyka operacyjne, kredytowe, rynkowe i regulacyjne szybciej niż tradycyjne metody, automatyzuje złożone procesy, zwiększa precyzję predykcji i zapewnia zgodność z obowiązującym prawem. Biorąc pod uwagę powyższe zastosowania, można uznać, że AI jest obecnie ważnym narzędziem zarządzania szeroko pojętym ryzykiem w działalności banku. Równocześnie jednak samo wdrażanie i wykorzystywanie AI rodzi pewne specyficzne ryzyka.

Obszary ryzyka we wdrażaniu i funkcjonowaniu AI

Ryzyka prawne i regulacyjne

Wdrożenie systemów AI w bankowości detalicznej generuje ryzyka prawne i regulacyjne wynikające z nieprzejrzystości algorytmów oraz trudności w zapewnieniu kontroli człowieka nad decyzjami automatycznymi. EU AI Act klasyfikuje systemy oceny zdolności kredytowej jako „wysokiego ryzyka”, nakładając obowiązek wdrożenia systemów zarządzania ryzykiem, przejrzystości decyzji oraz dokumentacji cyklu życia modelu, z karami do 35 mln euro lub 7% globalnego obrotu rocznego (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689, 2024).

General Data Protection Regulation (GDPR, w Polsce: Rozporządzenie o Ochronie Danych Osobowych – RODO), obowiązujące od 25 maja 2018 r. w całej UE, w art. 22 wymaga prawa do wyjaśnienia decyzji automatycznych, jednak mechanizmy takie jak SHAP¹ czy LIME² nie spełniają prawnych wymogów „wyjaśnienia”, generując jedynie techniczne przybliżenia nieprzystające do oczekiwań regulacyjnych (Edwards i Veale, 2017). Kroll i in. (2017) wskazują, że pełna transparentność kodu źródłowego algorytmów prowadzi do paradoksu: ujawnienie umożliwia obchodzenie systemu przez zainteresowanych lub osłabia konkurencyjność twórców. Proponują zamiast tego kryptograficzne mechanizmy procedury zgodności wyników z polityką decyzyjną bez ujawniania algorytmu. Citron i Pasquale (2014) dokumentują nieprzejrzystość systemów oceny kredytowej (*scoring*), gdzie instytucje finansowe odmawiają dostępu do szczegółów metodologii, uniemożliwiając audyt indywidualnych decyzji, co prowadzi do arbitralnych ocen kredytowych. Szostek i in. (2022) analizują specyficzne ryzyka dla polskiego sektora bankowego, wskazując na odpowiedzialność banków za systemy AI stron trzecich, trudności w kwalifikacji modeli jako wysokiego ryzyka oraz wymogi dokumentacji zgodne z AI Act. Financial Stability Board (2024) podkreśla, że rosnąca zależność od zewnętrznych dostawców AI zwiększa koncentrację ekspozycji, gdzie awarie lub błędy u jednego dostawcy mogą wywołać efekty systemowe. Podczas gdy istnieje znacząca literatura dotycząca akceptacji technologii oraz zaufania do automatyzacji (Lee i See, 2004; Venkatesh i in., 2003), brakuje szczegółowych badań empirycznych na temat długoterminowego wpływu interakcji z systemami AI na zachowania finansowe klientów banków detalicznych. Raport World Economic Forum (2025) wskazuje, że wymaga się większej wiedzy na temat stosunku pracowników do AI oraz dynamiki zmian miejsc pracy w kontakcie z AI. Brakuje również badań na temat psychologicznych skutków stosowania AI przez pracowników i klientów. Pytania: jak klienci reagują na wielokrotne błędy AI? Czy generatywna AI faktycznie buduje zaufanie, czy je podważa? — pozostają w dużej mierze niezbadane. Brakuje też empirycznych badań na temat tego, w jaki sposób łączne zastosowanie Blockchain i AI mogłoby zwiększyć bezpieczeństwo transakcji i zapobiegać oszustwom w bankach detalicznych, szczególnie w kontekście zapewniania audytowalności i transparentności rozwiązań informatycznych (Pramudito i in., 2025).

Ryzyko operacyjne i automatyzacji procesów

Ryzyko operacyjne definiowane jest jako potencjalne straty wynikające z nieadekwatnych lub nieskutecznych procesów wewnętrznych, ludzi oraz systemów lub

¹ SHAP (SHapley Additive exPlanations) działa na zasadzie wartości Shapleya z teorii gier – krok po kroku wyjaśnia, ile każda cecha przyczyniła się do konkretnej predykcji modelu.

² LIME (Local Interpretable Model-agnostic Explanations) działa lokalnie – krok po kroku aproksymuje skomplikowany model (*black-box*) prostym modelem liniowym w otoczeniu konkretnej predykcji.

z wydarzeń zewnętrznych (McLemore i Mihov 2026). W bankowości detalicznej automatyzacja procesów za pomocą sztucznej inteligencji – obejmująca m.in. poznanie swojego klienta (KYC – *know your customer*), przeciwdziałanie praniu pieniędzy (AML – *anti-money laundering*), detekcję nadużyć (*fraud detection*), ocenę kredytową (*scoring*) i obsługę klienta przez rozmowy z AI – zmienia profil tego ryzyka poprzez zwiększoną złożoność systemów, zależność od dostawców zewnętrznych oraz nowe możliwości ataków hakerskich przez sieć kontaktu klienta z instytucją finansową. Jednym z najważniejszych ryzyk w tym obszarze jest tzw. stronniczość lub w kontekście społecznym uprzedzenie (*bias*) modeli wynikające z doboru danych wejściowych, które z różnych przyczyn zawierają wyniki preferujące lub częściej odrzucające wybranych klientów ze względu na ich cechy jak wiek, płeć, miejsce zamieszkania (Akinrele, 2025). Generatywna AI (GenAI) może udzielać klientom błędnych porad finansowych lub wprowadzać w błąd co do oferty, co prowadzi do strat finansowych i utraty zaufania (halucynacje i błędy modeli). Degradacja jakości modelu w czasie (np. gdy zmieniają się zachowania klientów), prowadzi do błędnych decyzji kredytowych lub związanych z wykryciem oszustwa (fraudowych), jeśli model nie jest stale rekalkulowany. Poleganie na kilku dużych dostawcach chmury/AI stwarza zagrożenie systemowe w przypadku awarii ich infrastruktury (koncentracja ryzyka kontrahenta). Ryzyko kontrahenta polega przede wszystkim na potencjalnych stratach wynikających z niewywiązania się z zobowiązań przez zewnętrznych dostawców rozwiązań AI, fintechy czy platformy technologiczne. Opóźnienia w dostawie, uaktualnieniach czy poprawie błędów systemu, nie mówiąc już o bankructwie lub zaprzestaniu działalności przez kontrahenta, może narazić bank na dezorganizację pracy, utratę zaufania i wysokie kary nadzoru. Nawet w pozornie dobrze działających systemach dostarczonych przez kontrahentów mogą występować błędy i uprzedzenia decyzyjne oraz możliwość wycieku danych i utraty prywatności, co stanowi osobne ryzyko opisane dalej.

Na poziomie strategicznym minimalizacja tych ryzyk wymaga określenia tolerancji wobec błędów oraz uprzedzeń, zatwierdzenia budżetu na audyty i szkolenia pracowników oraz ustanowienie struktury, np. komitetu ds. etyki AI, który nadzorować będzie zgodność z wytycznymi wewnętrznymi. Na poziomie operacyjnym powinno się opracować procedury testowania uprzedzeń w modelach oceny kredytowej – np. przez badanie, czy prawdopodobieństwo odrzucenia kredytu nie różni się istotnie między różnymi grupami. Zespoły odpowiedzialne za analizę danych (*data science*) i uczenie maszynowe (*machine learning*) powinny zadbać o reprezentatywność danych treningowych (uwzględnienie różnych grup demograficznych), zastosować techniki zapobiegania stronniczości (np. *reweighting*, *adversarial debiasing*) w procesie modelowania, przeprowadzić testy diagnostyczne uprzedzeń (*bias testing*) przed i po wdrożeniu, oraz dokumentować ograniczenia modelu w odniesieniu do różnych segmentów klientów.

Ryzyko wycieku danych i utraty prywatności

AI wymaga dostępu do dużych wolumenów wrażliwych danych, których niewłaściwa ochrona prowadzi do wycieków i naruszeń prywatności (Häuselmann, 2024). Wyzwania te są potęgowane przez wymogi GDPR/RODO i inne reżimy prawne narzucające konieczność wyjaśniania procesu decyzji przez AI (Wachter i in., 2017). Ponadto generatywne modele AI mogą zapisywać (zapamiętywać, memoryzować) wrażliwe dane z danych treningowych i reprodukować je niezamierzenie (Fredrikson i in., 2015). Zgodnie z prawem do wyjaśnienia (*right to explanation*), wprowadzonym przez RODO (art. 22), banki muszą mieć zdolność wyjaśnienia każdej decyzji algorytmicznej wpływającej na klienta. To wymaga nie tylko przejrzystych modeli, ale także stworzenia procedur i nadzorowania procesów zbierania, przechowywania i przetwarzania danych oraz otrzymanych wyników, które mogą wytrzymać audyt regulacyjny.

Ryzyka etyczne i społeczne

Ryzyka te mają swoje źródła w innych, wyżej już opisanych ryzykach, ale ich znaczenie jest nieco inne wymiarze społecznym i etycznym (Mäntymäki 2022). W erze mediów społecznościowych, informacja o powtarzającym się dyskryminowaniu określonych grup klientów banku rozprzestrzenia się wirusowo. Halucynowanie AI w zakresie doradztwa dla klienta może narazić bank na śmieszność i zarzuty braku profesjonalizmu. Wyciek danych klientów, oprócz aspektów prawnych, może spowodować utratę wiarygodności i zaufania, co jest niezwykle groźne w sektorze bankowym. Informacje o podatności na ataki hackerskie, o przerwach w elektronicznym kontakcie z klientami, o zawieszaniu się stron internetowych, szybko roznoszą się po sieci społecznościowej i budzą czasem przesadne obawy wśród klientów. Utrata zaufania może spowodować odpływ klientów, prowadzący w skrajnych wypadkach do utraty płynności. Konieczne w takich wypadkach będą skoordynowane działania działów marketingowych, prawnych i technicznych banku.

Ryzyko kadrowe i luka kompetencyjna

Brak pracowników potrafiących nadzorować i weryfikować działanie zaawansowanych modeli AI (*human-in-the-loop*) znacząco zwiększa ryzyko błędów operacyjnych. Wprowadzanie AI do działalności przedsiębiorstw i banków stało się krytycznym wyzwaniem dla kapitału ludzkiego (Nagarakanti, 2025). Narracja medialna często koncentruje się na utracie miejsc pracy. Nie jest to jednak jedyny efekt – ważniejszy leży w niedopasowaniu kompetencyjnym oraz zjawisku utraty tradycyjnych umiejętności pracowników pozostających w organizacji (Tshewang, 2024). Pracownicy mogą zacząć bezkrytycznie ufać wynikom generowanym przez AI (np. ocenie zdolności kredytowej lub rekomendacji inwestycyjnej), nie rozumiejąc probabilistycznej natury modelu. Pracownicy nieświadomi zjawiska halucynacji (w GenAI) lub uprzedzeń

(w modelach ML – *machine learning*) mogą nieumyślnie wprowadzać klientów w błąd lub naruszać regulacje, używając narzędzi AI w sposób niezgodny z przeznaczeniem. Personel polegający na automatyzacji traci zdolność do samodzielnego wykonywania złożonych zadań. Młodszy personel, który od początku kariery korzysta z automatycznych systemów (problem pokolenia Z), może nigdy nie nabyć głębokiej intuicji kredytowej ani zrozumienia fundamentów ryzyka, które posiadali ich poprzednicy. W sytuacji awarii systemu AI lub wystąpienia nietypowego przypadku, tacy pracownicy stają się bezradni operacyjnie. W przypadku konieczności powrotu do procedur manualnych (np. w wyniku cyberataku na infrastrukturę AI), zarządzający bankiem mogą odkryć, że nie posiadają już kadr zdolnych do ręcznego procesowania transakcji czy oceniania ryzyka w akceptowalnym czasie.

Współpraca na linii człowiek–AI generuje nowe typy błędów operacyjnych. Wprowadzenie „copilotów” (AI Copilots) do oddziałów i call center zmienia dynamikę pracy. Pracownicy mogą mieć tendencję do faworyzowania sugestii algorytmu nad własny osąd lub sprzeczne dowody, co jest szczególnie niebezpieczne w AML (*anti-money laundering*, przeciwdziałanie praniu pieniędzy) i *fraud* (wyłudzeniach danych, pieniędzy). Paradoksalnie, AI może zwiększyć obciążenie kognitywne pracowników. Zamiast wykonywać proste, powtarzalne czynności (które przejęło AI), pracownicy muszą stale zajmować się wyłącznie trudnymi, wyjątkowymi przypadkami, które odrzucił automat, co prowadzi do szybszego zmęczenia, a w konsekwencji wypalenia zawodowego. Luka kompetencyjna potęguje ryzyko operacyjne, wizerunkowe i tworzy asymetrię między szybkością wdrażania algorytmów a zdolnością personelu do ich bezpiecznej obsługi i nadzoru.

Opisane ryzyka nie wyczerpują wszystkich zagrożeń związanych z AI w tym obszarze. Identyfikacja ryzyk jako podstawa do wdrażania odpowiednich metod i technik zarządzania, powinna brać pod uwagę występujące luki badawcze. Najważniejsze z nich to: niedostatek długoterminowych studiów empirycznych nad interakcjami wielu modeli AI (tzw. bias kumulacyjny) i manipulacją algorytmami oraz brak kompleksowych badań nad erozją zaufania klientów wskutek błędów modeli i nad samym zastosowaniem AI. Świadomość takich luk powinna wyczulić menadżerów na obserwację nietypowych, nieopisanych zjawisk zachodzących w środowisku nadzorowanej pracy.

Dobrym i stosunkowo prostym narzędziem wskazującym pilność podejmowania działań przez zarządzających jest mapa ryzyk. We wdrażaniu AI w bankowości detalicznej wizualizować można zagrożenia według dwóch wybranych osi, np.: prawdopodobieństwa wystąpienia (niskie–wysokie) i wpływu na operacje lub klientów (niski–wysoki), dzieląc je na strefy: zieloną (niska pilność działania), żółtą (średnia) i czerwoną (wysoka). Przykładowo cyberataki na modele AI z wyciekiem danych mają wysokie prawdopodobieństwo wystąpienia i wysoki wpływ na opinie klientów (strefa czerwona). Brak zgodności dokumentów i procedur z regulacjami ma średnie

prawdopodobieństwo wystąpienia i stosunkowo niski wpływ na klientów. Opóźnienia we wdrażaniu nowych systemów ma wysokie prawdopodobieństwo wystąpienia, ale niski lub średni wpływ na operacje i klientów (strefa żółta). Niskie prawdopodobieństwo i niski wpływ (strefa zielona) mogą mieć np. większe błędy w raportach wewnętrznych (łatwe do wykrycia na wielu etapach) i niedostosowanie starszych pracowników do specyfiki pracy z AI (możliwość szkoleń, przesunięcie na stanowiskach).

Zarządzanie ryzykiem we wdrażaniu i funkcjonowaniu AI

O ile w latach 2020–2023 wdrażanie systemów uczących się (ML) oraz generatywnej sztucznej inteligencji (GenAI) miało charakter punktowy i eksperymentalny, o tyle w dwu kolejnych latach algorytmy przestały pełnić jedynie funkcję narzędzi wspierających analitykę marketingową czy proste interakcje z klientem (chatboty). Stały się nieodłącznym elementem procesów decyzyjnych o wysokim ryzyku, przede wszystkim takich jak ocena zdolności kredytowej (*credit scoring*), detekcja nadużyć w czasie rzeczywistym (*anti-fraud*) oraz automatyzacja procesów przeciwdziałania praniu pieniędzy (AML). Regulacje prawne na poziomie Unii Europejskiej, jak Rozporządzenie o sztucznej inteligencji (EU AI Act), a w Polsce Rekomendacje H i W Komisji Nadzoru Finansowego (KNF), powodują, że skuteczne wdrożenie AI w bankowości detalicznej nie jest już wyzwaniem tylko technologicznym, lecz przede wszystkim zarządczym i prawnym.

Jako przykłady wdrażania AI do wykrywania przestępstw finansowych można podać bank HSBC, który w 2024 r. dzięki AI analizował ok. 900 milionów transakcji miesięcznie na 40 milionach kont klientów (Calvery, 2024). Przykładem wykrycia występowania ryzyk wdrażania AI w bankowości detalicznej jest stronniczość algorytmów wykazana przez badaczy z Lehigh University. Duże modele językowe (LLM) częściej odmawiały kredytów i nakładały wyższe oprocentowanie na wnioski od czarnoskórych klientów w porównaniu do identycznych profili białych klientów, szczególnie przy wyższym ryzyku (Bowen III i in., 2024).

Podczas gdy skuteczność predykcyjna modeli AI rośnie dzięki zastosowaniu głębokich sieci neuronowych, ich transparentność i wyjaśnialność dla organów nadzorczych maleje. W bankowości detalicznej, która z definicji opiera się na zaufaniu klienta masowego oraz ścisłej ochronie konsumenta, ta asymetria informacyjna staje się ryzykiem systemowym. Tradycyjne podejście do zarządzania ryzykiem modelu (*model risk management* – MRM), znane z Rekomendacji W Komisji Nadzoru Finansowego, okazuje się niewystarczające. Klasyczne MRM koncentrowało się na stabilności statystycznej modeli ekonometrycznych. Zarządzanie ryzykiem AI wymaga natomiast podejścia socjotechnicznego, uwzględniającego nie tylko poprawność matematyczną, ale także sprawiedliwość (*fairness*), wyjaśnialność (*explainability*) oraz odporność (*robustness*) na ataki (*adversarial attacks*), mające na celu

oszukiwanie modeli AI poprzez m.in. subtelnie (ale często złośliwie) modyfikowane dane wejściowe.

Fundamentem ładu korporacyjnego w bankowości, szczególnie w aspekcie AI, jest model Trzech Linii Obrony (*Three Lines of Defense* – 3LoD), który wywodzi się z tradycyjnej doktryny audytu i zarządzania ryzykiem operacyjnym (Schuett, 2025). Choć nieformalne struktury podziału odpowiedzialności istniały w bankowości od dekad, model ten został formalnie skodyfikowany i spopularyzowany przez Instytut Audytorów Wewnętrznych (The Institute of Internal Auditors – IIA)³. Model IIA z 2013 r. (przywoływany w literaturze naukowej z zakresu finansów, zarządzania i audytu jako fundamentalny model teoretyczny stosowany w praktyce gospodarczej) *The Three Lines of Defense in Effective Risk Management and Control* (The Institute of Internal Auditors, 2013) zawierał odpowiedź na kryzys finansowy z lat 2007–2008, który obnażył strukturalne słabości w nadzorze bankowym – sytuacje, w których „wszyscy odpowiadali za ryzyko, więc nikt za to nie odpowiadał”. Model został szybko zaadaptowany przez Bazylejski Komitet Nadzoru Bankowego (Basel Committee on Banking Supervision – BCBS) jako globalny standard zarządzania ryzykiem operacyjnym. W klasycznym ujęciu model ten zakłada hierarchiczną separację funkcji:

- I linia (poziom operacyjny): zarządzający ryzykiem na co dzień w toku działalności operacyjnej dostarczają produktu/usługi, bezpośrednio zarządzając ryzykiem;
- II linia (ryzyko, zgodność, kontrola finansowa): wyznacza ramy, polityki i narzędzia do monitorowania ryzyka oraz rzuca wyzwanie I linii (testowanie pod kątem wybranych wskaźników⁴), raportuje zbiorcze ryzyko do zarządu;
- III linia (audyt wewnętrzny): zapewnia niezależną, obiektywną ocenę skuteczności działania dwóch pierwszych linii, raportując bezpośrednio do Rady Nadzorczej.

W literaturze przedmiotu (Tammenga, 2020) podkreśla się ryzyko „audytu fasadowego”. Występuje ono wtedy, gdy audytorzy sprawdzają jedynie istnienie dokumentacji („czy istnieje dokument opisujący model?”), a nie weryfikują faktycznej skuteczności modelu. W dobie AI III linia musi ewoluować w stronę tzw. audytu algorytmicznego. Polega on na tym, że audytorzy III linii muszą być w stanie niezależnie pobrać próbkę danych i przetestować model (*re-performance*). Następnie powinni zweryfikować, czy człowiek w pętli decyzyjnej (*human-in-the-loop*) faktycznie

³ W 2020 r. Instytut Audytorów Wewnętrznych opublikował zaktualizowaną wersję tego modelu pod nową nazwą, w której pominięto człon „obrony”: *The IIA's three lines model: An update of the three lines of defense*. (The Institute of Internal Auditors, 2020). Nowe podejście zamiast sztywnej obrony kładzie większy nacisk na:

- współpracę i komunikację między liniami zamiast tworzenia izolowanych „silosów”,
- wsparcie realizacji celów, a nie tylko ochronę przed stratami,
- wykorzystanie technologii, w tym AI i automatyzacji, do ciągłego monitorowania ryzyk w czasie rzeczywistym.

⁴ II linia odpowiada również za interpretację regulacji (np. EU AI Act) i przełożenie ich na konkretne metryki techniczne, które I linia musi spełnić (np. wskaźnik *fairness* na poziomie minimum 80%).

nadzoruje AI, czy tylko bezrefleksyjnie zatwierdza jego decyzje (zjawisko *automation bias*). Docelowo powinni ocenić kulturę ryzyka w organizacji: czy presja na wynik biznesowy (I linia) nie prowadzi do ignorowania ostrzeżeń generowanych przez systemy monitorujące. Inne wyzwanie, dotyczące głównie II linii, polega na luce kompetencyjnej. Tradycyjni pracownicy (głównie prawnicy) sprawdzający zgodność z przepisami (*compliance*) często nie posiadają wiedzy technicznej, by ocenić ryzyko związane z parametrami sieci neuronowej. Dlatego w nowoczesnym modelu 3LoD, II linia musi zostać wyposażona w kompetencje techniczne. Wskazane jest zatem zatrudnianie lub/i przesuwanie do zespołu „walidatorów technicznych” – najlepiej pracowników posiadających kompetencje w zakresie analityki danych (*data scientists*).

Opisany powyżej model Trzech Linii przeszedł drogę od koncepcji teoretycznej do standardu praktyki zawodowej. KNF w swoich rekomendacjach – przede wszystkim w H (system kontroli wewnętrznej), ale pośrednio i w innych: D (testy i odporność), M (automatyzacja ryzyka), W (walidacja i monitoring) – wprost wymaga od banków posiadania struktury opartej na Trzech Liniach. Komitet Bazylejski włączył ten model do globalnych wytycznych nadzorczych dla sektora bankowego, co uczyniło go standardem globalnym. W najbliższych latach najważniejszymi dokumentami w zakresie zarządzania ryzykiem i bezpieczeństwem w bankach staną się standard ISO/IEC No. 42001:2023 (International Organization for Standardization, 2023) oraz Artificial Intelligence Risk Management Framework (National Institute of Standards and Technology, 2023).

Pierwszy dokument został opublikowany 18 grudnia 2023 r. jako norma międzynarodowa i jest rodzajem warstwy dla tworzenia polityk zarządczych i wyznaczania odpowiedzialnych za ryzyka – ustanawia komitety sterujące i zarządza przeprowadzanie audytów wewnętrznych (odpowiednik linii II i III w modelu Trzech Linii). Drugi standard (styczeń 2023) jest dokumentem rządowym ze Stanów Zjednoczonych, skąd pochodzą najważniejsze i największe systemy AI, nie ma więc w Europie i w Polsce znaczenia obowiązującego, ale stanowi rodzaj podręcznika dla projektantów systemów i informatyków dostarczających rozwiązania AI w bankowości (odpowiednik linii I w modelu Trzech Linii).

Norma ISO 42001 nie skupia się wyłącznie na inżynierii modelu ML, lecz na całościowym systemie zarządzania organizacją (AIMS – Artificial Intelligence Management System). Oznacza to przesunięcie punktu ciężkości z poprawności kodu na odpowiedzialność organizacyjną, co dobrze wpisuje się w wymogi EU AI Act oraz oczekiwania organów nadzoru finansowego (w Polsce KNF). Norma składa się z 10 klauzul głównych (obligatoryjnych) oraz czterech załączników o charakterze normatywnym i informacyjnym. Przykładowo klauzula 4 wymusza m.in. identyfikację interesariuszy: klientów (obawiających się dyskryminacji), regulatora oraz dostawców technologii. Klauzula 6 wymaga przeprowadzenia oceny ryzyka AI (*AI risk assessment*) w kontekście niezamierzonego wyniku działania modelu

(np. halucynacji GenAI) lub szkody społecznej (np. wykluczenia finansowego). Klauzula 7 wymusza szkolenia nie tylko dla inżynierów, ale także dla personelu odpowiedzialnego za kontakt z klientem (np. doradców klienta korzystających z rekomendacji AI), aby uniknąć zjawiska bezkrytycznego ufania maszynie. Odpowiada to w pewnym stopniu drugiej linii obrony w modelu Trzech Linii. Klauzula 8 nakłada rygorystyczne wymogi co do kontroli dostawców zewnętrznych, za których błędy bank (instytucja kupująca usługę) odpowiada jak za błędy własne. Klauzula 9 wprowadza wymóg ciągłego monitorowania modelu AI pod kątem jego „zdrowia” (np. *data drift*, spadek dokładności) i raportowania wyniku do zarządu (II linia obrony). Audyt wewnętrzny (III linia obrony) musi okresowo weryfikować zgodność systemu z normą i raportować do organu wyższego (np. rady nadzorczej). Załączniki zawierają listę celów stosowania zabezpieczeń, określają konieczność sformalizowania zasad etycznych – nie tylko deklaratywnie, ale także w postaci procedury operacyjnej. Określają kontrolę projektowania (np. czy system ma prawo odmówić kredytu samodzielnie?), cyklu życia, weryfikacji i walidacji (tzw. V&V) – testów przed zatwierdzeniem i wdrożeniem modelu do działania (II linia). Kolejne załączniki określają kontrolę danych dla modeli AI (wymagają sprawdzenia, czy dane treningowe nie zawierają historycznych uprzedzeń), wprowadzenia procedur transparentności i wyjaśnialności decyzji dla klientów. Podsumowując, norma ta stanowi pomost między wizją technologii (inżynierów ML), a światem regulacji (prawników) i wdrażania (zarządu, nadzoru), jej wdrożenie jest dowodem dojrzałości cyfrowej organizacji. W erze mediów cyfrowych, gdy klienci boją się dehumanizacji bankowości, znak jakości ISO 42001 pełnić może także funkcję marketingową. Jest komunikatem, że algorytmy banku są bezpieczne, audytowane i pod kontrolą. W relacjach B2B certyfikat może być warunkiem koniecznym współpracy.

Drugi wspomniany dokument powstał w 2023 r. w Narodowym Instytucie Standaryzacji i Technologii (NIST) przy Departamencie Handlu USA. Formalnie jest to standard dobrowolny może on jednak pełnić rolę „miękkiego prawa” w sektorze finansowym, stanowiąc merytoryczne dopełnienie dla „twardych” regulacji takich jak EU AI Act czy norma ISO/IEC 42001. Ogólna idea tego dokumentu (podobnie jak wspomnianych wcześniej regulacji i norm) wskazuje na odejście od traktowania systemu AI jako czysto matematycznego modelu (kodu), na rzecz analizy jego interakcji z otoczeniem społecznym. W bankowości oznacza to, że błąd algorytmu nie jest mierzony tylko stratą finansową banku, ale także szkodą wyrządzoną klientowi (*harm to individuals*), grupie społecznej (*harm to groups*) lub rynkowi (*harm to society*). Struktura tego dokumentu opiera się na czterech wzajemnie przenikających się funkcjach:

1. Zarządzaj strategicznie (*govern*) – w ramach tej funkcji wyższe kierownictwo instytucji finansowej ustala apetyt na ryzyko, buduje kulturę organizacyjną promującą bezpieczeństwo oraz zapewnia zasoby niezbędne do skutecznego nadzoru.

To tutaj tworzone powinny być polityki określające, jakie systemy AI są dopuszczalne do wdrożenia, a jakie naruszają standardy etyczne banku. Kluczowym zadaniem funkcji *govern* jest również ustanowienie jasnych struktur odpowiedzialności, eliminujących zjawisko rozmycia winy w przypadku błędów algorytmicznych, oraz integracja zarządzania ryzykiem AI z istniejącymi systemami prawnymi i cyberbezpieczeństwa.

2. Mapuj (*map*) – funkcja ta polega na systematycznym wykrywaniu zależności, ograniczeń technologii oraz założeń przyjętych na etapie projektowania, które w rzeczywistym świecie mogą okazać się błędne. Kluczowym aspektem jest tu analiza całego cyklu życia systemu – od doboru danych treningowych, przez wdrożenie, aż po wycofanie z eksploatacji – w celu przewidzenia potencjalnych negatywnych skutków, zanim one wystąpią.
 3. Mierz (*measure*) – funkcja polega na zastosowaniu metod ilościowych i jakościowych do oceny zidentyfikowanych wcześniej ryzyk, z wykorzystaniem rygorystycznych testów i audytów technicznych. W ramach tej funkcji organizacja wdraża konkretne metryki do oceny takich parametrów jak sprawiedliwość algorytmiczna (*fairness*), wyjaśnialność decyzji czy odporność na ataki, i monitoruje zachowanie modelu w warunkach kontrolowanych oraz produkcyjnych. Pomiar ten nie może być tylko jednorazowym aktem, lecz ciągłym procesem, który ma na celu wykrycie degradacji jakości modelu lub pojawienia się nowych zagrożeń w czasie.
 4. Zarządzaj operacyjnie (*manage*) – funkcja ta obejmuje wdrażanie technicznych i organizacyjnych mechanizmów kontrolnych, takich jak korekta algorytmów, czyszczenie danych czy wprowadzenie nadzoru ludzkiego nad decyzjami maszyny. W sytuacjach gdy ryzyka nie da się skutecznie ograniczyć, faza ta legitymizuje decyzję o rezygnacji z wdrożenia systemu lub jego wyłączeniu. Zarządzanie operacyjne obejmuje również ciągły monitoring powdrożeniowy, reagowanie na incydenty oraz komunikację z interesariuszami na temat zidentyfikowanych zagrożeń. W odniesieniu do powyższych funkcji NIST zdefiniował siedem cech jakości systemów AI:
1. Poprawny i niezawodny (*valid & reliable*): system działa zgodnie z założeniami nie tylko w laboratorium, ale na rzeczywistych danych produkcyjnych, które są często zaszumione.
 2. Bezpieczny (*safe*): system nie stwarza zagrożenia dla życia, zdrowia ani mienia. W bankowości oznacza to np. stabilność systemu transakcyjnego sterowanego AI.
 3. Zabezpieczony i odporny (*secure & resilient*): odporność na ataki typu zatrucie danych treningowych (*data poisoning*) czy kradzież własności intelektualnej modelu (*model extraction*).
 4. Rozliczalny i przejrzysty (*accountable & transparent*): możliwość odtworzenia ścieżki decyzyjnej. Kto, kiedy i dlaczego zatwierdził daną wersję modelu?

5. Wyjaśnialny i interpretowalny (*explainable & interpretable*): możliwość zrozumienia decyzji przez człowieka. Jest to wymóg prawny (RODO) w przypadku decyzji automatycznych.
6. Chroniący prywatność (*privacy-enhanced*): wykorzystuje takie narzędzia i techniki, które trenują modele bez ujawniania wrażliwych danych klientów.
7. Sprawiedliwy (*fair with harmful bias managed*): aktywnie zarządza uprzedzeniami historycznymi i społecznymi zawartymi w danych.

Warto podkreślić, że NIST traktuje te cechy jako wzajemnie powiązane, choć czasem pozostające w konflikcie. W praktyce zarządzania bezpieczeństwem wdrażania i funkcjonowania AI w bankowości detalicznej oba opisane dokumenty pełnią już ważną rolę i będą miały coraz większe znaczenie. Dokument NIST dostarcza precyzyjnego języka, taksonomii ryzyk oraz konkretnych metryk do pomiaru sprawiedliwości czy odporności algorytmów. Jest on swoistą „instrukcją obsługi” regulacji, pozwalającą przetłumaczyć abstrakcyjne pojęcia prawne na procedury testowe. Z kolei ISO 42001 uzupełnia ten obraz o warstwę zarządczą, oferując strukturę pozwalającą na integrację nadzoru nad AI z istniejącymi procesami korporacyjnymi, co czyni bezpieczeństwo procesem audytowalnym i zrozumiałym dla zarządów.

Polska, jako członek Unii Europejskiej, podlegać będzie przepisom EU AI Act od 2 sierpnia 2026 r. Zarządzający bankami powinni więc przygotować się z wyprzedzeniem (stworzyć formalne struktury zarządzania AI i wyszkolić pracowników), zamiast czekać na sankcje regulacyjne. Inwestycja w szeroko pojęte bezpieczeństwo AI na etapie wdrażania jest znacznie tańsza niż retrospektywne naprawy po incydentach lub sankcjach nadzorczych. Kluczowe jest powołanie zespołów i określenie ich kompetencji i odpowiedzialności, np. wg opisanego powyżej modelu Trzech Linii. Upraszczając, powinny to być co najmniej trzy zespoły:

1. nadzoru nad AI, który zdefiniuje zasady bezpieczeństwa, skoordynuje procesy zarządzania i rozwoju wszystkich systemów, zapewni zgodność z celami biznesowymi i przepisami prawa, zintegruje z politykę wykorzystania AI z innymi systemami banku;
2. testerów systemów AI, odpowiadający za każdy system AI w jego całym cyklu życia – od planowania do wycofania; zespół ten powinien odpowiadać za specyfikację przypadków użycia, ocenę ryzyka, dokumentowanie parametrów, monitoring wydajności, a także kontrolę jakości każdego wdrożonego modelu;
3. inżynierów poszczególnych systemów, odpowiedzialny bezpośrednio za każdy algorytm (zarówno wewnętrznie rozwinięty, jak i pozyskany od zewnętrznych dostawców); zespół ponosi odpowiedzialność za ciągły monitoring behawioralny algorytmu, jego bieżącą konfigurację, testowanie, weryfikację.

Role te powinny być formalnie zdefiniowane w strukturze organizacyjnej oraz wpisane w systemy odpowiedzialności i motywacji pracowników.

Najmniej rozpoznane w literaturze przedmiotu i w zasadzie niezbadane na większych i różnorodnych grupach pozostaje opisane wcześniej ryzyko kadrowe i luka kompetencyjna (Kowalik i in., 2025; Bell i in., 2025). W tym obszarze banki powinny:

- prowadzić systematyczną diagnostykę i szkolenia rozwijające kompetencje pracowników w obszarach wykorzystujących AI,
- przedefiniować role pracowników – z bezkrytycznych operatorów systemów na nadzorców i interpretatorów AI,
- utrzymywać i okresowo ćwiczyć „manualne” procedury, aby w razie awarii AI lub cyberataku organizacja nie utraciła zdolności operacyjnych,
- budować ścieżki kariery i systemu premiowego dla ról związanych z AI.

Podobnie słabo zbadany pozostaje obszar reakcji klientów banków na coraz szersze wdrażanie systemów AI. Banki w tym zakresie powinny (Bharti i in., 2023; Naveen i in., 2026):

- przeprowadzać reprezentatywne badania ankietowe na klientach ($n > 500$), mierząc postawy wobec AI w różnych obszarach ich styku z technologią,
- przeprowadzać wywiady pogłębione ($n = 20$ do 30) z klientami ze zróżnicowanych segmentów (młodzi, starsi, częściowo/całkowicie wykluczeni itd.), identyfikujące obawy wobec AI w sposób jakościowy,
- prowadzić badania w obszarze *user experience* (np. *eyetracking*, analiza map ciepła, testy A/B),
- wdrażać pilotażowe wersje usług AI (chatboty, robodoradcy) dla podgrup klientów,
- mierzyć behawioralne wskaźniki po kontakcie z AI: np. satysfakcji, lojalności, rezygnacji (*churn*),
- analizować dane behawioralne: np. czas sesji, liczba sesji porzuconych, konwersja zapytań na transakcje,
- segmentować klientów, np. wg demografii, częstotliwości korzystania, zaufania do technologii.

Wymienione powyżej badania i wnioski z nich płynące tradycyjnie pozostają w gestii szeroko pojętych działów/komórek marketingu. W obszarze AI powinny jednak być konsultowane z omówionymi wcześniej strukturami odpowiedzialnymi za bezpieczeństwo i wdrażanie systemów AI.

Podsumowanie

Coraz szersze wykorzystanie sztucznej inteligencji we wszystkich obszarach naszego życia sprawia, że w bankowości detalicznej nie wystarczy tylko adaptować nowe narzędzia, aby nadążyć za konkurencją. Konieczne jest wprowadzenie dużych zmian organizacyjnych. Działania te mogą opierać się na gotowych ramach z aktów prawnych, wytycznych branżowych i literatury naukowej – ale sukces wymagać będzie

także własnej inicjatywy w adaptacji do specyfiki lokalnego rynku. Opisane tu i w innych publikacjach naukowych i branżowych rozwiązania zapewnić mogą fundament, ale banki muszą dostosować swoje działania do własnej specyfiki: posiadanych zasobów, zbadanych luk (np. kompetencyjnych) i lokalnego rynku (klientów). Twórcze rozwiązania powinny powstać w ramach interdyscyplinarnych zespołów skupiających naukowców i informatyków analizujących duże zbiory danych (*data scientists*), prawników, psychologów behawioralnych, marketingowców i managerów specjalizujących się w strukturach bankowych. Wydaje się, że oprócz konkurencji o klienta (co można na pewnym etapie pozostawić działom marketingu) banki mogłyby też współpracować na poziomie stworzenia specyficznych standardów, np. w formie międzybankowego konsorcjum (z KNF, ZBP), np. do walidacji modeli AI na polskich danych. Taka inicjatywa może być pomostem pomiędzy regulacjami skupiającymi się na zgodności, wytycznymi branżowymi skupiającymi się na obsłudze technologii i pracami naukowymi operującymi na teorii. Banki potrzebują praktycznych narzędzi z danymi lokalnymi. Koszty badań i wdrożeń powinny zwrócić się przez uniknięcie kar i wzrost zaufania klientów (Bharti i in., 2023). Kluczowym zadaniem dla zarządzających ryzykiem we wdrażaniu AI jest integracja wszystkich wymiarów i obszarów przedstawionych w artykule oraz zastosowanie branżowych standardów zarządzania. Menadżerowie muszą bezustannie śledzić nowe technologie, pojawiające się standardy, analizować bieżące przypadki zagrożeń w swojej pracy, tak aby szybko – samodzielnie, w zespołach lub raportując do specjalistów i wyższych szczebli zarządzania – wypełniać luki badawcze między teorią a praktyką.

Bibliografia

- Akinrele, O. (2025). Bias mitigation in AI-driven banking: Legal, ethical, and regulatory perspectives. *International Journal of Science and Research Archive*, 17(2), 373–379. <https://doi.org/10.30574/ijrsra.2025.17.2.3013>
- Baesens, B., Roesch, D., Scheule, H. (2016). *Credit risk analytics: Measurement techniques, applications, and examples in SAS*. John Wiley & Sons.
- Bell, S., Gadanecz, B., Gambacorta, L., Perez-Cruz, F., & Shreeti, V. (2025, 24 kwietnia). Artificial intelligence and human capital: Challenges for central banks, *BIS Bulletin*, 100. <https://www.bis.org/publications/bulletin-100-artificial-intelligence-and-human-capital-challenges-central-banks.pdf>
- Bharti, S. S., Prasad, K., Sudha, S., & Kumari, V. (2023). Customer acceptability towards AI-enabled digital banking: A PLS-SEM approach. *Journal of Financial Services Marketing*, 28(4), 779–793. <https://doi.org/10.1057/s41264-023-00241-9>
- Bowen III, D. E., McKay Price, S., Stein, L. C. D., Yang, K. (2024, 3 czerwca). Measuring and mitigating racial disparities in LLMs: Evidence from a mortgage underwriting experiment. SSRN. <http://dx.doi.org/10.2139/ssrn.4812158>
- Calvery, J. (2024, 10 czerwca). *Harnessing the power of AI to fight financial crime*. HSBC. <https://www.hsbc.com/news-and-views/views/hsbc-views/harnessing-the-power-of-ai-to-fight-financial-crime>

- Centrum Procesów Bankowych i Informatyki. (2024). *Era AI: jak sztuczna inteligencja zmienia bankowość?* Wydawnictwo Centrum Procesów Bankowych i Informatyki. https://bank.pl/wp-content/uploads/2024/12/Raport_ERA_AI.pdf
- Citron D. K., Pasquale F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89(1), 1–34.
- Edwards, L., Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. *Duke Law & Technology Review*, 16(1), 18–84. <https://scholarship.law.duke.edu/dltr/vol16/iss1/2>
- Financial Stability Board (2024, 14 listopada). *The financial stability implications of artificial intelligence*. <https://www.fsb.org/uploads/P14112024.pdf>
- Fredrikson, M., Jha, S., Ristenpart, T. (2015, 12–16 października). Model inversion attacks that exploit confidence information and basic countermeasures. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1322–1333). <https://doi.org/10.1145/2810103.2813677>
- International Organization for Standardization. (2023). *Information technology — Artificial intelligence — Management system* (ISO/IEC Standard No. 42001:2023). <https://www.iso.org/standard/81230.html>
- Häuselmann, A. N. (2024, 23 kwietnia). *EU privacy and data protection law applied to AI: unveiling the legal problems for individuals* [Doctoral thesis, Leiden University]. <https://scholarlypublications.universiteitleiden.nl/handle/1887/3747996>
- Kowalik, Z., Lewandowski, P., Geodecki, T., & Grodzicki, M. (2025). Automation in shared services centres: Implications for skills and autonomy. *The Economic and Labour Relations Review*, 36(2), 563–581. <https://doi.org/10.1017/elr.2025.10026>
- Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165(3), 633–705.
- Lee, J. D., See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 46(1), 50–80. https://doi.org/10.1518/hfes.46.1.50_30392
- Mäntymäki, M., Minkinen, M., Birkstedt, T., Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, 2, 603–609. <https://doi.org/10.1007/s43681-022-00143-x>
- McLemore, P., Mihov, A. (2026). AI and operational losses: Evidence from U.S. Bank Holding Companies. *The Review of Corporate Finance Studies*, artykuł cfag003. <https://doi.org/10.1093/rcfs/cfag003>
- Nagarakanti, R. C. (2025). Human-AI collaboration in financial services: Augmenting decision-making with cloud-native intelligence. *European Journal of Computer Science and Information Technology*, 13(22), 23–41. <https://doi.org/10.37745/ejcsit.2013/vol13n222341>
- National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. <https://doi.org/10.6028/NIST.AI.100-1>
- Naveen, K. R., Janani, M., Pavithra, R. (2026). Assessing the influence of AI adoption and trust on customer satisfaction in digital banking services. *SAM Advanced Management Journal*, 91(2), 165–183. <https://doi.org/10.1108/SAMAMJ-12-2024-0100>
- Nimmagadda, V. S. P. (2022). Artificial Intelligence for automated loan underwriting in banking: Advanced models, techniques, and real-world applications. *Journal of Artificial Intelligence Research and Applications*, 2(1). <https://aimlstudies.co.uk/index.php/jaira/article/view/204>
- Noriega, J. P., Rivera, L. A., Herrera, J. A. (2023). Machine learning for credit risk prediction: A systematic literature review. *Data*, 8(11), artykuł 169. <https://doi.org/10.3390/data8110169>

- Pramudito, D., Na'am, J., Ernawan, F. (2025). Exploring blockchain and AI in digital banking: A literature review on transactions enhancement, fraud detection, and financial inclusion. *Sistemasi: Jurnal Sistem Informasi*, 14(3), 1448–1459. <https://doi.org/10.32520/stmsi.v14i3.5231>
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji). *Dziennik Urzędowy Unii Europejskiej*, Dz.U. L 2024/1689. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1689>
- Sachan, S., Yang, J. B., Xu, D. L., Benavides, D. E., Li, Y. (2020). An explainable AI decision-support-system to automate loan underwriting. *Expert Systems with Applications*, 144, artykuł 113100. <https://doi.org/10.1016/j.eswa.2019.113100>
- Schuett, J. (2025). Three lines of defense against risks from AI. *AI & Society*, 40, 493–507. <https://doi.org/10.1007/s00146-023-01811-0>
- Shi, S., Tse, R., Luo, W., D'Addona, S., Pau, G. (2022). Machine learning-driven credit risk: a systemic review. *Neural Computing and Applications*, 34(17), 14327–14339. <http://doi.org/10.1007/s00521-022-07472-2>
- Szostek, D., Bar, G., Prabucki, T., Nowakowski, M. (2022, sierpień). *Zastosowanie sztucznej inteligencji w bankowości – szanse oraz zagrożenia. Analiza prawnoregulacyjna wpływu technologii uczenia maszynowego i pokrewnych na obowiązki sektora bankowego z zakresu zapewnienia zgodności (compliance) oraz zarządzania ryzykiem*. Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.
- Tammenga, A. (2020). The application of Artificial Intelligence in banks in the context of the three lines of defence model. *Maandblad voor Accountancy en Bedrijfseconomie*, 94(5/6), 219–230. <https://doi.org/10.5117/mab.94.47158>
- The Institute of Internal Auditors. (2013). The Three Lines Of Defense In Effective Risk Management And Control [Position paper]. <https://theiia.fi/wp-content/uploads/2017/01/pp-the-three-lines-of-defense-in-effective-risk-management-and-control.pdf>
- The Institute of Internal Auditors. (2020). *The IIA's Three Lines Model: An update of the Three Lines of Defense* [Position paper]. <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>
- Tshewang S. (2024, 6 kwietnia), Impact of artificial intelligence on job market in the banking sector: A focus on the Indian context. SSRN. <http://dx.doi.org/10.2139/ssrn.4786492>
- Uddin, N. (2025). Role of AI in preventing financial crime: A comprehensive analytical review. *Journal of Economic Criminology*, 13, artykuł 100200. <http://doi.org/10.1016/j.jeconc.2025.100200>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. <http://doi.org/10.2307/30036540>
- Wachter, S., Mittelstadt, B., Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <http://doi.org/10.1093/idpl/ix005>
- World Economic Forum. (2025). *Future of Jobs Report 2025*. <https://www.weforum.org/reports/the-future-of-jobs-report-2025>

Ziółkowska, E. (2023), Wpływ sztucznej inteligencji na rynek finansowy w procesie podejmowania decyzji ekonomicznych – szanse, wyzwania i rekomendacje, *Studia i Prace Kolegium Zarządzania i Finansów*, 192, 89–108. <https://doi.org/10.33119/SIP.2023.192.5>

Bezpieczeństwo i analiza ryzyka we wdrażaniu sztucznej inteligencji w bankowości detalicznej

Streszczenie

W artykule omówiono najważniejsze zastosowania sztucznej inteligencji w bankowości detalicznej, wskazano ryzyka we wdrażaniu i funkcjonowaniu AI. Zidentyfikowano luki pomiędzy teorią a praktyką oraz zaproponowano ramy koncepcyjne ich wypełnienia. W zakresie zarządzania ryzykiem przedstawiono model Trzech Linii, zestawiając go z normą ISO/IEC 42001:2023 oraz standardem opublikowanym przez Narodowy Instytut Standaryzacji i Technologii (NIST) przy Departamencie Handlu USA. Następnie zaproponowano, jak wybrane koncepcje teoretyczne, normy i zalecenia przełożyć na tworzenie i zarządzanie strukturami nadzorującymi funkcjonowanie AI w banku, tak aby były zgodne z wchodzącym w pełni w życie od sierpnia 2026 r. unijnym aktem w sprawie sztucznej inteligencji (EU AI Act). Wskazano też na przyszłe działania poprawiające bezpieczeństwo systemu branży bankowej. Innowacyjne rozwiązania mogą nie tylko służyć konkurencji poszczególnych banków, ale także w pewnym zakresie wspierać współpracę w dziedzinie szeroko pojętego bezpieczeństwa.

Słowa kluczowe: sztuczna inteligencja, bankowość detaliczna, zarządzanie ryzykiem, zarządzanie bezpieczeństwem

Security and risk analysis in the implementation of artificial intelligence in retail banking

Abstract

The article discusses the most important applications of artificial intelligence in retail banking, identifies risks in the implementation and operation of AI. It highlights gaps between theory and practice and proposes conceptual frameworks to address them. In the area of risk management, it examines the Three Lines model, juxtaposing it with the standard ISO/IEC 42001:2023 and the standard published by the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce. Then it proposes how selected theoretical concepts, standards, and recommendations can be translated into creating and managing structures overseeing the operation of AI in a bank, ensuring compliance with the EU AI Act, which comes fully into force in August 2026. It also points to future actions that improve the safety of the banking sector system. Innovative solutions can not only serve the competition of individual banks but also, to some extent, support cooperation in the broadly understood area of security.

Keywords: artificial intelligence, retail banking, risk management, security management

Wkład autorów / Author Contributions

Konceptualizacja / Conceptualization: D.F.

Metodologia / Methodology: D.F.

Analiza formalna / Formal analysis: D.F.

Badania / Investigation: D.F.

Zasoby / Resources: D.F.

Przygotowanie wersji wstępnej / Writing – original draft: D.F.

Recenzja i edycja / Writing – review & editing: D.F.

Materiały dodatkowe / Supplementary Materials

Nie dotyczy / Not applicable.

Finansowanie / Funding

Badania nie otrzymały żadnego zewnętrznego finansowania. / This research received no external funding.

Oświadczenie o zatwierdzeniu etycznym / Ethics Approval Statement

Nie dotyczy / Not applicable.

Oświadczenie o świadomej zgodzie / Informed Consent Statement

Nie dotyczy / Not applicable.

Oświadczenie o dostępności danych / Data Availability Statement

Udostępnianie danych nie ma zastosowania do tego artykułu, ponieważ w ramach badania nie wygenerowano ani nie analizowano żadnych nowych danych. / Data sharing is not applicable to this article as no new data were generated or analyzed in this study.

Oświadczenie o użyciu generatywnej sztucznej inteligencji / Declaration of Generative AI Use

Do przygotowania niniejszego artykułu nie wykorzystano narzędzi generatywnej sztucznej inteligencji. / No generative artificial intelligence tools were used in the preparation of this manuscript.

Podziękowania / Acknowledgments

Nie dotyczy / Not applicable.

Konflikt interesów / Conflict of Interest

Dariusz Fatuła deklaruje brak konfliktu interesów. / Dariusz Fatuła declares no conflict of interest.

Rola strategii we wzmacnianiu odporności jednostek samorządu terytorialnego

Paweł Ptaszek

dr

<https://orcid.org/0009-0003-6931-7110>

Wprowadzenie

Zmienność i stałość. Struktura systemu i jego ewolucja. Stagnacja i rozwój. Teza i antyteza. Te przeciwieństwa w sposób elementarny opisują podstawową cechę rzeczywistości, jaką jest sprzeczność działających sił. Każdy system z jednej strony musi wykazywać się stabilnością, posiadać strukturę zapewniającą homeostazę. Z drugiej strony rozwój i ewolucja niemożliwe są bez zmiany, bez naruszenia porządku rzeczy. Tak jest w przypadku sił natury, podobnie – w przypadku organizacji społecznych.

Szczególnym typem organizacji społecznej jest organizacja terytorialna w języku prawniczym określana jako jednostka samorządu terytorialnego (JST). Jednostki samorządu terytorialnego (gmina, powiat, województwo) to terytorialne wspólnoty mieszkańców posiadające osobowość prawną, własne zasoby (w tym majątek), wykonujące w imieniu własnym i na własną odpowiedzialność zadania publiczne określone ustawami.

Samorząd terytorialny w polskim modelu ustrojowym posiada znaczną autonomię i szeroki zakres kompetencji. Poza rolę regulacyjną posiada znaczące uprawnienia w zakresie kształtowania rozwoju lokalnego i regionalnego. Gwałtowne i nieciągłe zmiany cywilizacyjne, gospodarcze i kulturowe, w szczególności pandemia oraz wojna

na Ukrainie stawiają przed wspólnotami samorządowymi nowe wyzwania w postaci odporności organizacyjnej i związanej z nią presją czynników zewnętrznych. Coraz częściej w sferze realnej, w sferze praktyki zarządzania pojawia się zagadnienie odporności regionu wobec kryzysów gospodarczych, zdrowotnych czy militarnych. Przykładem dostrzeżenia wagi problemu jest Strategia Rozwoju Województwa Małopolskiego 2030, akcentująca odporność Małopolski na obecne i przyszłe kryzysy.

Celem artykułu jest opis oraz wyjaśnienie znaczenia strategii dla odporności organizacji terytorialnej jaką jest JST. Cel ogólny będzie osiągnięty za pomocą następujących celów szczegółowych:

1. Określenie czynników odporności organizacyjnej JST;
2. Wskazanie roli strategii w podnoszeniu odporności organizacyjnej JST;
3. Analiza powiązań pomiędzy odpornością organizacyjną a rozwojem organizacyjnym.

Odporność organizacyjna i antykruchłość

Zagadnienie odporności organizacyjnej na gruncie nauk o zarządzaniu przeżywa renesans za sprawą wyzwań związanych z szybkimi zmianami technologicznymi, pandemią COVID-19, a także wojną na Ukrainie i związanymi z nią perturbacjami gospodarczymi. Na gruncie literatury przedmiotu brak jest jednej powszechnie akceptowanej definicji odporności organizacyjnej. Przegląd literatury wskazuje jednak na wspólne, powtarzające się element koncepcji odporności organizacyjnej (Wildavsky, 1988; Weick, 1993; Weick i Sutcliffe, 2001; Hamel i Valikanges, 2003; Ponomarov i Holcomb, 2009; Perechuda 2010; British Standards Institution, 2014; International Organization for Standardization, 2017). Do nich z pewnością należy zaliczyć:

- zdolność przewidywania niekorzystnych zmian,
- zdolności absorpcji szoku (odporność operacyjną w obliczu wystąpienia negatywnych bodźców),
- adaptację systemu (modyfikację działania systemu pod wpływem bodźców),
- transformację systemu do nowego stanu równowagi (rozwój dzięki doświadczeniu kryzysu).

Rozwinięciem koncepcji odporności organizacyjnej jest koncepcja tzw. antykruchłości (Taleb, 2012). Istotą antykruchłości jest nie tylko zdolność systemu do powrotu do stanu poprzedniego, lecz rozwój jako wynik działania czynnika zagrażającego homeostazie. W tym ujęciu negatywny bodziec (kryzys, zagrożenie) stanowi czynnik rozwoju, długofalowo przynoszący korzyść organizacji w postaci adaptacji ewolucyjnej do wyzwań płynących z otoczenia. W ujęciu systemowym stresor jest więc przesłanką ewolucji systemu w kierunku pozytywnym – jest czynnikiem rozwoju. Sztuka zarządzania kryzysem polega więc na przekształceniu zagrożenia w szansę rozwoju.

Czynniki odporności organizacyjnej jednostki samorządu terytorialnego

By zidentyfikować czynniki odporności organizacyjnej należy wpierv dokonać kategoryzacji źródeł potencjalnych zagrożeń z punktu widzenia samorządu terytorialnego.

Tabela 1. Źródła zagrożeń

Naturalne	Wewnętrzne	Osuwiska, lokalne powodzie, gradobicia
	Zewnętrzne	Susze, upały, epidemie
Ekologiczne (antropogeniczne)		Zanieczyszczenie gleby, hałas, nielegalne składowiska odpadów, zanieczyszczenie powietrza i wody
Polityczne	Wewnętrzne	Destabilizacja wewnętrzna
	Zewnętrzne	Ingerencja, zmienność zasad polityki regionalnej, uznaniowość decyzji
Ekonomiczne	Wewnętrzne	Kryzys demograficzny, upadek branży gospodarki regionalnej
	Zewnętrzne	Gwałtowne obniżenie dochodów zewnętrznych

Źródło: opracowanie własne.

Przedstawione wyżej źródła zagrożeń zostały podzielone na cztery kluczowe kategorie: naturalne, ekologiczne (mające związek z wpływem systemu społecznego na środowisko naturalne), polityczne oraz ekonomiczne. Dodatkowo zagrożenia ekonomiczne, polityczne i naturalne zostały podzielone na wewnętrzne i zewnętrzne z punktu widzenia JST. Na podstawie wyżej zaproponowanej klasyfikacji zagrożeń można określić ich cechy. Tak więc zagrożenia dla odporności systemu organizacji terytorialnej mają charakter:

- nagły (zagrożenie występuje niespodziewanie);
- istotny z punktu widzenia trwania organizacji;
- nieprzewidywalny (trudno prognozować wpływ zagrożenia na system);
- dotyczą wielu sfer organizacji (znaczenie strategiczne).

Używając metafory Taleba, źródła zagrożeń mają charakter „czarnych łabędzi”. Po wystąpieniu wyżej wymienionego zagrożenia decydenci mają skłonność do racjonalizacji zarówno jego przewidywalności, jak i przebiegu. Z punktu widzenia zarządzania strategicznego, kryzysy są źródłem niepewności strategicznej i mogą w znacznej mierze wynikać ze zjawiska szeroko opisanego krótkowzroczności strategicznej (Człon, 2018).

Na podstawie zidentyfikowanych źródeł zagrożeń proponuje się wprowadzenie następujących kategorii czynników odporności organizacyjnej JST: przywództwo adaptacyjne, kapitał organizacyjny, redundancja zasobowa, adekwatność problemu do poziomu decyzji.

Tabela 2. Czynniki odporności organizacyjnej jednostek samorządu terytorialnego

Czynniki odporności	Opis	Wskaźniki
Przywództwo adaptacyjne	Orientacja strategiczna, skuteczna komunikacja, ocena ryzyka, planowanie scenariuszowe, strategia jako opcje, strategia ewolucyjna	1. Scenariusze strategiczne na wypadek zagrożeń 2. Estymacja czynników ryzyka w oparciu o badania fokusowe w organizacji 3. Gry symulacyjne
Kapitał organizacyjny	Otwartość na sygnały z otoczenia i z wewnątrz organizacji,	Syntetyczny wskaźnik kapitału organizacyjnego
Redundancja zasobowa	Rezerwy finansowe, materialne, kadrowe	1. Wskaźnik redundancji finansowej 2. Wskaźnik redundancji zasobów materialnych 3. Wskaźnik redundancji zasobów ludzkich
Adekwatność problemu do poziomu decyzji i wdrożenia	Krótkie ścieżki decyzyjne adekwatne do wagi rozwiązywanego problemu, dekoncentracja zadań	Indeks dekoncentracji i decentralizacji

Źródło: opracowanie własne.

Przywództwo adaptacyjne bierze swój początek w konstatacji, iż środowisko organizacyjne cechuje się zmiennością, niepewnością, złożonością oraz niejednoznacznością (tzw. VUCA). Powoduje to, iż dotychczasowe style przywództwa przestają być skuteczne. Odpowiedzią na te wyzwania jest posiadanie jasnej wizji rozwoju i zrozumienie jego uwarunkowań, jasności co do podejmowanych działań oraz możliwości wpływania na bieg zdarzeń, a także zwinność (elastyczność) w kierowaniu organizacjami. Przywództwo adaptacyjne z kolei powiązane jest z kapitałem organizacyjnym, który obejmuje modele decyzyjne, formalne i nieformalne struktury relacji oraz normy i wartości, jakimi kieruje się dana organizacja. Dwa wymienione wyżej czynniki wymagają występowania redundancji zasobowej, będącej zaprzeczeniem filozofii *lean management*. Koncepcja redundancji oznacza zachowywanie rezerw strategicznych. Redundancja staje się warunkiem niezbędnym przywództwa adaptacyjnego oraz kapitału organizacyjnego. Czwartym czynnikiem wzmocnienia odporności organizacyjnej jest adekwatność poziomu decyzyjnego względem problemu. Wymaga to budowy odpowiednio zdecentralizowanej struktury administracji, która pozwala na elastyczne i stosunkowo szybkie rozwiązywanie problemów.

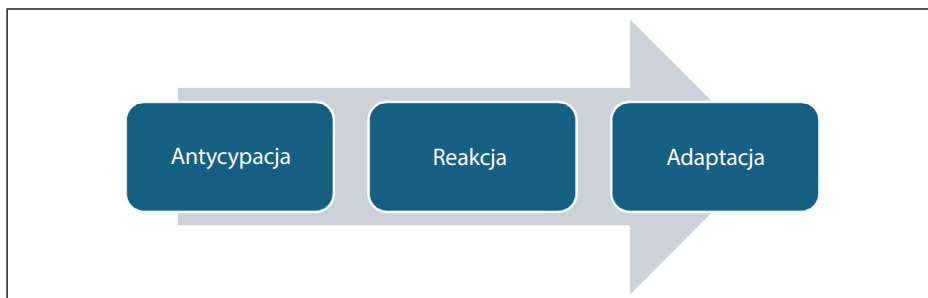
Na podstawie wymienionych wyżej czynników można postawić hipotezę, iż czynniki te współdziałają na rzecz zwiększenia odporności organizacyjnej. Analizując zagadnienie na poziomie koncepcyjnym: organizacja odporna będzie organizacją zwinną (*agile*). Dużym wyzwaniem natury praktycznej pozostaje operacjonalizacja pojęcia czynników odporności organizacji terytorialnej, która wymaga dalszych badań, zwłaszcza empirycznych.

Strategiczny wymiar odporności organizacyjnej

Na przestrzeni ostatnich kilkunastu lat w sferze teorii i praktyki zarządzania przywiązuje się dużą wagę do kwestii strategicznego zarządzania rozwojem lokalnym i regionalnym. Funkcje strategii w rozwoju społeczno-ekonomicznym zostały dosyć szeroko opisane na gruncie literatury przedmiotu (Kudłacz, 1999; Klasik, 2006; Winiarski, 2008; Strahl, 2010). Stosunkowo nowym wymiarem w zarządzaniu strategicznym jest postrzeganie strategii jako środka zapewniania odporności organizacyjnej. W tym kontekście można wyróżnić trzy zasadnicze funkcje strategii:

1. Strategia jako narzędzie antycypacji zagrożeń;
2. Strategia jako narzędzie reagowania na zagrożenia;
3. Strategia jako narzędzie adaptacji.

Rys. 1. Strategia jako narzędzie odporności organizacyjnej



Źródło: opracowanie własne.

By strategia rozwoju społeczno-gospodarczego JST mogła rzeczywiście pełnić wyżej opisane funkcje, powinna spełniać następujące warunki:

1. Strategia jest realnym narzędziem zarządzania, nie tylko dokumentem formalnie przyjętym;
2. Strategia przedstawia scenariusze (opcje);
3. Scenariusze (opcje) tworzą asymetrię w rozumieniu koncepcji antykruchości (ryzyko jest asymetryczne);
4. Opcje są formułowane w kategoriach kosztów alternatywnych;
5. Asymetria ryzyka w ramach opcji spełnia następujący warunek: straty są ograniczone i kontrolowalne, potencjalne zyski są znaczne (nieograniczone) i przewyższają straty.
6. Monitoring realizacji strategii jest oparty na mierzalnych, obiektywnych wskaźnikach realizacji.

Celem przetestowania spełniania warunków strategii jako środka do wzmacniania odporności proponuje się wykorzystać koncepcję strategii w ujęciu Mintzberga (Mintzberg i Quinn, 1996), w ramach której strategia postrzegana jest w pięciu wymiarach (tzw. 5P).

Tabela 3. Wymiary strategii

Wymiary strategii	Pytanie testujące
Strategia jako plan	Czy przewidziano scenariusze strategiczne, w szczególności scenariusze negatywne? Czy w organizacji występuje wiedza na temat potencjalnych zagrożeń? Czy organizacja posiada plan awaryjny? (związany z redundancją zasobów). Czy strategia formułuje zestaw realnych opcji odpowiadających zdiagnozowanym zagrożeniom?
Strategia jako wzór działania	Czy rutyny działania zapewnią ograniczenie skutków kryzysu? Czy organizacja posiada stopień decentralizacji/dekoncentracji zapewniający adekwatną reakcję? Jak istotna jest dźwignia operacyjna w przypadku kryzysu? (zastosowanie w sektorze publicznym do spółek komunalnych).
Strategia jako taktyka dla uzyskania przewagi konkurencyjnej	Czy kryzys wzmocni przewagę konkurencyjną JST? Czy organizacja wykorzysta kryzys jako szansę rozwoju?
Strategia jako pozycja	Jak kryzys wpłynie na pozycję JST w otoczeniu? Jak zmieniają się relacje z kluczowymi interesariuszami?
Strategia jako perspektywa	Czy kryzys jest okazją do zmian, reorganizacji i rozwoju?

Źródło: opracowanie własne.

W zaprezentowanej powyżej koncepcji weryfikacji strategii pod kątem odporności organizacji stawia się pytania otwarte, co pozwala na jakościową weryfikację. Propozycja ta nie wskazuje konkretnych działań organizacyjnych, lecz może stanowić ramy koncepcyjne dla praktyki zarządzania.

Z ewolucyjnym, emergentnym podejściem do kształtowania strategii odpornej na kryzysy związana jest koncepcja efektuacji (Sarasvathy, 2001). Koncepcja ta w istocie rzeczy stanowi zaprzeczenie dotychczas znanego i powszechnego modelu planowania i podejmowania decyzji opartego na jasno zdefiniowanym celu, przyczynowości, rozbudowanym procesie podejmowania decyzji oraz minimalizacji ryzyka. Strategia nie jest kierunkowym planem, lecz zestawem opcji, które organizacja wybiera w zależności od sytuacji. Pozwala to na elastyczne postępowanie w zależności od wspomianej dynamiki otoczenia (VUCA). Specyfika podejścia efektuacyjnego sprowadza się do pięciu zasad:

- zasada „wróbel w garści” polega na koncentracji na posiadanych, niepełnych i ograniczonych i częściowo niekontrolowanych zasobach i ich szybkim wykorzystaniu zamiast opracowywania rozbudowanych planów działania i czekania na pozyskanie wszystkich koniecznych zasobów do realizacji celu;
- zasada dopuszczalnej straty oznacza koncentrowanie się na dopuszczalnej maksymalnej stracie – zamiast na maksymalizacji zysku;

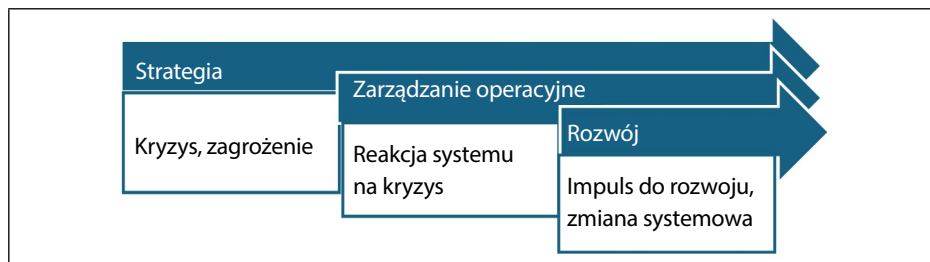
- zasada szalonego patchworku (*crazy quilt*) oznacza wykorzystywanie synergii w sieciach współpracy – zamiast podejścia konkurencyjnego;
- zasada „lemoniady” oznacza znaną heurystykę sprowadzającą się do: „graj tymi kartami, które masz, lepszych może nie być”; nieprzewidziane szanse mają być wykorzystywane do tworzenia możliwości;
- zasada „pilota w samolocie” koncentruje się na dwóch aspektach: kontroli czynników, które rozumiemy i nad którymi panujemy, zamiast przewidywania przyszłości oraz tworzenia trendów; tworzenia sposobności zamiast podążania za już istniejącymi, co obniża zależność od zmienności otoczenia, której nie kontrolujemy.

Koncepcja efektuacji pierwotnie odnosiła się do przedsiębiorczości i jej zastosowanie ma ograniczenia wynikające z specyfiki sektora publicznego, którego częścią jest samorząd terytorialny. Tym niemniej mając na uwadze raptowne i nieciągłe zmiany otoczenia, tworzące nowe nieznane wcześniej wyzwania, zasadna wydaje się adaptacja tej koncepcji do formułowania strategii, zwłaszcza w kontekście odporności organizacyjnej. Pierwszą przesłanką do przyjęcia takiego stanowiska jest fakt, iż sektor prywatny (przedsiębiorcy) i publiczny zmagają się z podobnymi wyzwaniami. Drugą przesłanką jest generalnie akceptowane stanowisko, iż metody i koncepcje zarządzania są stosowalne zarówno w odniesieniu do sektora publicznego, jak i prywatnego, czego wyrazem jest koncepcja Nowego Zarządzania Publicznego. Trzecią przesłanką jest konwergencja sektora publicznego i prywatnego i zacieranie się wyraźnych granic pomiędzy nimi, co w konsekwencji prowadzi do unifikacji stosowanych metod i technik zarządzania

Rozwój organizacji terytorialnej jako skutek odporności

Rozwój organizacji terytorialnej utożsamia się z rozwojem lokalnym i regionalnym, a przede wszystkim należy go odróżnić od rozwoju organizacji, jaką jest urząd i inne jednostki. W bogatej literaturze przedmiotu z zakresu ekonomii rozwoju brak jest jednej szeroko uznawanej koncepcji rozwoju lokalnego i regionalnego (Grosse, 2002; Szajnowska-Wysocka i Sitek, 2015). Tym niemniej proponuje się na rozwój spojrzeć z perspektywy reakcji systemu społeczno-gospodarczego (gminy, regionu) na wystąpienie sytuacji kryzysowej. Rysunek 2 prezentuje schemat reakcji systemu społeczno-gospodarczego na kryzys. W ujęciu systemowym stresor, jakim jest kryzys, powoduje reakcję organizacji, która z kolei stanowi czynnik rozwoju. Rolą strategii jest antycypowanie zmiany oraz jej wykorzystanie na poziomie operacyjnym. Efektem jest impuls rozwojowy, nowy kierunek rozwoju.

Rysunek 2. Reakcja systemu społeczno-gospodarczego na kryzys



Źródło: opracowanie własne.

Przedstawiona koncepcja zbliżona jest do koncepcji antykruchości systemu opisanej w pracy Taleba (2012). Istotą antykruchości jest asymetria w relacji korzyści i potencjalnego ryzyka. System antykruchy to system, w którym kryzysy są czynnikiem rozwoju. Sytuacja taka możliwa jest dzięki strategii posiadającej następujące cechy:

- redundancję (rezerwy zasobowe),
- opcjonalność (możliwość wyboru pomiędzy wariantami w sytuacji decyzyjnej, gdzie występuję duży potencjał korzyści przy minimalnych i przewidywalnych stratach),
- odpowiedzialność zarządzających za decyzje,
- stopień decentralizacji i dekoncentracji adekwatny do zapewnienia efektywności ekonomicznej,
- transformowalność strategii w działania operacyjne (strategia jako wzorzec działania, ramy koncepcyjne).

Odporność organizacyjna w ujęciu strategicznym na przykładzie Małopolski

Kluczowym instrumentem zarządzania strategicznego w regionie jest strategia rozwoju. Obecna Strategia Rozwoju Województwa „Małopolska 2030” została przyjęta w grudniu 2020 roku, z horyzontem czasowym do roku 2030. Zagadnienie odporności organizacyjnej nie jest traktowane w niej w sposób autonomiczny, lecz kwestie związane z odpornością strategiczną wpisane są kompleksowo w cele, priorytety i zadania. W części diagnostycznej Strategii, w analizie SWOT w kategorii „zagrożenia” wymienione są liczne źródła zagrożeń. Do zagrożeń zaliczono m.in.: skutki pandemii, brak stabilności finansowej z uwagi na kryzys demograficzny, ekstremalne zjawiska atmosferyczne. W porównaniu z zidentyfikowanymi źródłami zagrożeń (tabela 1) należy stwierdzić, iż zagrożenia mogące być źródłem kryzysu strategicznego zostały potraktowane w sposób dosyć ogólnikowy. Z kolei wyodrębnione w Strategii obszary

stanowiące główne kierunki rozwoju (klimat i środowisko, Małopolskie, gospodarka, rozwój zrównoważony terytorialne oraz strategiczne zarządzanie rozwojem) wprost nie odnoszą się do zagadnienia odporności organizacyjnej. Można jedynie przyjąć, iż obszary te traktowane komplementarnie na zasadzie efektu synergii mają przyczyniać się do wzmocnienia odporności organizacyjnej.

W styczniu 2026 przyjęta została Regionalna Strategia Adaptacji, będąca planem działania na rzecz wzmocnienia odporności na skutki zmian klimatycznych. Głównym celem Strategii jest przygotowanie regionu do gwałtownych zmian klimatycznych, w szczególności susz, powodzi czy wichur.

Przykładem działań samorządowych związanych z reakcją na kryzys wywołany pandemią COVID-19 jest Małopolska Tarcza Antykryzysowa. Działania podejmowane w ramach Tarczy wskazują na aktywną, interwencyjną politykę regionalną skierowaną na wsparcie kluczowych sektorów z punktu widzenia regionu. Małopolska Tarcza Kryzysowa koncentrowała się na następujących priorytetach: wsparciu przedsiębiorstw, wsparciu sektora opieki zdrowotnej, wsparciu edukacji (w tym cyfryzacji placówek oświatowych), a także wsparciu lokalnych projektów przyczyniających się do rozwoju lokalnego. Tarcza Małopolska jest programem mającym łagodzić skutki społeczne i gospodarcze kryzysu wywołanego pandemią, a jej ewaluacja stała się przedmiotem licznych opracowań.

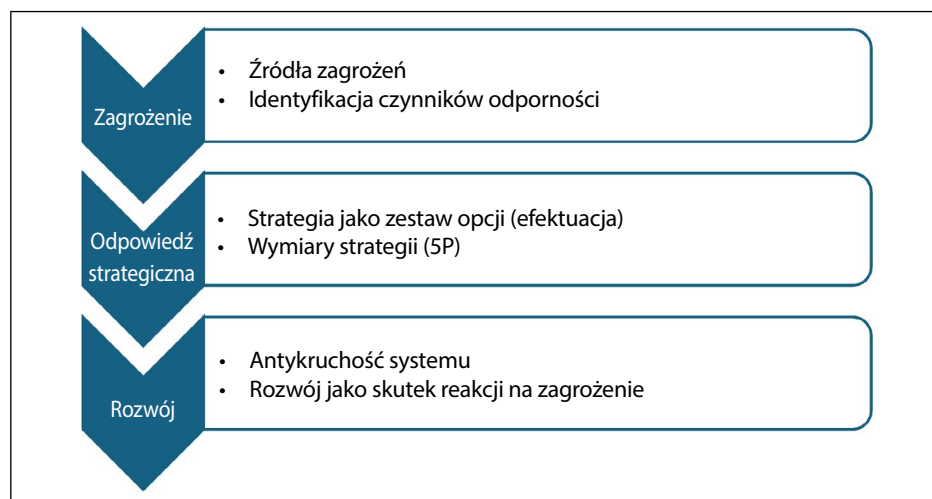
Jak wskazano uprzednio w tabeli 1, katalog zagrożeń związanych z odpornością jest bardzo szeroki i z natury rzeczy trudny lub niemożliwy do przewidzenia. Stąd wraz z sygnalizowaną zmianą koncepcji strategii w kierunku efektywności, portfela opcji i zarządzania sytuacyjnego, należy rozważyć potrzebę nowego modelu rozwoju społeczno-gospodarczego, którego immanentną cechą będzie występowanie kryzysów, które dzięki właściwej strategii mogą stać się czynnikami rozwoju organizacji terytorialnej. Podejście takie wymaga nie tylko zmiany systemowej w zakresie zarządzania rozwojem regionalnym i lokalnym, lecz także zmiany koncepcyjnej w zakresie trwałych podstaw leżących u zachowania ładu społeczno-gospodarczego.

Model odporności strategicznej jednostek samorządu terytorialnego

Zaprezentowany na rysunku nr 3 model odporności strategicznej integruje opisane wyżej koncepcje i pojęcia związane z odpornością strategiczną organizacji terytorialnej. Model ten składa się z trzech podstawowych faz kształtowania odporności organizacyjnej: wystąpienia zagrożenia oraz jednoczesnej identyfikacji czynników odporności, odpowiedzi ujętej w ramach strategii oraz rozwoju jako skutku przeciwdziałania zagrożeniu. W ujęciu tym rozwój jest efektem kompleksowej strategicznej reakcji organizacji na występujące zagrożenie. Należy w tym przypadku zwrócić uwagę, iż klasyczne podejście do strategii jako planu działania okazuje się niewystarczające. Strategia rozumiana szeroko w ujęciu koncepcji Mintzberga

dostarcza adekwatnych ram pojęciowych dla analizy zachowań w obliczu kryzysu. Dodatkowo ujęcie to może być wzmocnione koncepcją efektuacji akcentującą iteracyjne i adaptacyjne podejście. Antykruchłość systemu z kolei stanowi zdolność organizacji do wykorzystania kryzysu do transformacji oraz rozwoju.

Rysunek 3. Model odporności strategicznej jednostek samorządu terytorialnego



Źródło: opracowanie własne.

Podsumowanie

Zmienne otoczenie stawia przed jednostkami samorządu terytorialnego nowe wyzwania w postaci konieczności radzenia sobie z kryzysami i zagrożeniami zarówno naturalnymi, jak i antropogenicznymi. Szybkość zmian, nieprzewidywalność zdarzeń skłania do budowania strategii odpornych na zagrożenia. Strategiczne podejście do odporności wykracza poza wąsko rozumianą reaktywność organizacji na potencjalne zagrożenia. Jest podejściem aktywnym, otwartym na zmiany i wyzwania, przed którymi stają samorządy. Dużym pozytywnym krokiem w zarządzaniu samorządem było wprowadzenie strategicznego podejścia. W świetle wyżej wymienionych faktów, obecnie jednostki samorządu terytorialnego stoją przed kolejnym wyzwaniem, jakim jest włączenie do strategii elementu odporności organizacyjnej. O ile jednak stosunkowo łatwo o zbudowanie ram koncepcyjnych dla strategii odpornych na kryzysy z wykorzystaniem znanych koncepcji teoretycznych, o tyle wyzwaniem jest operacjonalizacja zagadnienia i wdrożenie w sferę praktyki. Z pewnością wymaga to badań studiów przypadków pozwalających w indukcyjny sposób na wskazanie strategicznych czynników odporności organizacyjnej. Ponadto istnieje potrzeba analizy powiązań pomiędzy poziomem strategii a zarządzaniem operacyjnym w kontekście reagowania na kryzysy, a także analizy rozwoju organizacji w wyniku reakcji na kryzys.

Mając na uwadze powyższe, zasadne wydaje się sformułowanie następujących wniosków:

1. Istnieje potrzeba identyfikacji kluczowych czynników odporności organizacyjnej uwzględniającej kategorie potencjalnych zagrożeń.
2. Strategie rozwoju samorządu powinny w sposób bezpośredni uwzględniać zagadnienie odporności organizacyjnej.
3. Klasyczne podejście do planowania strategicznego w samorządzie wymaga rewizji. Zarządzanie strategiczne powinno uwzględniać strategie ewolucyjne, inkrementalne oraz podejście efektywne.
4. Strategia rozwoju organizacji terytorialnej powinna zapewniać systemowi właściwości antykruchości, tj. zdolności nie tylko przetrwania kryzysu, lecz rozwoju i transformacji w kierunku nowego stanu odpowiadającego nowym wyzwaniom.

Bibliografia

- British Standards Institution. (2014). *BS 65000:2014 – Guidance on organizational resilience*. <https://knowledge.bsigroup.com/products/guidance-on-organizational-resilience>
- Czakon, W. (2018). Problem krótkowzroczności strategicznej. *Przegląd Organizacji*, 3, 17–22. <https://doi.org/10.33141/po.2018.03.03>
- Grosse, T. G. (2002). *Przegląd koncepcji teoretycznych rozwoju regionalnego*. *Studia Regionalne i Lokalne*, 1(8), 25–48.
- Hamel, G., & Välikangas, L. (2003). The quest for resilience. *Harvard Business Review*, 81(9), 52–63.
- International Organization for Standardization. (2017). *ISO 22316:2017 – Security and resilience – Organizational resilience – Principles and attributes*. <https://www.iso.org/standard/50053.html>
- Klasik, A. (red.). (2006). *Strategia rozwoju regionów*. Katowice: Akademia Ekonomiczna w Katowicach.
- Kudłacz, T. (1999). *Programowanie rozwoju regionalnego*. Wydawnictwo Naukowe PWN.
- Mintzberg, H., & Quinn, J. B. (1996). *The strategy process: Concepts, contexts, cases* (3rd ed.). Prentice Hall.
- Perechuda, K. (2010). *Zarządzanie wiedzą w przedsiębiorstwie*. Wydawnictwo Naukowe PWN.
- Ponomarev, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management*, 20(1), 124–143. <https://doi.org/10.1108/09574090910954873>
- Sarasvathy, S. D. (2001). Causation and effectuation: Toward a theoretical shift from economic inevitability to entrepreneurial contingency. *Academy of Management Review*, 26(2), 243–263. <https://doi.org/10.5465/amr.2001.4378020>
- Strahl, D. (red.). (2010). *Metody oceny rozwoju regionalnego*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.
- Strategia Rozwoju Województwa „Małopolska 2030”. (2020). *Urząd Marszałkowski Województwa Małopolskiego*. <https://www.malopolska.pl/strategia-2030>
- Szajnowska-Wysocka, A., & Sitek, S. (2015). *Koncepcje teoretyczne rozwoju regionalnego*. Wydawnictwo Uniwersytetu Śląskiego.
- Taleb, N. N. (2012). *Antifragile: Things That Gain from Disorder*. Random House.

- Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly*, 38(4), 628–652.
- Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected: Assuring high performance in an age of complexity*. Jossey-Bass.
- Wildavsky, A. (1988). *Searching for safety*. Transaction Publishers.
- Winiarski, B. (red.). (2008). *Polityka gospodarcza*. Warszawa: Wydawnictwo Naukowe PWN.

Rola strategii we wzmacnianiu odporności jednostek samorządu terytorialnego *Streszczenie*

Celem artykułu jest opis i wyjaśnienie roli strategii rozwoju w budowaniu odporności organizacyjnej jednostek samorządu terytorialnego. Tekst prezentuje przegląd zagrożeń naturalnych i społecznych, z jakimi mogą zmagać się jednostki samorządu terytorialnego, i proponuje przegląd czynników wpływających na podniesienie odporności. W dalszej części, wykorzystując koncepcje wymiarów strategii H. Mintzberga, dokonuje analizy strategii jako punktu wyjścia dla antycypacji kryzysu, reagowania na kryzys oraz adaptacji. W prezentowanym ujęciu strategia stanowi nie tylko instrument planowania rozwoju gospodarczego i społecznego, lecz dostarcza także ram koncepcyjnych dla przezwyciężenia kryzysu i zapewnienia rezyliencji organizacyjnej. Jednocześnie zwraca uwagę na potrzebę nowego podejścia do formułowania strategii jako portfela opcji opartej na koncepcji efektuacji.

Słowa kluczowe: odporność organizacyjna, samorząd terytorialny, strategia, rozwój regionalny

The role of strategy in strengthening the resilience of local government units *Abstract*

The aim of the text is to describe and explain strategies of regional development as tools of strengthening organizational resilience. The paper presents a brief review of threats both natural and social that may affect organizational *equilibrium*. Moreover, a catalogue of factors that enhance organizational resilience is discussed. Subsequently using H. Mintzberg's concept of strategy, conceptual frames are identified as tools for crisis anticipation, crisis reaction and adaption. From the presented perspective strategy is not only tool for planning social and economic development but also a crucial instrument for overcoming crisis and strengthening organizational resilience. Simultaneously new strategic approach is required understood as a set of options based on effectuation theory.

Key words: organizational resilience, local self-government, strategy, local development

Wkład autorów / Author Contributions

Konceptualizacja / Conceptualization: P.P.

Metodologia / Methodology: P.P.

Analiza formalna / Formal analysis: P.P.

Badania / Investigation: P.P.

Zasoby / Resources: P.P.

Przygotowanie wersji wstępnej / Writing – original draft: P.P.

Recenzja i edycja / Writing – review & editing: P.P.

Materiały dodatkowe / Supplementary Materials

Nie dotyczy / Not applicable.

Finansowanie / Funding

Badania nie otrzymały żadnego zewnętrznego finansowania. / This research received no external funding.

Oświadczenie o zatwierdzeniu etycznym / Ethics Approval Statement

Nie dotyczy / Not applicable.

Oświadczenie o świadomej zgodzie / Informed Consent Statement

Nie dotyczy / Not applicable.

Oświadczenie o dostępności danych / Data Availability Statement

Udostępnianie danych nie ma zastosowania do tego artykułu, ponieważ w ramach badania nie wygenerowano ani nie analizowano żadnych nowych danych. / Data sharing is not applicable to this article as no new data were generated or analyzed in this study.

Oświadczenie o użyciu generatywnej sztucznej inteligencji / Declaration of Generative AI Use

Do przygotowania niniejszego artykułu nie wykorzystano narzędzi generatywnej sztucznej inteligencji. / No generative artificial intelligence tools were used in the preparation of this manuscript.

Podziękowania / Acknowledgments

Nie dotyczy / Not applicable.

Konflikt interesów / Conflict of Interest

Paweł Ptaszek deklaruje brak konfliktu interesów. / Paweł Ptaszek declares no conflict of interest.

The involvement of employees in retailers' operational departments in loss prevention in distribution logistics

Janusz Liber

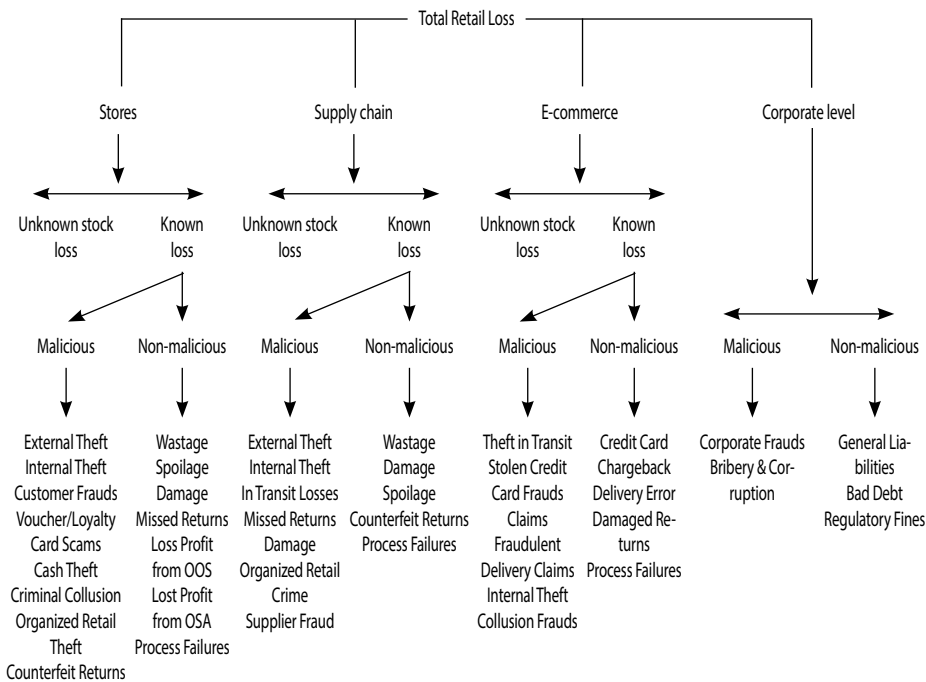
BEng, PhD, Faculty of Security Sciences, Andrzej Frycz Modrzewski Krakow University, Kraków, Poland

<https://orcid.org/0000-0003-4562-4661>

Introduction

A retail chain plays a crucial role in distribution logistics, representing the final step that transfers products from distribution centres to the customer via stores, handling inventory management, transport, and last-mile delivery to meet demand efficiently and profitably. Shrinkage in retail chains negatively impacts their financial performance and customer buying behaviours (Figiel et al., 2020). The concept of 'Total Retail Loss' (TRL) (Beck, 2016) presents the complexity of loss in retail chains, as well as the challenges associated with developing a loss-prevention policy. TRL includes elements that are not considered in the loss-prevention strategy of the supply chain examined here, such as natural disasters, so the author has limited the scope of the study accordingly (Figure 1).

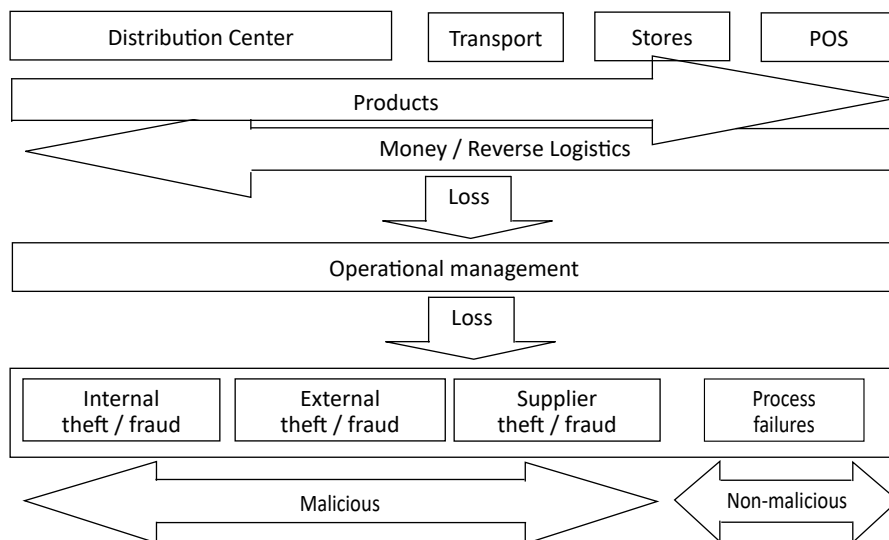
Figure 1. Total Retail Loss



Source: own work, based on: Beck, 2016; Figiel et al., 2020.

According to the Centre for Retail Research (Bamfield, 2008) shrinkage is the term generally used in the retail industry to measure ‘inventory losses from crime and waste’, expressed here as a percentage of retail sales. To systematize research in this area, Efficient Consumer Response (ECR) adopted the following definition (Beck, 2004: 3): shrinkage is a combination of inter-company fraud, process failures, internal theft and external theft. Loss is defined as the difference between the recorded quantity of goods and their actual quantity, where the discrepancy arose from internal theft, external theft, supplier fraud or process errors (Beck, 2002: 11–12). A similar definition can be found in the literature in Polish (Fertsh, 2006: 2008): ‘stock loss is the loss of inventory occurring in the supply chain or in a store, which is a result of errors, theft, fraud, etc.’ (Figure 2).

Figure 2. Shrinkage in distribution logistics (retail chain), excluding corporate losses



Source: own work, based on: Beck et al., 2002: 27; Figiel et al., 2020.

To systematize the concept of shortage/loss, it should be noted that shortage is the quantitative difference between the actual and recorded state of goods, while loss is the value of the missing goods. The amount of loss is calculated by multiplying the number of missing products by their price. In this article, the author adopts the definition of loss proposed by the ECR, which allows for the interchangeable use of the terms loss and shrinkage.

In the realities of operational management of retail chains, stock losses are divided in several ways. The first of them is: known and unknown loss (Beck et al., 2002: 30).

- known stock loss: shrinkage that we know has occurred (we can identify the goods, their location and the time of their occurrence). Examples include products past their expiry date, physically damaged or destroyed goods, etc.;
- unknown stock loss: unexplained discrepancies in inventory (shrinkage) that cannot be defined (when, where, or sometimes even the type of missing product). They are most often the result of crimes. This type of loss is usually discovered during routine inspections, such as inventory counts.

Another division of losses accepted by academic communities and business is divided into two categories:

- non-malicious shrinkage: these are losses of products or monetary value within the supply chain that occur as a result of unintentional actions, without the intention of generating them. They are most often caused by non-compliance or improper process design (Figiel et al., 2020: 13–16).

- malicious shrinkage: damage to products or monetary value in the supply chain that was caused by the perpetrator intentionally, through his or her knowing action (Figiel et al., 2020: 20,25).

It is worth noting that non-malicious losses are typically less dynamic than intentional losses, and therefore more susceptible to preventative action (Beck, 2002: 10). This makes it easier to identify and implement measures to counteract their causes. In the case of intentional losses, countermeasures will aim to deter potential perpetrators or discourage them from committing an act that results in a loss.

It should be pointed out that one element of a loss-prevention policy common to the above-mentioned types of losses (non-malicious / malicious) is the implementation of preventative actions, which are primarily aimed at hindering or preventing losses by monitoring¹ pre-defined people, processes, goods and places at a specific period of time².

Retail chain vulnerabilities

The purpose of a supply chain is to deliver goods from the manufacturer to the end user. Therefore, it can be assumed that risk itself in the supply chain occurs in the form of any event that may affect the movement of materials and disrupt the planned flow of goods (Waters, 2011: 7). The specific nature of risk in a supply chain is the transfer of the consequences of an event occurring in a single link to other entities. The essence of this is that each link is exposed not only to its own risk, but also to the consequences of negative incidents occurring in other links in the same chain. 'The value of the supplier-recipient relationship is influenced by the excellence of the business partners' actions, because the effects of disruptions occurring in one of them may affect the other party or reach further in the supply chain. It is extremely important to shape the awareness of its participants as to the importance of risk issues' (Wieteska 2012: 76–125). Therefore, even if the individual risk of each part of supply chain is low, the cumulative effect of several hundred, or even several thousand, links concentrated in large organizations becomes significant (Waters, 2011: 49).

Risk is not distributed evenly across time, space and location. Nor is it distributed evenly across products and processes etc. within the supply chain. Individual locations, products, processes, and even people are significantly more vulnerable to loss than others (Figiel et al., 2020: 30–31). A useful tool for obtaining a real picture of losses is the 'hot' concept (Beck, Chapman, 2003: 16), which assumes that certain elements in the supply chain – places, products, processes, and people – are more susceptible to generating losses than others. Identifying them is the basis for preparing and

¹ Providing CCTV (Closed Circuit Television), applying EAS (Electronic Article Surveillance), changing processes, etc.

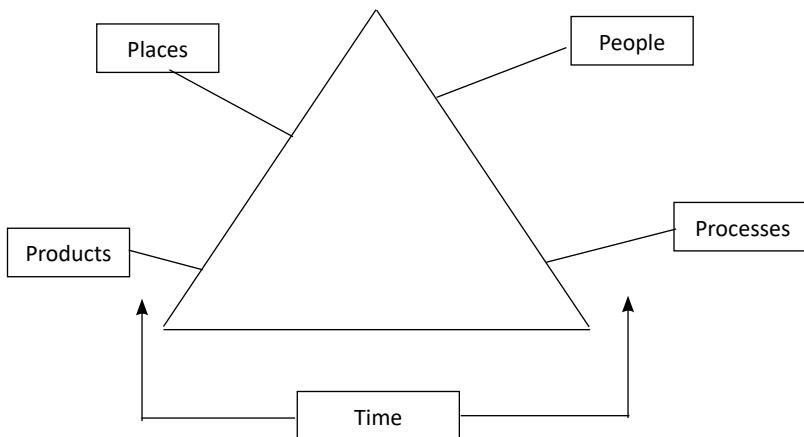
² An example of such action is the "hot concept", described later in this article.

implementing preventative measures (Figiel et al., 2020). As a result of this research, the author of this article has 'enriched the essence of the hot concept with an additional element (the time of loss generation) (see Figure 3).

This proposal (including the time element in the concept of 'hot') is based on scientific data, business news and unpublished results of research conducted by the author.³ These sources indicate that losses in retail chains increase during specific seasons, such as holidays (Pannell, 2019; Bamfield, 2014: 30, 52, 60–61), festivities (Figiel et al. 2020: 44; Bamfield, 2014: 30, 38, 52, 60–61), the back-to-school period (Bamfield, 2014: 30, 38, 61), and even sales promotion activities (Carter, 1995: 57–64; Carter et al., 1995: 81–82).

In most retail chains, dedicated departments are responsible for implementing loss-reduction activities, including utilizing the 'hot concept'⁴. These activities are supported by other organizational units⁵ that, as part of their operations and identified threats (hot elements), implement the initiatives defined in the loss-prevention policy (Beck et al., 2003: 7).

Figure 3. 'Hot' concept



Source: own work, based on Beck, Chapman, 2003: 16.

Previous research, conducted primarily by academics in Poland (Liber, Szczepankiewicz, 2012: 111–122) and Western Europe (Beck et al., 2002; Beck et al., 2003;

³ In the past, the author worked for leading retailers and led numerous loss-prevention projects, where "hot time" was identified as a key factor in reducing losses, e.g. having worked for TESCO PLC, the author held the posts of Corporate Security Manager (Poland), Fraud Prevention and Security Manager (Poland, Czech Republic, Slovakia), Central Europe Corporate Security & Resilience Manager (Poland, Czech Republic, Slovakia, and Hungary).

⁴ In retail chains, these organizational units have different names: security, loss prevention, audit, control, etc.

⁵ HR, H&S, logistics, purchasing, legal department, IT, etc.

Beck, Chapman, 2003; Beck, Peacock, 2009; Beck, Chapman, 2020) has focused on analyzing the collaboration between individual organizational units within the retail network (supply chain) to reduce losses. They did not include an attempt to establish possible connections between the position of operational departments' employees in the organizational structure⁶, their personal responsibility for losses, or the possibility of obtaining information that may be of significant importance for the preparation and implementation of a loss-reduction policy.

Taking the circumstances into account, as well as the need to address the research gap, the following research question was adopted: Is there a relationship between the position within a retail chain's organizational structure from which an employee is involved in loss reduction and the ability to obtain information necessary to develop a loss-prevention policy?

These circumstances are particularly significant due to the ongoing optimization of employment in retail chains, which is generally associated with reducing staff in support departments⁷ and/or outsourcing loss-prevention processes. Given the facts mentioned above, the following assumption was made in the research:

Hypothesis: There is a relationship between the position within a retail chain's organizational structure from which an employee is involved in loss reduction and the ability to obtain information necessary to develop a loss-prevention policy.

Research methodology and key findings

This article presents some of the results of a research project conducted by the author on the supply chain of a product that, according to global data, generates some of the highest shrinkage (hot product) in the FMCG sector.

The complexity of FMCG supply chains, including their high susceptibility to losses, distinguishes entities operating in this industry from other retail chains. The FMCG sector is characterized by significant product differentiation⁸, high sales volume, low margins and a variety of distribution channels. The specificity of this sector is also determined by the need to store and transport goods⁹ under strictly defined conditions¹⁰ (e.g. cold chain supply), as well as the very frequent movement of products. These factors lead to the need to integrate processes and operations across

⁶ Organizational units that are not directly responsible for the level of loss.

⁷ Security, loss prevention, audit, control, risk management, etc.

⁸ FMCG retail chains offer up to 250,000 SKUs for sale. Managing such "mass of goods" between manufacturers, distribution centres and retail chains clearly requires collaboration across the supply chain.

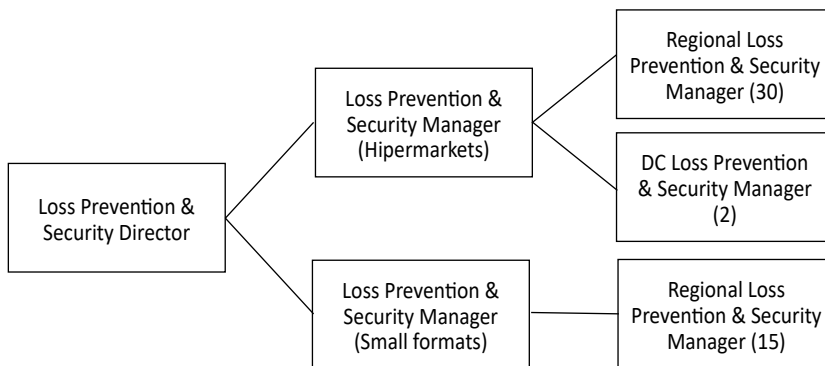
⁹ Transport management in the FMCG sector is a complex process. As exemplified by the study results, the LPS Department of the international retailer taking part in the research collaborates with approximately 400 transport companies, some of which are sole proprietorships.

¹⁰ An example would be the delivery of a kind of cheese to the retail chain participating in the research: a long supply chain and a luxury product, susceptible to improper storage conditions. In the case of interruption e.g. delivery time slots problems, supplier fraud, food spoilage, etc., it is almost impossible to meet customer satisfaction (needs) by offering alternative products.

the entire supply chain to prevent losses.

The empirical study was planned to encompass 300 current and former managers (various levels) responsible for loss prevention across the supply chain studied here. The research was based on a questionnaire distributed to respondents. 224 completed questionnaires were received, representing 74.7% of the total sample. After analyzing the initial research results, 40 respondents were selected for personal interviews to further elaborate on their responses to selected survey questions. Since the scope of this article concerns distribution logistics, this study utilizes data obtained from respondents who were knowledgeable about this part of the supply chain. The supply chain under investigation featured various organizational forms of loss-prevention units (Figure 4).

Figure 4. Structure of the security and loss-prevention department of one of the retail chains participating in the study



Source: own work based on the author's research in the supply chain covered by the article.

The hypothesis was tested by contingency tables obtained from the summary of respondents' answers to the following questions and the Chi-square test of independence. The author verified that the assumptions of Pearson's chi-square test of independence were met, ensuring that the expected cell frequencies satisfied the minimum requirements (i.e. at least 80% of the cells had expected counts ≥ 5 and no cell had an expected count < 1), thereby warranting the valid interpretation of the statistical results.

Question 1. Please indicate the scope of information analyzed at your institution regarding loss prevention. Please select all applicable answers.

- 1) 'Hot products'.
- 2) 'Hot places'.
- 3) 'Hot processes'.

- 4) 'Hot people'.
- 5) 'Hot time'.
- 6) Other elements (please specify).

Question 2. At which level of your organization's hierarchy does the obligation to prevent losses originate?

- a) Employee.
- b) Department Manager.
- c) Head of Unit (store, DC, etc.).
- d) Regional Manager.
- e) General Manager.
- f) There is no such obligation.

Table 1 compares the level of responsibility for shrinkage to loss-prevention information analyzed.

Table 1. The relationship between the level of responsibility for shrinkage and information analyzed in the field of loss prevention

The relationship between the level of responsibility for shrinkage and:	p value for the Chi-square test of independence	Cramer's V
'Hot products' identification	0,00	0,85
'Hot processes' identification	0,00	0,81
'Hot places' identification	0,00	0,77
'Hot time' identification	0,00	0,31

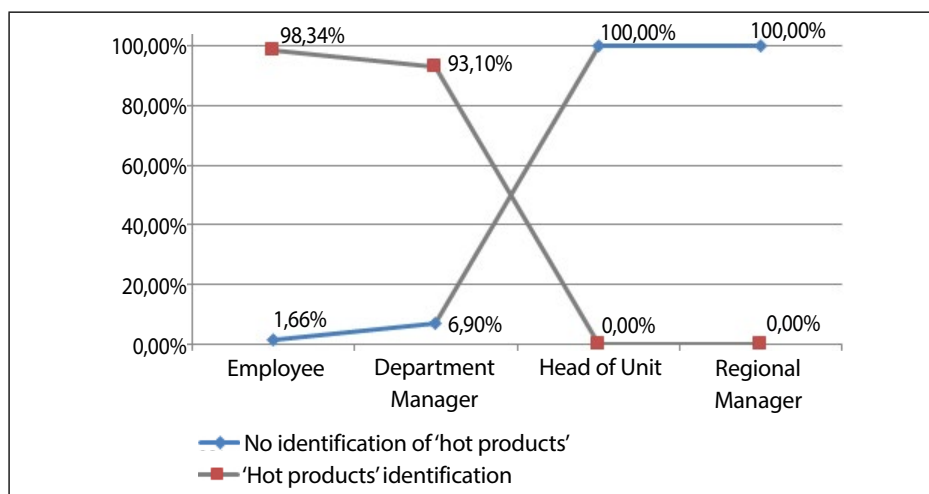
Source: own research.

The first column contains the name of the variables, the second column shows the p value for the Chi-square test of independence, and the third column presents the value of Cramer's V, which gives information about the strength of the relationship between the variables.

A value in the second column below 0.05 indicates a statistically significant relationship between the variables. If a relationship is found, its strength should be assessed, as indicated by the value in the third column. Cramer's V coefficient ranges from 0 to 1, which is mutually closed. Values close to zero indicate a weak relationship, while values close to one indicate a strong relationship between the variables. From several statistically significant relationships, the strongest ones were selected; these are highlighted in the corresponding rows. It should be clearly emphasized that these are strong relationships.

Details of the relationship between the level of loss prevention and the identification of 'hot products' (Chart 1).

Chart 1. Relationship between the level of loss prevention and the identification of 'hot products'



Source: own research.

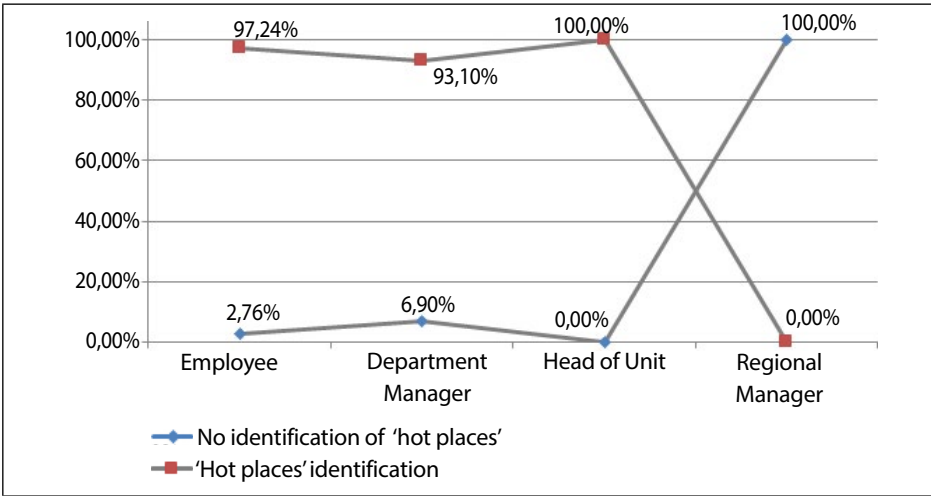
Among retail chains (units), where the level of responsibility for shrinkage begins at the employee, approximately 98% identify the products generating the highest losses, while just under 2% do not analyze this information. Among respondents who indicated that responsibility for shrinkage begins with the department manager, approximately 93% identify the products associated with the highest losses, while approximately 7% do not analyze this information. Among those participants who indicate that responsibility for shrinkage lies with heads of units or the regional manager, none identify the products generating the highest losses.

Details of the relationship between the level of loss prevention and the identification of 'hot places' (Chart 2).

Among companies where responsibility for losses begins at the employee, approximately 98% identify the areas associated with the highest losses, while nearly 3% do not analyze this information. Among respondents who indicated that responsibility for shrinkage originates with the department manager, approximately 93% identify the areas associated with generating the highest losses, while approximately 7% do not analyze this information. Among those surveyed who indicated that responsibility for shrinkage lies with heads of units, 100% of respondents identify the element associated with loss, whereas in cases where the regional manager is responsible for losses, none of the companies identify the areas associated with generating the highest losses.

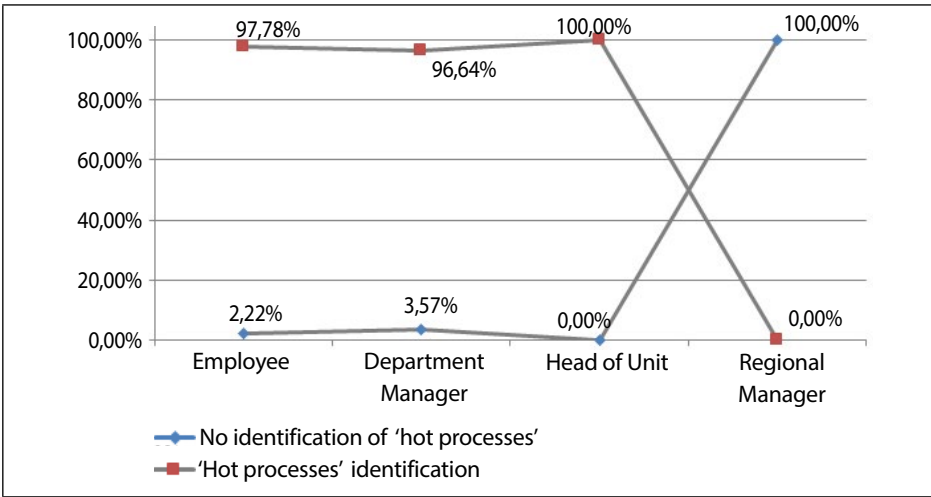
Details of the relationship between the level of loss prevention and the identification of 'hot processes' (Chart 3).

Chart 2. Relationship between the level of loss prevention and the identification of 'hot places'



Source: own research.

Chart 3. Relationship between the level of loss prevention and the identification of 'hot processes'



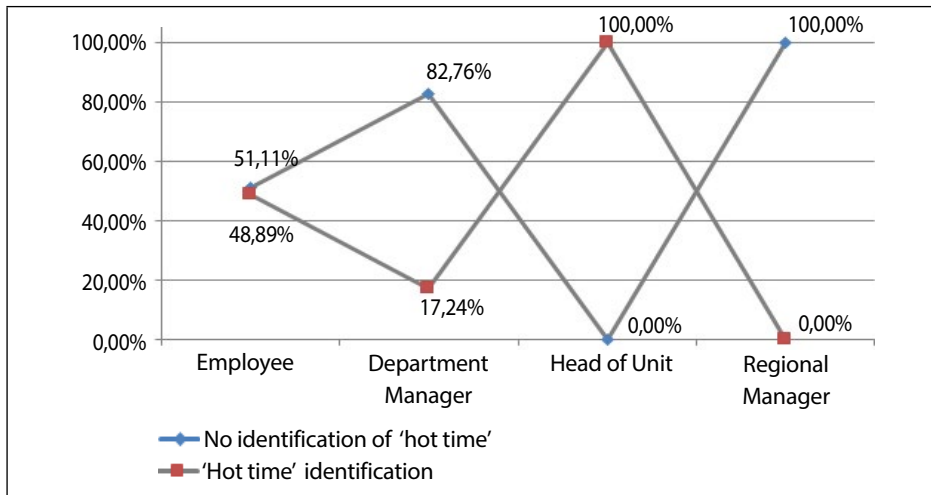
Source: own research.

Among companies where responsibility for shrinkage begins at the employee, nearly 98% identify the processes generating the highest losses, while approximately 2% do not analyze this information. Among respondents who indicated that responsibility for shrinkage originates with the department manager, approximately 96% identify the processes associated with generating the highest losses, while nearly 4%

do not analyze this information. 100% of companies that indicate that the responsibility for shrinkage lies with heads of units identify the element associated with loss, whereas in the case of responsibility for shrinkage at the regional level, none of the companies identify the processes associated with generating the highest losses.

Details of the relationship between the level of loss prevention and the identification of 'hot time' are provided in Chart 4.

Chart 4. Relationship between the level of loss prevention and the identification of 'hot time'



Source: own research.

Among companies where responsibility for shrinkage begins at the employee, nearly 49% identify the time/period in which the highest losses occur, while approximately 51% of respondents do not analyze this information. Among respondents who indicated that responsibility for shrinkage originates at the department manager level, approximately 17% identify the period associated with the occurrence of the highest losses, while nearly 83% do not analyze this information. 100% of companies that indicate that the level of responsibility for shrinkage lies with heads of units identify the element associated with loss, whereas in the case of responsibility for shrinkage at the regional level, none of the entities identify the time/period associated with generating the highest losses.

Conclusions

The research results confirm the correlation between the variables studied here. The level at which loss prevention is required in distribution logistics has a significant

impact on the type of information necessary to prepare and implement current and long-term loss-prevention policies. The survey results revealed an interesting picture: the potential responsibility of regional and top-level managers for shrinkage does not result in the collection of the information identified in the 'hot concept'.

The best results in this regard are achieved by imposing loss-prevention obligations on employees, department managers and heads of units. In this case, we obtain complementary information on all elements of the 'hot concept', excluding knowledge about those individuals that generate the highest losses.

The reason for the lack of analysis of information regarding 'hot people' in the supply chain reviewed here was identified during interviews with selected respondents. The research results indicate that loss reduction in retail chains is primarily focused on implementing preventative measures. The identification of 'hot people' is, in most cases, a result of monitoring previously identified processes, products and places within a specific period of time¹¹. Typically, this type of information is obtained in two stages: firstly, as a result of the analysis of specific risk elements ('hot concept'), secondly, the implementation of the loss-prevention policy tailored to the pre-identified threats.

Based on these findings, the author makes targeted recommendations for the implementation of the loss-prevention strategy and proposes that the effectiveness of operations be measured not only by what risks are controlled, but also by how controls interact to prevent, identify and respond to the main causes of losses. One of the most frequently applied strategic approaches is the Deter, Detect, Delay, Deny, Defend, and Defeat methodology. To overcome these challenges, it is necessary to implement a comprehensive loss-prevention strategy, which could be based on the principles of ISO 18788:2015¹², ISO 31000:2018¹³, or ISO 28000:2022¹⁴. However, in such cases, shrink-reduction initiatives should consider various solutions, especially the research findings presented in this article as a new and universal loss-prevention tool.

¹¹ 'Hot people' are not usually analysed directly (except when caught red-handed) because of various factors. First of all GDPR (General Data Protection Regulations), which strictly stipulate how personal data is processed, e.g. those of offenders. Secondly, in loss-prevention activities, especially malicious shrinkage reduction, the most preventative actions are based on the 'theft/fraud triangle', which indicates that theft / fraud occurs when three elements coincide: pressure (need), opportunity (weak controls), and rationalization (justifying the act). This is used to identify risks and prevent theft / fraud by focusing on reducing opportunities through internal controls on 'hot' processes, places, products, in, but not only, 'hot' time. Due to the confines of the article, the author has limited himself to only a partial explanation of the issue of how to analyze 'hot people', which depends on many elements, e.g. types of losses (malicious, non-malicious), perpetrators (customers, employees, suppliers, Organized Retail Rings), and the loss-prevention policy, always tailored to pre-identified risk as well as vulnerabilities.

¹² Management system for private security operations — Requirements with guidance for use.

¹³ Risk Management.

¹⁴ Supply Chain Security.

The proposed loss-prevention tool results from the circumstances that ISO standards show only the 'bigger picture' of management, which has to be detailed (pinpointed) in day-to-day operations to ensure that loss-prevention activities are correctly applied in 'hot elements', at each echelon in an organizational structure, across distribution logistics.

References

- Bamfield, J. (2008). *The Global Retail Theft Barometer (2008) Monitoring the Costs of Shrinkage and Crime on the Global Retail Industry. The Worldwide Shrinkage Survey*, Centre for Retail Research.
- Bamfield, J. (2014). *The New Barometer (2013–2014) A study of the cost of merchandise theft and merchandise availability for the global retail industry*, Centre for Retail Research.
- Beck, A. (2002). *Automatic Product Identification & Shrinkage: Scoping the Potential, A White Paper for ECR Europe*, Efficient Consumer Response.
- Beck, A., Bilby, Ch., Chapman, P. (2002). Shrinkage in Europe: Stock Loss in the Fast-moving Consumer Goods Sector, *Security Journal*, 15(4), 25–40.
- Beck, A., Bilby, Ch., Chapman, P. (2003). Tackling Shrinkage in the Fast Moving Consumer Goods Supply Chain: Developing a Methodology. *Security Journal*, 16(2), 61–75, <https://link.springer.com/article/10.1057/palgrave.sj.8340133> [accessed 30.12.2025].
- Beck, A., Chapman, P. (2003). *Hot Spots in The Supply Chain: Developing and Understanding of What Makes Some Retail Stores Vulnerable to Shrinkage*, White Paper for ECR Europe.
- Beck, A., Chapman, P., Peacock, C. (2003). *Shrinkage: A Collaborative Approach to Reducing Stock Loss in the Supply Chain*, Efficient Consumer Response Europe.
- Beck, A. (2004). *Shrinkage in Europe 2004: A Survey of Stock Loss in the Fast Moving Consumer Goods Sector*, Efficient Consumer Response in Europe.
- Beck, A., Peacock, C. (2009). *New Loss Prevention-Redefining Shrinkage Management*, Palgrave Macmillan.
- Beck, A. (2016). *Beyond Shrinkage: Introducing Total Retail Loss*, Retail Industry Leaders Association, https://www.researchgate.net/publication/312523995_Beyond_Shrinkage_Introducing_Total_Retail_Loss?channel=doi&linkId=58807df008ae9a860ffa6257&showFull-text=true [accessed 30.12.2025].
- Beck, A., Chapman, P. (2020). *A proven approach to shrinkage reduction*, Research Paper, ECR Loss, <https://ecrloss.com/research-paper/shrinkage-and-stock-loss-in-supply-chain/> [accessed 30.12.2025].
- Carter, N. (1995). Increased theft as a side effect of sales promotion activities: An exploratory study, *Journal of Business and Psychology*, 10(1), 57–64.
- Carter, N., Kindstedt, A., Melin, L. (1995). Increased sales and thefts of candy as a function of sales promotion activities: preliminary findings, *Journal Of Applied Behavior Analysis*, 28(1), 81–82.
- Fertsh, M. (Ed.) (2006). *Słownik terminologii logistycznej*, Instytut Logistyki i Magazynowania, Poznań, <https://www.logistyka.net.pl/niezbednik-logistyka/slownik/main?start=0&keyword=ubytek> [accessed 30.12.2025].
- Figiel, A., Koziół, L., Liber, J. (2020). *Instrumenty zapobiegania stratom w łańcuchach dostaw logistycznych sektora FMCG*, MWSE.

- Liber, J., Szczepankiewicz, W. (2012). Współpraca w łańcuchu dostaw jako element zapobiegania stratom. In S. Kauf (Eds.), *Logistyka i inne koncepcje zarządzania w naukach ekonomicznych* (pp. 111–122). Uniwersytet Opolski.
- Pannell, K. (2019). *Shoplifting traditionally increases during holiday season, along with arrests*, U.S. Army, 16.12, https://www.army.mil/article/231031/shoplifting_traditionally_increases_during_holiday_season_along_with_arrests [accessed 10.03.2026].
- Waters, D. (2011). *Supply Chain Risk Management. Vulnerability and Resilience in logistics*, The Chartered Institute of Logistics and Transport (UK), KoganPage.
- Wieteska, G. (2012). *Zarządzanie ryzykiem w łańcuchu dostaw na rynku B2B*. Difin.

The involvement of employees in retailers' operational departments in loss prevention in distribution logistics

Abstract

This article explores shrinkage in retail chains, the main causes of their occurrence and selected methods for analyzing information in order to develop a loss-prevention policy. This paper presents the research methodology and findings on the relationship between the employee's position within retailers' organizational structures and their involvement in loss reduction, and the ability to obtain information necessary to develop a loss-prevention policy. The paper fills a research gap in this area; to date, no research on this topic has been conducted in Poland (Europe).

Keywords: supply chain, retail chain, shrinkage, loss, risk management, loss prevention

Author Contributions

Conceptualization: J.L.

Methodology: J.L.

Formal analysis: J.L.

Investigation: J.L.

Resources: J.L.

Writing – original draft: J.L.

Writing – review & editing: J.L.

Supplementary Materials

Not applicable.

Funding

This research received no external funding.

Ethics Approval Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

All relevant aggregated data generated and analysed during this study are included within the article. The raw datasets (individual survey responses and interview transcripts)

are not publicly available due to Non-Disclosure Agreements (NDAs) and to ensure the anonymity of the participating managers and the confidentiality of their organizations.

Declaration of Generative AI Use

No artificial intelligence tools were used in the preparation of this manuscript.

Acknowledgments

Not applicable.

Conflict of Interest

Janusz Liber declares no conflict of interest.

The transformation of the European economic environment under the impact of the war in Ukraine: An analytical assessment of key challenges and future development trajectories

Iryna Kravets

MPA, PhD in Economics, Assoc. Prof., Sozialprojekte Niederrhein, Germany
<https://orcid.org/0000-0001-5919-6560>

Valentyna Yakobchuk

PhD in Economics, Professor, Polissia National University, Ukraine
<https://orcid.org/0000-0003-2147-7994>

Introduction

Over the past decade, the Russian-Ukrainian war has emerged as a critical external driver of structural change in Europe's economic system. Since 2014, and especially following Russia's full-scale military invasion of Ukraine in 2022, the European economic environment has undergone profound and multidimensional transformations that extend far beyond short-term cyclical fluctuations. The war in Ukraine has constituted not only a major security crisis but also an additional exogenous shock to the European economic model, which had not yet fully recovered from the COVID-19 pandemic. It has accelerated structural changes across the domains of energy, finance, trade, industrial policy, the labour market and social policy. Taken

together, these developments are shaping a new configuration of Europe's economic space, increasingly defined by the logic of security, geo-economic competition and strategic autonomy.

The annexation of Crimea and the outbreak of the war in eastern Ukraine in 2014 constituted the first signal of the erosion of European stability in the aftermath of the 2008 global financial crisis. This assessment is corroborated in the analytical section of this paper through an analysis of the Economic Policy Uncertainty index (Baker et al., 2016, pp. 1593–1636). However, it was the events of 2022–2025 that transformed the Russian-Ukrainian war into a fundamental challenge to the entire system of European and global economic order.

The disruption of energy supply chains linked to Russia, the reconfiguration of trade routes, rising military expenditures, inflationary pressures and the intensification of social polarization have emerged as the key consequences of this transformation, as documented in reports by the European Commission (2025b), the Centre for Economic Policy Research (Federle et al., 2024, pp. 9–12), European Central Bank (Adolfson et al., 2022, pp. 5–7) and the World Economic Forum (2025).

To interpret these transformations, this study draws on contemporary strands of theoretical and applied economic and political economy research that conceptualize the growing interdependence of markets, state power, and security considerations. The geoeconomic approach articulated by Blackwill and Harris (Blackwill & Harris, 2016, pp. 34–36) conceptualizes economic instruments as tools of statecraft and strategic influence deployed under conditions of intensified geopolitical competition, in which efficiency-based criteria are increasingly subordinated to strategic and security imperatives.

This analytical perspective is complemented by the work of Nadin, Stead, Dąbrowski, and Fernández-Maldonado (Nadin et al., 2021, p. 795) on integrated, adaptive and participatory policy frameworks in Europe, which emphasizes resilience, cross-sectoral policy coordination and institutional flexibility as core responses to systemic shocks and structural uncertainty. At the same time, contributions by Knaap, Nedović-Budić, and Carbonell (Knaap et al., 2015, pp. 270–275) in the field of state and spatial planning in the United States and Europe underscore the reassertion of public authority in steering economic development and managing strategic sectors under conditions of crisis and post-crisis transformation. Taken together, these theoretical approaches support the argument that the European Union is gradually moving away from the paradigm of open multilateralism towards a hybrid economic model that combines market mechanisms, industrial policy and the securitization of economic relations. The socio-economic dimension of these transformations is no less significant. Forced emigration from Ukraine, structural shifts in labour markets, increased fiscal burdens, heightened socio-economic inequality and rising risks of social polarization pose long-term

challenges for European economies. According to Eurostat and the State Statistics Service of Ukraine, between 2022 and 2025 Europe experienced the largest population displacement since World War II (UNHCR, 2026, Regional data). Although this influx of migrants has led to additional short-term costs associated with social support, it has also created potential opportunities for the renewal and more efficient redistribution of human capital in the economies of recipient countries.

Particular attention should also be paid to the growing role of information and cyber-economic challenges. Cyberattacks, disinformation campaigns, and digital interference in financial and energy systems have become integral parts of modern economic confrontation, forcing European states to review existing approaches to digital security and critical infrastructure management. Recent assessments by the European Union Agency for Cybersecurity and the Council of Europe highlight the growing convergence between economic resilience, technological sovereignty and national security within the European political agenda.

Against this backdrop, the aim of this article is to provide a comprehensive analysis of the transformation of the European economic environment under the influence of the war in Ukraine over the period 2014–2025, with a particular focus on systemic challenges, structural changes and potential trajectories for future development. The study considers the following future scenarios for EU countries: adaptive differentiation, security-oriented consolidation and strategic economic reconfiguration. It also examines alternative development paths for both Ukraine and the European Union depending on the outcome of the war, namely a Ukrainian victory, a temporary truce, or an outcome unfavourable to Ukraine. This approach makes it possible not only to assess current trends but also to create an analytical basis for the formulation of long-term policies aimed at economic stability, post-war recovery and the integration of Ukraine as a key component of the future European economic and security architecture.

Materials and methods

The study is based on a combination of secondary quantitative and qualitative data and applies an analytical research approach in order to assess the transformation of the European economic environment under the impact of the war in Ukraine. The methodological framework integrates contemporary theories of political economy, such as geoeconomics, institutional analysis and statistical analysis, which allows for a comprehensive examination of systemic shocks, structural changes and emerging development trajectories of the European Union. Within this framework, particular attention is paid to the concept of geoeconomics, which provides a key analytical lens for interpreting the transformation of the European

economic environment. Geoeconomics refers to the use of economic instruments – including trade policy, energy supply, financial regulation and industrial policy – as tools of strategic power under conditions of intensified geopolitical competition. In the context of Russia's full-scale invasion of Ukraine, economic relations are no longer governed solely by considerations of efficiency and market optimization, but are increasingly shaped by security imperatives and risk management strategies.

In this regard, the study introduces the notion of a “geoeconomic development model” of the European Union, understood as a transition from a system based on deep global interdependence and cost minimization towards a model centred on resilience, diversification and strategic autonomy. Prior to 2022, the EU economy relied heavily on open markets, global supply chains and relatively cheap external energy resources. However, the war in Ukraine has exposed the structural vulnerabilities of this model and accelerated its transformation into a hybrid system in which economic policy is increasingly subordinated to security considerations, including energy independence, technological sovereignty and the protection of critical infrastructure

The empirical basis of the study consists of official macroeconomic and structural data from Eurostat, the European Commission, The Organisation for Economic Cooperation and Development (OECD, 2025), the World Bank, Ukrstat (State Statistics Service of Ukraine, 2026) and others. The dataset includes indicators of economic growth, inflation, labour market dynamics, fiscal balances, public debt, energy prices, trade flows and indices of economic uncertainty for the period 2014–2025, with a particular emphasis on the post-2022 phase, which reflects the accelerated transformations caused by the full-scale war in Ukraine.

In addition to statistical data, the study relies on analytical reports and strategic policy documents, including the World Economic Forum's Global Risks Reports for 2023–2025 (Elsner et al., 2025), official EU macroeconomic forecasts and materials related to industrial policy, energy security, economic governance and strategic autonomy. The study also employs the extrapolation method to identify trends in economic uncertainty and the strategic planning method to determine potential future scenarios for the development of the European economic environment: adaptive differentiation, security-oriented consolidation and strategic economic reconfiguration. These scenarios are constructed on the basis of observed policy trends, institutional constraints, and geopolitical conditions.

This integrated methodological approach enables a multidimensional assessment of the challenges facing the European economy and provides an analytical basis for policy-relevant conclusions on economic resilience, strategic autonomy and prospects for cooperation with Ukraine during and after the war.

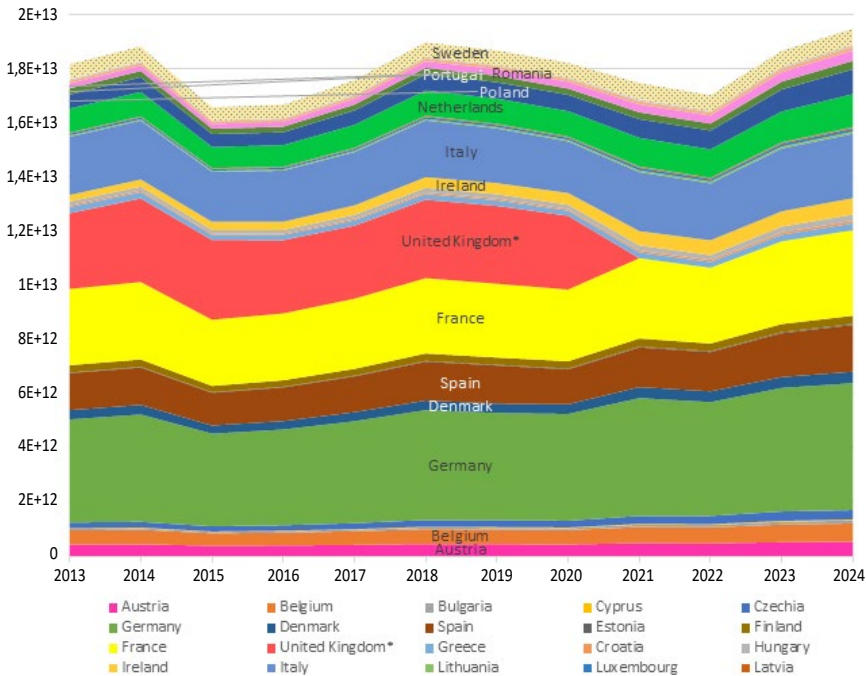
Results

Since 2014, the macroeconomic dynamics of the European Union have been characterized by several waves of crisis that have successively changed the trajectory of economic growth and undermined the potential for long-term development. The period from 2014 to 2016 was marked by the first geopolitical shock related to the annexation of Crimea and the start of the war in eastern Ukraine. Although the direct macroeconomic impact on the European Union cannot be attributed solely to the outbreak of the war in Ukraine, given that it was not the only factor behind the decline in EU GDP, the onset of the conflict marked the beginning of a gradual deterioration in investment expectations, accompanied by heightened geopolitical risks and increased economic uncertainty, particularly in the sphere of international trade. The introduction of the first sanctions against Russia (Council of the European Union, 2025a) coincided with the development of a strategy aimed at diversifying export markets for goods and raw materials. Together with the persistent sovereign debt problems of several southern EU-countries, these factors contributed to a deceleration of economic growth during the period 2014–2019 (Figure 1).

The next sharp negative shock was the COVID-19 pandemic in 2020, which led to the deepest economic recession in the EU since World War II, that is -5.6% of GDP in 2020 according to Eurostat and the World Bank's Open Data (World Bank Group, 2026). The recovery in 2021 was rapid but largely based on fiscal and monetary stimulus, making it vulnerable to subsequent challenges. The data in Figure 1, which show the dynamics of EU GDP structured by individual EU member states, confirm that the period after 2014 was characterized not by a sharp decline, but by a slowdown in growth dynamics in the EU. After the initial geopolitical shock associated with the annexation of Crimea and the start of the war in eastern Ukraine, EU GDP continued to grow in nominal terms, but the pace of growth slowed significantly in 2014–2016, reflecting the onset of a phase of heightened uncertainty.

The data in the figure also show the economic heterogeneity of EU member states and their corresponding vulnerability. The major economies, notably Germany, France, Italy and the United Kingdom, continue to account for the largest share of aggregate GDP and largely determine the overall trajectory of the EU's economic development. At the same time, the relatively subdued dynamics of some southern EU countries (e.g. Portugal and Spain) are evident. The decline in GDP in 2020 is clearly visible in almost all member states, confirming the systemic nature of the shock caused by COVID-19. The scale and synchrony of the decline distinguish the recession caused by the pandemic from previous shocks related to geopolitical tensions.

Figure 1. Dynamics of Gross Domestic Product of EU Member States, measured in current US dollars, 2013–2024



* Here: United Kingdom is included in the EU GDP prior to Brexit (including the transition period).

Source: authors' own work based on World Bank Group (2026).

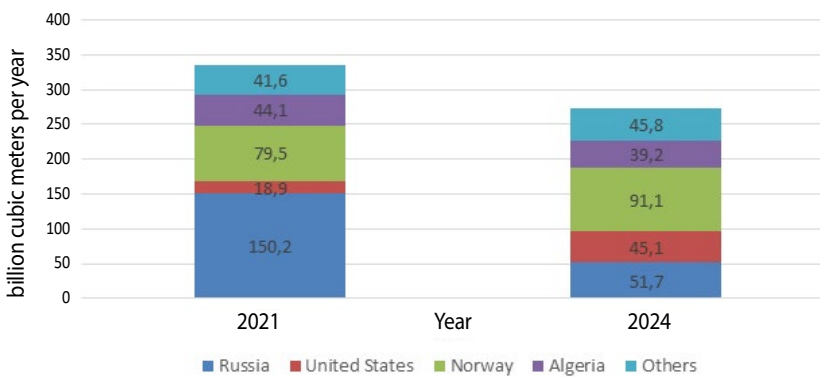
The subsequent recovery in 2021–2022 was driven by fiscal and monetary measures rather than a return to stable long-term growth fundamentals. The dynamics after 2022 point to a new phase of transformation in the European economic environment. Although aggregate GDP is recovering and even exceeding pre-pandemic levels, growth appears increasingly uneven and unstable. This reflects the cumulative impact of numerous cross-cutting shocks, the consequences of the pandemic, the renewed escalation of the war in Ukraine, energy price volatility and the restructuring of trade and supply chains. In this sense, Figure 1 visually reinforces the main thesis of the study: the war in Ukraine is not so much an isolated shock as a catalyst for long-term structural changes that are reshaping investment patterns, sectoral composition and future trajectories of the EU economy.

Russia's full-scale invasion of Ukraine in 2022 was a qualitatively new macroeconomic shock that combined energy, inflationary and geo-economic dimensions. It was at this point that the EU's GDP growth trajectory entered a phase of structural slowdown, reflected in subdued growth in 2023–2025.

In contrast to previous crises, such as the global financial crisis of 2008–2009 or COVID-19, the challenge facing the EU in connection with Russia's full-scale

military invasion of Ukraine has a clear geo-economic and security dimension. The combination of economic and security factors has forced the EU to rethink its development model, which until 2022 was based on a high level of global interdependence, prioritizing market efficiency and minimizing costs. Before the full-scale war began, the European economy was heavily dependent on imports of relatively cheap Russian energy resources, which was considered economically rational within the neoclassical model. In 2021, Russia accounted for approximately 40% of natural gas imports to the EU and about 25% of oil imports (Figure 2).

Figure 2. EU gas imports by country, billion cubic metres per year, 2021–2024



Source: authors' own work based on: Council of the European Union, 2025b.

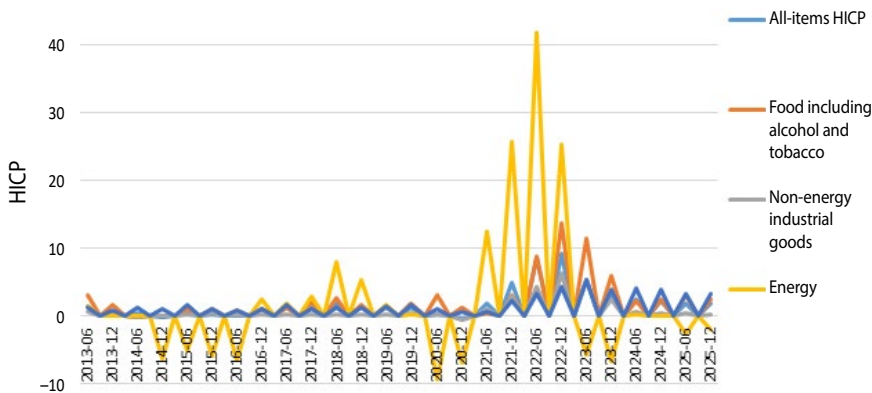
The data presented in Figure 2 illustrate a profound structural shift in the composition of EU gas imports between 2021 and 2024, directly reflecting the geo-economic consequences of Russia's full-scale invasion of Ukraine and the subsequent reorientation of European energy policy. In 2021, Russia was by far the dominant supplier of natural gas to the EU, accounting for approximately 150 billion cubic metres per year, which underscores the scale of the EU's pre-war energy dependence. By 2024, Russian gas imports had declined dramatically to about 52 billion cubic metres, indicating a sharp and deliberate reduction driven by sanctions, and strategic policy decisions aimed at enhancing energy security. This contraction represents not merely a cyclical adjustment but a structural geopolitical shift in the EU's external energy relations. At the same time, the figure shows a substantial increase in gas imports from alternative suppliers. Imports from the United States more than doubled between 2021 and 2024, reflecting the rapid expansion of liquefied natural gas (LNG) deliveries and the growing role of transatlantic energy ties.

Norway has further strengthened its position as a key player in the EU gas market and is characterized as a "relatively stable supplier", becoming the largest source of gas imports to the EU by 2024. Supplies from Algeria and other sources also remain

significant, confirming the EU's continued strategy of diversifying its energy portfolio. This rapid change in gas supply routes and partners can be interpreted as a direct response to increased geopolitical and security risks. While this reconfiguration has reduced the EU's strategic vulnerability to a single dominant supplier, it has also created new challenges, including higher import costs, greater vulnerability to global LNG market volatility, and infrastructure constraints. In this sense, the data in Figure 2 provide empirical evidence that the war in Ukraine has transformed energy dependence from a choice driven by efficiency into a central dimension of systemic economic risk management. Thus, the restructuring of EU gas imports confirms a shift from efficiency-driven energy dependence towards a security-oriented and risk-sensitive energy model.

The energy factor played a key role in the large-scale inflationary processes in the EU. Until 2021, inflation in the EU remained relatively moderate, reflecting weak aggregate demand and relatively stable energy prices. From 2021 onwards, and especially after Russia's full-scale military invasion of Ukraine in 2022, sharp volatility in gas, oil and electricity prices became the main source of inflationary pressure (Figure 3).

Figure 3. HICP Inflation in the European Union amid the War in Ukraine: Energy Dependence, Transmission Channels, and Uncertainty, 2013–2025



Source: authors' own work based on Eurostat (2026).

Energy prices directly shaped the dynamics of consumer inflation and were indirectly transmitted through rising production costs, particularly in energy-intensive sectors of the economy. In 2024–2025, the energy component remained a key source of uncertainty for inflation forecasts, a point repeatedly emphasized in analytical materials of the European Central Bank. Inflation driven by the energy shock had pronounced distributional effects. In 2022–2023, increases in the cost of living outpaced the growth of nominal wages, leading to a decline in real household incomes. In 2024–2025, the recovery of purchasing power remained incomplete due to the

inertial nature of price shocks. At the same time, persistently high energy costs negatively affected the price competitiveness of the EU economy, particularly in industrial sectors, constraining export potential compared with countries that have access to cheaper or more diversified energy sources. This indicates that inflation in the EU has become increasingly driven by structural and external factors rather than cyclical demand dynamics.

Between 2014 and 2025 EU fiscal policy also underwent significant changes under the influence of security-related and macroeconomic shocks. After 2014, defence spending gradually increased but remained restrained until 2021 amid fiscal consolidation. After 2022, a qualitative shift occurred: Russia's war against Ukraine triggered a large-scale and sustained increase in defence expenditures across EU countries, as well as substantial spending on military and financial support for Ukraine. In 2024, total defence spending by EU member states reached approximately €343 billion, indicating a long-term change in budgetary priorities. At the same time, governments expanded social programmes to mitigate the impact of inflation and the energy crisis on households and businesses. This, together with the legacy of the COVID-19 pandemic, sustained high levels of budget deficits and public debt. Although deficits gradually declined in 2024–2025, the debt burden remained elevated, particularly in southern EU countries, constraining fiscal space and increasing sensitivity to rising interest rates. This reflects a broader transformation of fiscal policy from a framework of discipline and consolidation towards one focused on stabilization and security-oriented intervention.

Russia's full-scale war against Ukraine has also placed a heavy burden on the social systems of European Union countries, primarily due to large-scale forced migration flows. As of 2024, approximately 6.8 million people had been registered as receiving temporary protection in EU countries (5,310,800 of whom were from Ukraine (UNHCR, 2026, Regional data). The financial consequences of this transformation are systemic. According to European Commission estimates, the costs associated with supporting Ukrainian refugees within the EU alone amounted to approximately €17 billion, not including macro-financial assistance to Ukraine and defence support costs. At the same time, beyond fiscal and social pressures, the inflow of Ukrainian refugees has had a significant impact on labour markets across the European Union. While the initial phase of integration has been constrained by language barriers, recognition of qualifications and skill mismatches, these challenges reflect broader structural adjustments within host economies. In many EU member states, particularly those facing demographic ageing and labour shortages, Ukrainian migrants represent an important source of human capital that can support labour market stabilization and economic resilience. Over time, their integration is facilitated through institutional support mechanisms, education systems and the development of socio-economic networks, which enhance employment opportunities and accelerate adaptation processes.

From a longer-term perspective, migration should therefore be viewed not only as a cost factor but also as a potential driver of labour market renewal and economic sustainability. In line with migration theory, the possibility of return migration remains significant, suggesting that the current redistribution of human capital may generate positive spillovers for both the European Union and Ukraine in the post-war period. At the same time, the war has been a catalyst for an energy shock that has forced EU governments to roll out large-scale compensation programmes for households and businesses. The total amount of fiscal measures aimed at mitigating the rise in energy prices is estimated at approximately €540 billion, which is one of the largest examples of countercyclical government intervention in the history of the EU (Sgaravatti et al., 2023).

Energy subsidies reveal the structural nature of the challenge: they rose from €213 billion in 2021 to €397 billion in 2022 and remained very high at €354 billion in 2023, reflecting strong fiscal inertia. IMF estimates show that the 2022 surge in fossil fuel prices increased the cost of living for European households by nearly 7% on average, with low-income households most affected, deepening inequality. Over the medium term, this poses a dual challenge for EU resilience, combining higher social spending with demographic ageing (European Commission, 2025a).

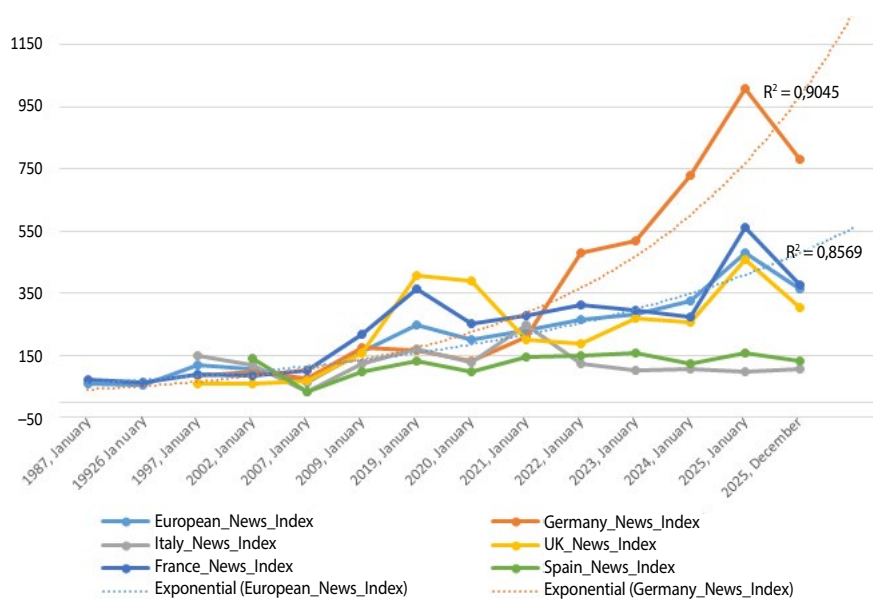
With the onset of Russia's invasion of Ukraine, the European Union also faced new political, economic and cyber-economic challenges that exposed the deep interconnections between social stability, economic security and digital resilience. Socio-economic pressures associated with the rising cost of living, together with the broader consequences of the war, are increasingly translating into political risks – most notably societal polarization and uneven support for EU foreign policy. The cyber threat environment in EU countries has changed significantly over the past decade, elevating cyber-attacks to the level of economic warfare. The ENISA Threat Landscape 2024 report, published by the European Union Agency for Cybersecurity, reports more than 11,000 cyber incidents in 2023–2024, targeting mainly the public sector, transport and financial services (ENISA, 2024). Disruptions in these closely linked sectors have significant knock-on effects, increasing transaction costs and embedding “cyber risk costs” into corporate economic behaviour strategy, which limits investment and innovation.

In response, the European Union has accelerated the strengthening of its regulatory framework for digital resilience. NIS2 Directive: securing network and information systems, created in 2022 and implemented in 2024, expanded mandatory cybersecurity obligations across critical sectors, while the Digital Operational Resilience Act (DORA), applicable from 17 January 2025, harmonized ICT risk management in the financial sector. Alongside the Critical Entities Resilience Directive, these measures reflect a strategic shift from cost efficiency towards systemic reliability. The war in Ukraine has thus acted as a catalyst for reasserting digital sovereignty and

embedding cyber resilience at the core of European economic governance under conditions of heightened geopolitical and internal stress.

From the above, we can conclude that the war in Ukraine has exposed the strategic vulnerabilities of the EU's economic model, in particular by turning energy dependence into a major source of socio-economic risk and a factor in increasing macroeconomic instability. These circumstances have significantly increased economic uncertainty in all European countries, exacerbating existing social pressures and strengthening the link between geopolitical tensions, economic security, and sustainability. This dynamic is clearly reflected in the Economic Policy Uncertainty (EPU) for major European economies and the United Kingdom. Since 2022, the index has shown a marked and sustained upward trend, with particularly strong growth observed in Germany and in the aggregate European news-based index (Figure 4).

Figure 4. Economic uncertainty in Europe and selected European countries based on the Economic Policy Uncertainty (EPU) index, 1987–2025



Source: authors' own work based on Economic Policy Uncertainty (2026).

The level of economic uncertainty in 2024–2025 exceeds that observed during both the global financial crisis and the COVID-19, underscoring the uniqueness of the war as a shock that combines economic, geopolitical and security risks. The highest EPU values are recorded in Germany (the EU's key industrial economy and the country most dependent on the pre-war energy model), which helps explain the scale of state intervention and anti-crisis measures undertaken there. Therefore, rising

economic uncertainty should be interpreted not as a temporary fluctuation but as a structural feature of the EU's ongoing economic transformation.

The rise in economic uncertainty is closely linked to the structural transformation of the EU energy sector. The nearly threefold reduction in imports of Russian gas between 2021 and 2024, alongside a rapid increase in supplies from the United States, Norway and other sources, marked a shift towards a more expensive but significantly more secure energy supply model. This transition became one of the main drivers of inflationary pressures, heightened volatility in commodity and financial markets, and increased expected uncertainty, all of which are reflected in the dynamics of the EPU index. In response to the energy shock and elevated uncertainty, EU member states substantially expanded the role of fiscal and regulatory policy. Large-scale support packages for firms and households, notably Germany's anti-crisis measures amounting to approximately €200 billion, served not only as tools of short-term macroeconomic stabilization but also as mechanisms for managing social and political risks. In this context, persistently high EPU levels function not merely as indicators of crisis intensity but also as explanatory factors behind the EU's gradual departure from a neoliberal paradigm in favour of a more active and strategic role of the state in the economy.

At the same time, by 2024 the European Union had implemented an unprecedented sanctions regime against the Russian Federation. As already mentioned in this study, restrictive measures had been imposed on more than 2,700 individuals and legal entities (Council of the European Union, 2025a). The combination of sanctions and elevated economic uncertainty has effectively precluded a return to the pre-war model of economic relations and reinforced long-term structural shifts. Persistently high EPU values between 2023 and 2025 indicate a transformation not only of current economic conditions but also of the expectations of economic agents. Businesses, investors, and governments increasingly prioritize resilience, diversification and security considerations over cost minimization, a shift that is institutionally reflected in the activation of EU industrial policy, including the adoption of the European Chips Act and the relaxation of state-aid rules.

Thus, the war in Ukraine constitutes a deep systemic exogenous shock whose consequences for the European Union's economy are long-lasting and structural. The dynamics of the Economic Policy Uncertainty index confirm that the EU has entered a phase of structural uncertainty associated with the transition towards a new geo-economic development model. The shift from a logic of economic efficiency to a logic of security, the expansion of the state's role and the pursuit of strategic autonomy are shaping a new development trajectory in which stability is achieved not through cost minimization but through the reduction of systemic risks and the strengthening of economic resilience. Unlike the crises of 2008–2009 and the COVID-19 pandemic, the consequences of Russia's full-scale invasion are persistent and complex, combining

economic, geopolitical and security factors. Prolonged economic uncertainty, the restructuring of energy chains and increased defence and social spending signal an irreversible change in the European development model and significantly limit the applicability of traditional forecasting approaches. In this context, we have identified the following scenarios for interpreting the possible trajectories of the European Union's further development.

Scenarios for the development of European Union economies

1. Adaptive differentiation.

The adaptive differentiation scenario envisages the preservation of internal heterogeneity within the European Union, with increased asymmetry in economic development between countries and regions. According to this logic, Member States adapt to the consequences of war and geo-economic fragmentation at different speeds and with different instruments, depending on their fiscal space, energy structure and institutional capacity. In theory, this scenario echoes the concept of a “multi-speed Europe”, which has been discussed since the 1970s within the theory of differentiated integration (Schimmelfennig et al., 2014). In economic terms, this means that the northern and western EU countries are recovering faster, while the southern and some eastern European economies remain in a mode of structural adjustment. Under this scenario, the EU retains common markets and institutions, but without a radical strengthening of supranational coordination. The risk is a gradual deepening of economic fragmentation and social inequality, which could undermine the long-term political cohesion of the European Union.

2. Security-Oriented Consolidation.

The second scenario, security-oriented consolidation, assumes that the war in Ukraine accelerates the transformation of the European Union into a more centralized and coordinated economic actor, driven by security imperatives. In this case, economic policy is increasingly subordinated to strategic objectives, such as energy security, defence readiness and protection of critical infrastructure. Historically, this trajectory resembles post-war European reconstruction in the late 1940s and early 1950s, when economic integration was explicitly linked to security concerns through mechanisms such as the Marshall Plan and the European Coal and Steel Community. From a theoretical perspective, this scenario aligns with Keynesian-institutionalist (Keynes, 2007, pp. 112–115) of crisis-driven state expansion. Under security-oriented consolidation, the EU strengthens common fiscal instruments, coordinates industrial and defence policies, and relaxes traditional competition rules for strategic sectors. However, this model also entails trade-offs, including higher public debt, increased regulatory intervention and potential efficiency losses in the private sector.

3. Strategic Economic Reconfiguration.

The third scenario, strategic economic reconfiguration, represents the most transformative pathway. It assumes that the war in Ukraine acts as a historical turning point leading to the deliberate construction of a new European economic model centred on strategic autonomy, technological sovereignty and geoeconomic competitiveness. This scenario is grounded in contemporary geoeconomic theory, notably the work of Blackwill and Harris (Blackwill & Harris, 2016), which conceptualizes economic instruments as tools of strategic power in an era of intensified geopolitical rivalry. Empirically, it is supported by the EU's shift towards active industrial policy, the expansion of strategic investment programmes and the prioritization of resilience over cost minimization. Strategic economic reconfiguration implies a long-term reorientation of growth drivers, deeper integration of security and economic planning, and the repositioning of Europe within a fragmented global economy. While potentially enhancing systemic resilience, this trajectory requires substantial political consensus, sustained investment and acceptance of higher short-term adjustment costs.

Alternative Scenarios for Ukraine and Europe

1. Scenario of a Ukrainian Victory.

Ukrainian victory would create conditions for large-scale post-war reconstruction and integration, structurally comparable to post-war Western Europe. For the EU, this would reduce long-term security risks and allow Ukraine to become a driver of economic growth, particularly in energy, agriculture and defence-related industries.

2. Scenario of a Temporary Truce or Frozen Conflict.

A temporary ceasefire or a frozen conflict would lead to a prolonged state of geopolitical uncertainty without a definitive resolution to the war. Under such a scenario, economic and security risks would remain high, limiting investment and slowing the reconstruction process. The European Union would maintain high levels of defence spending and continue to provide financial support to Ukraine for the sake of overall security in the region, operating in an environment of constant instability and fragmented economic relations.

3. Scenario Unfavourable to Ukraine.

An outcome unfavourable to Ukraine would represent a systemic shock to the European security order, undermine international norms and reinforce global fragmentation. Europe would face prolonged militarization, heightened uncertainty and structurally lower growth prospects.

In all scenarios, the war in Ukraine has irreversibly changed and will continue to change the trajectory of Europe's development. Economic policy can no longer be

separated from security considerations, and sustainability has become a fundamental principle of the European model. Europe's future will depend not on restoring the pre-war status quo, but on its ability to manage uncertainty, review strategic priorities and integrate Ukraine into a renewed economic and security structure.

Conclusions

This study demonstrates that the war in Ukraine has become not merely another external disturbance for the European Union, but a systemic and long-term exogenous shock that has accelerated the transformation of the European economic model. Unlike previous crises, its effects combine macroeconomic, geopolitical, energy, social and security dimensions, thereby reshaping the foundations of economic governance in Europe. The empirical evidence presented in this article confirms that the EU is moving away from a model based primarily on efficiency, cost minimization and deep external dependence towards one structured around resilience, diversification and strategic autonomy.

The analysis shows that this transformation is most clearly visible in four interconnected areas: the restructuring of energy dependence, the persistence of inflationary and fiscal pressures, the rise of structural economic uncertainty, and the growing integration of security considerations into economic and regulatory policy. In this sense, the war has not only intensified existing vulnerabilities, but also redefined the hierarchy of policy priorities within the EU. Energy security, industrial policy, critical infrastructure protection and digital resilience are no longer supplementary policy areas, but central components of the Union's future development model.

At the same time, the study indicates that the consequences of the war are unevenly distributed across member states, reinforcing internal differentiation within the EU. This asymmetry increases the risk of fragmentation, but also creates pressure for stronger coordination at the supranational level. The future trajectory of the European Union will therefore depend on its capacity to reconcile national diversity with common strategic objectives, especially in the fields of fiscal policy, industrial development, defence and labour market adaptation.

Particular importance should be attached to the socio-economic dimension of these changes. The migration of Ukrainians to EU countries has created immediate fiscal and social challenges, yet it also represents a structural source of labour market adaptation and human capital renewal. In the longer term, the interaction between refugee integration, return migration and post-war reconstruction may become one of the key channels linking the future development of Ukraine and the European Union.

Among the scenarios examined in this article, strategic economic reconfiguration appears to be the most transformative and analytically convincing trajectory. It best reflects the observable shift towards a security-oriented, state-supported and strategically

coordinated economic order. Although this path entails substantial costs and political constraints, it also offers the greatest potential for strengthening long-term resilience under conditions of continued geopolitical instability.

Overall, the war in Ukraine should be understood as a turning point in the evolution of the European economic environment. The central conclusion of this study is that the future of the European Union will depend not on restoring the pre-war status quo, but on its ability to institutionalize a new balance between economic efficiency and security, while integrating Ukraine into a renewed European economic and security architecture.

References

- Adolfson, J., Kuik, F., Magdalena, E., Schuler, T. (2022). The impact of the war in Ukraine on euro area energy markets. *ECB Economic Bulletin*, 4. https://www.ecb.europa.eu/press/economic-bulletin/focus/2022/html/ecb.ebbox202204_01~68ef3c3dc6.en.html [accessed: 24.12.2025].
- Baker, S.R., Bloom, N., Davis, S.J. (2016). Measuring Economic Policy Uncertainty. *The Quarterly Journal of Economics*, 131(4), 1593–1636. <https://doi.org/10.1093/qje/qjw024>
- Blackwill, R., Harris, J.M. (2016). *War by Other Means: Geoeconomics and Statecraft*. Harvard University Press. <https://doi.org/10.2307/j.ctt1c84cr7>
- Council of the European Union. (2025a). *Sanctions against Russia*, <https://www.consilium.europa.eu/en/topics/russia-s-war-against-ukraine/> [accessed: 10.01.2026].
- Council of the European Union. (2025b). *Where does the EU's gas come from?* <https://www.consilium.europa.eu/en/infographics/where-does-the-eu-s-gas-come-from/> [accessed: 10.01.2026].
- Economic Policy Uncertainty. (2026). *Monthly EPU Indices for 22 Countries*, https://www.policyuncertainty.com/all_country_data.html [accessed: 10.01.2026].
- Elsner, M., Atkinson, G., Zahidi, S. (2025). *Global Risks Report 2025*, World Economic Forum, 15.01.2025. <https://www.weforum.org/publications/global-risks-report-2025/> [accessed: 10.01.2026].
- ENISA. (2024). *ENISA Threat Landscape 2024. July 2023 to June 2024*. https://www.securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf [accessed: 11.01.2026].
- European Commission. (2025a). *Energy subsidies report shows progress in 2023*, European Commission, 29.01.2025. https://energy.ec.europa.eu/news/energy-subsidies-report-shows-progress-2023-2025-01-29_en [accessed: 10.01.2026].
- European Commission. (2025b). *The cost of EU Member States' proximity to the war*, European Commission, 17.11.2025. https://economy-finance.ec.europa.eu/cost-eu-member-states-proximity-war_en [accessed: 20.12.2025].
- Eurostat. (2026). *HICP (Harmonised Index of Consumer Prices) – monthly data (annual rate of change) (1997–2025)*. https://ec.europa.eu/eurostat/databrowser/view/prc_hicp_manr_custom_19665835/default/table [accessed: 10.01.2026].
- Federle, J., Meier, A., Müller, G., Mutschler, W., Schularick, M. (2024). *The Price of War*. CEPR Discussion Paper, no. DP18834. <https://cepr.org/publications/dp18834> [accessed: 20.12.2025].
- Keynes, J.M. (2007). *The General Theory of Employment, Interest, and Money*. Palgrave Macmillan.

- Nadin, V., Stead, D., Dąbrowski, M., Fernandez-Maldonado, A. (2021). Integrated, adaptive and participatory spatial planning: trends across Europe. *Regional Studies*, 55(5), 791–803. <https://doi.org/10.1080/00343404.2020.1817363>
- Knaap, G.-J., Nedović-Budić, Z., Carbonell, A. (Eds.). (2015). *Planning for states and nation-states in the U.S. and Europe* (pp. 259–497). Lincoln Institute of Land Policy.
- OECD. (2025). Resilient Growth but with Increasing Fragilities. *OECD Economic Outlook. Volume 2025, Issue 2*, https://www.oecd.org/en/publications/oecd-economic-outlook-volume-2025-issue-2_9f653ca1-en.html [accessed: 10.01.2026].
- Schimmelfennig, F., Leuffen, D., Rittberger, B. (2014). The European Union as a System of Differentiated Integration: Interdependence, Politicization and Differentiation. *IHS Political Science Series*, 137.
- Sgaravatti G., Tagliapietra, S., Trasi, C., Zachmann, G. (2023). *National fiscal policy responses to the energy crisis*, Bruegel, 26.06.2023. <https://www.bruegel.org/dataset/national-policies-shield-consumers-rising-energy-prices> [accessed: 10.01.2026].
- State Statistics Service of Ukraine (2026), <https://stat.gov.ua/uk/publications> [accessed: 10.01.2026].
- UNHCR. (2026). *Ukraine Refugee Situation*, The Operational Data Portal, <https://data.unhcr.org/en/situations/ukraine> [accessed: 11.01.2026].
- World Bank Group. (2026). *GDP (current US\$) – European Union*, <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU> [accessed: 10.01.2026].

The transformation of the European economic environment under the impact of the war in Ukraine: An analytical assessment of key challenges and future development trajectories

Abstract

This paper analyzes the transformation of the European economic environment under the impact of the Russian–Ukrainian war between 2014 and 2025, demonstrating that the war represents not a cyclical crisis but a systemic exogenous shock to the European Union's economic system. The study examines key macroeconomic and socio-economic effects, including the 2022 energy shock, inflation, economic uncertainty, and labour market adjustments related to migration flows. The results reveal an asymmetric impact across EU member states and increasing risks of internal fragmentation. The findings indicate an accelerated shift of the EU towards a geoeconomic development model based on resilience, strategic autonomy and the integration of economic and security policies.

Keywords: systemic shock, geoeconomic transformation, European Union economy, economic policy uncertainty, energy security transition, strategic autonomy, war-induced structural change, European transformation under stress

Author Contributions

Conceptualization: I.K., V.Y.

Methodology: I.K., V.Y.

Formal analysis: I.K.

Investigation: I.K.

Writing – original draft: I.K.

Writing – review & editing: I.K.

Visualization: I.K.

Supplementary Materials

Not applicable.

Funding

This research received no external funding.

Ethics Approval Statement

Not applicable. The study used publicly available secondary data and published sources and did not involve human participants.

Informed Consent Statement

Not applicable.

Data Availability Statement

The study is based on publicly available secondary data and published sources, which are cited in the article and listed in the references.

Declaration of Generative AI Use

No generative artificial intelligence tools were used in the preparation of this manuscript. The authors used DeepL to improve the language and readability of the manuscript. They subsequently checked and revised the text and accept full responsibility for the content of the published article.

Acknowledgments

Not applicable.

Conflict of Interest

The authors declare no conflicts of interest.

Civic engagement of Ukrainian forced migrants in Estonia: Key challenges and perspectives

Oksana Pyatkovska

PhD, International Institute of Education, Culture and Diaspora Relations
of Lviv Polytechnic National University; 2024/2025 Fellow of the Virtual Ukraine Institute
for Advanced Study (VUIAS)
<https://orcid.org/0000-0003-1859-4233>

Introduction

The full-scale Russian invasion of Ukraine, which occurred in 2022, caused an unprecedented wave of forced emigration from Ukraine, which reached almost 6 million people globally, among whom more than 5 million found international protection in European countries (UNHCR, 2025). As of March 2025, 65,335 Ukrainian forced migrants had applied for temporary protection in Estonia, with 42,550 officially recorded in this country (Eurostat, 2025a), making it the third-largest EU receiving country in relative terms, i.e. in terms of the number of Ukrainians with temporary protection per 1000 residents (Eurostat, 2025b).

Furthermore, the Ukrainian migration to Estonia, which had a long history before 2022, made Ukrainians the second-largest national minority group in this country (Minority Rights Group International, 2024). According to Estonian statistics, the number of people of Ukrainian ethnicity in 2025 reached 73,597, which means that the number of Ukrainian forced migrants (UFMs) is significantly higher than the number of Ukrainians that lived in Estonia before 2022 (Statistics Estonia, 2025). Taking only the sheer numbers into consideration, we can assume that the newcomers

have a significant effect on Ukrainian community building as well as the development of Ukrainian diaspora organizations in Estonia.

At the same time, Ukrainian community building in Estonia before 2022 was characterized by several challenges and problems. Prior to 2022, Ukrainian diaspora organizations struggled with low engagement, as their activities reached only a small minority of the community despite a long history and state funding (Kasianczuk, 2022). Community development was significantly hindered by internal institutional issues, including conflicts of interest, a lack of transparent internal policies and visible competition between organizations. Furthermore, political disagreements and a focus on self-promotion among some leaders also contributed to social fragmentation and a general sense of dissatisfaction among community members (Kasianczuk, 2022).

The aim of this article is to examine the key challenges and prospects of civic engagement among UFM in Estonia and to analyze their potential impact on the processes of Ukrainian community building within the host country.

Literature Review

The concept of “civic engagement” has gained prominence over the past three decades as an important topic in developmental science. Much has been learnt about what civic engagement means, how it is measured and how people develop civic engagement. In particular, P. A. Arvanitidis (2017), through an analysis of recent literature, shows that civic engagement is a complex multidimensional concept, taking multiple forms and encompassing a variety of behaviours and actions related to both political and social aspects. Accordingly, civic engagement refers to how an active citizen participates in the life of a community in order to improve conditions for others or to help shape the community’s future, including wide-ranging activities undertaken alone or in concert with others designed to identify and address issues of public concern. Other scholars, e.g. Jonathan F. Zaff et al. (2010), who consider the definition of civic engagement, provide insights into trends of civic engagement over the past 30 years, disentangle the various competing theories on the development of civic engagement, and subsequently place the development of civic engagement within a development systems lens.

Scholars pay special attention to various aspects of the civic engagement of immigrants. By analyzing some of them we can capture several key research findings that have emerged over the past years. The results of these studies often focus on the following key parameters: factors that influence immigrants’ motivations to participate in civic life, especially in the process of integration (Aleksynska, 2011; Vogel & Triandafyllidou, 2005; Cappiali, 2015; Maidanik, 2025a; Voicu & Rusu, 2012), the forms of participation migrants engage in (Maidanik, 2025b; Pajnik & Bajt, 2013), and reasons for the development of migrants’ associations (Caselli, 2009).

Methodology and Data

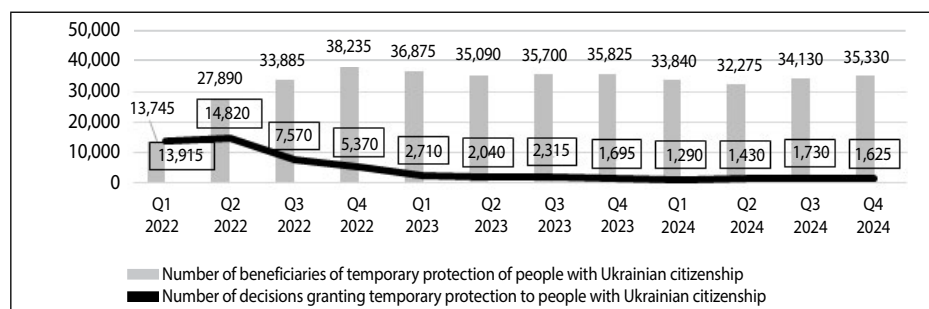
This paper is based on secondary data analysis and two online surveys (quantitative and qualitative) conducted by the International Institute of Education, Culture and Diaspora Relations of Lviv Polytechnic National University (IIEC). The quantitative part of the study was carried out among adult (18 years and older) Ukrainian migrants who had been forced to leave Ukraine for Estonia due to Russia's full-scale invasion and were residing in this country at the time of the survey. Information was collected using an online survey based on the Computer-Assisted Web Interviewing (CAWI) method, implemented through a pre-coded Google Forms questionnaire designed for self-completion. The survey was conducted in April 2024 and the number of the respondents was 112 (91.1% of whom had moved to Estonia during 2022). A key limitation of the study is that the survey is non-representative and is intended to describe the current situation rather than to identify causal relationships. The questionnaire allows general trends in respondents' answers to be traced; the findings cannot be generalized to the broader population of Ukrainian forced migrants in Estonia.

The qualitative component consisted of in-depth semi-structured interviews with representatives of Ukrainian non-governmental organizations (NGOs). The fieldwork for this component lasted from June to September 2024. During this period, 12 interviews were conducted with leaders and activists of Ukrainian diaspora organizations (type 1), Ukrainian forced migrants who joined the activities of these organizations (type 2) and leaders and activists of Ukrainian organizations established after the onset of the war (type 3). To identify the participants, the snowball sampling method was used. In addition, respondents were recruited with the support of IIEC's research partner, the Association of Ukrainian Organizations in Estonia. Interviews were conducted remotely via the platform Zoom. The questionnaire consisted of thematic blocks and contained more than 30 questions, which were adapted to the specifics of each of the three types of respondents listed above. The key limitations of the qualitative study component are as follows: (1) in-depth interviews captured the subjective experiences, views and assessments of individual respondents, i.e. representatives of officially registered NGOs, and therefore entail certain limitations in terms of objectivity and interpretative generalization, and (2) the qualitative sample includes leaders and activists of Ukrainian NGOs in Estonia primarily engaged in cultural and educational activities, while organizations of other orientations (e.g. volunteer groups supporting the Ukrainian army, non-formal activists etc.) are not represented. Thus, the use of the snowball sampling approach and engagement of the partner organization in Estonia lead to selection bias and a relatively homogeneous sample, as respondents and partners tend to recruit participants from their own social and organizational networks.

Migration Dynamics

Analyzing the dynamics of temporary protection beneficiaries and corresponding administrative decisions concerning individuals with Ukrainian citizenship in Estonia over the period from the first quarter of 2022 to the fourth quarter of 2024, we can see that at the initial stage of the full-scale Russian invasion of Ukraine (Q1–Q2 2022), Estonia experienced a rapid and substantial inflow of Ukrainian nationals seeking temporary protection (Fig. 1). The number of beneficiaries increased almost twofold, i.e. from 13,745 in Q1 2022 to 27,890 in Q2 2022, reflecting the country's immediate humanitarian response and the large-scale displacement triggered by the onset of hostilities (Fig. 1). The number of decisions granting protection peaked in Q2 2022 (14,820), which confirms the administrative system's intensive engagement during the crisis's acute phase. The total number of beneficiaries continued to grow throughout 2022, reaching its highest level in Q4 2022, i.e. 38,235 persons (Fig. 1). During 2023–2024, the total number of beneficiaries remained relatively stable within the range of approximately 32,000–36,000 individuals, indicating a consolidation of the displaced population already present in the country. At the same time, the number of new protection decisions declined sharply: from 7,570 in Q3 2022 to fewer than 2,000 per quarter by 2024 (Fig. 1). This divergence between the relatively stable stock of beneficiaries and the declining number of new administrative decisions suggests a transition from the emergency reception phase towards a period characterized by longer-term residence and integration of Ukrainian displaced persons in Estonia. By the end of 2024, 35,330 Ukrainians remained under temporary protection in Estonia, which signifies sustained demographic presence and relative permanence of displacement (Fig. 1).

Figure 1. Dynamics of the number of beneficiaries of temporary protection and decisions granting temporary protection to people with Ukrainian citizenship in Estonia, 2022–2024, quarter data



Source: compiled by the author based on Eurostat, 2025a; 2025c.

By analyzing the demographic indicators of Ukrainians with temporary protection in Estonia, we observe a notable structural transformation between June 2022 and December 2024 (Table 1). During this period, the overall number of beneficiaries of temporary protection increased from 27,890 to 35,330 persons, indicating the continued arrival of displaced Ukrainians as well as the prolonged stay of those who had previously sought protection. At the same time, significant shifts occurred in the gender and age composition of the displaced population. In particular, the share of male beneficiaries increased from 30% to 38.8%, suggesting a sharp increase in the arrival of additional male cohorts after the initial predominantly female and child refugee wave (Table 1). The age structure of the Ukrainian population under temporary protection also demonstrates a gradual change: the proportion of migrants aged over 65 years rose from 4.9% to 6.2%, indicating aging of the displaced population, potentially due to an extended duration of stay and family reunifications involving older relatives. Conversely, the share of children under 18 decreased markedly: from 40% to 28.8%, and for those under 14 years – from 30.8% to 20.7% (Table 1). This trend may reflect the gradual return of families with children to Ukraine or their onward migration to other EU member states, as well as the stabilization of adult migrants' status in Estonia.

Table 1. Selected key demographic parameters of Ukrainian citizens with temporary protection status in Estonia, 2022, 2024

	June 2022	December 2024
total number of beneficiaries of temporary protection status	27,890	35,330
share of males	30%	38.8%
share of migrants over 65 years old	4.9%	6,2%
share of migrants under 18 years old	40%	28.8%
share of migrants under 14 years old	30.8%	20.7%

Source: compiled by the author based on Eurostat, 2025a.

Estonian Societal Openness to UFM

Analyzing how UFM perceive Estonian state policy and societal attitudes towards them following Russia's full-scale invasion of Ukraine in 2022, we observe that both the qualitative and quantitative surveys conducted by IIEC prove the multidimensional nature of openness and overwhelming positiveness, spanning governmental response, people's solidarity and support. In particular, the statements made by the respondents to the qualitative survey, such as "the Estonian state literally carried each refugee in its arms" and "created conditions not even 100%, but 120%", reveal a deep appreciation for Estonia's initial humanitarian response. This framing

presents the state not merely as an administrative entity, but as a moral actor embodying empathy and responsibility. In policy terms, Estonia's early response demonstrates solidarity-based governance, an approach that combines rapid institutional coordination with a humanitarian ethos. However, the same respondents also identify unintended consequences: the preferential treatment of Ukrainians relative to other minorities created perceptions of inequality. The observation that other minorities "wanted a parity basis" underscores the challenge of avoiding hierarchies of deservingness in refugee policy.

As to societal openness, 13.4% of UFM in Estonia assess the attitudes of Estonian society towards them as totally positive and 54.5% as positive. Only 4.5% considered it negative with less than 1% – totally negative. The remaining 26.8% assess it as neutral. Besides, the findings of in-depth interviews on public attitudes show strong initial solidarity from ethnic Estonians, exemplified by voluntary offers of accommodation and community support. Respondents attribute this empathy to shared historical memory, and more specifically to the collective trauma of Soviet domination. As one migrant notes, "Estonians remember their families' experiences with Russia, [...] so they understand the situation firsthand."

This alignment of historical narratives facilitates symbolic identification between host and receiving communities, reinforcing national self-conceptions rooted in resistance to Russian imperialism. It reflects what scholars term affective solidarity: emotional resonance grounded in parallel experiences of oppression. In the Baltic context, this form of solidarity operates as both a moral bond and a geopolitical statement of alignment with Ukraine's struggle.

Furthermore, it should be stressed that UFM experienced discrimination and negative attitudes predominantly in their interactions with Russians; this was pointed out by 48.2% of respondents to the quantitative survey carried out by IIEC. These specifics were also observed in the qualitative survey results:

Of course, there are some people who don't like this whole situation with Ukrainians coming here – mostly Russian-speaking Estonians. They've got their own propaganda, their own kind of pain, so we just don't pay attention to that. But the ethnic Estonians, who are the majority here, treat us really well and understand why this is happening, that we didn't just come here to live for no reason (forced migrant).

In this context it should be emphasized that Estonia's contemporary socio-political environment is strongly shaped by its historical experience and demographic structure. The country's collective memory of Soviet occupation, repression and mass deportations during the twentieth century has contributed to a persistent perception of security risks associated with Russian geopolitical ambitions, making Russia's war against Ukraine a matter of particularly close public and political attention (Ploom et al., 2025). At the same time, the Russian-speaking minority in Estonia, which constitutes around 21% of the population (Ploom et al., 2025), creates a complex societal

landscape in which differing historical narratives, information spaces and political attitudes generate tensions in public discourse and influence the broader context.

Only a small share of UFM (9.8%) experienced negative attitudes in their interactions with the Ukrainian community. This is also an important indicator when it comes to effective community building and civic engagement in Ukrainian diaspora organizations in Estonia.

Civic Engagement and Community-Building

Among the respondents to the IIEC's quantitative survey, more than half (55.4%) indicated that they had participated or continue to participate in the activities of Ukrainian NGOs in Estonia. Among the variety of events organized by Ukrainian diasporic associations that forced migrants attended during their stay in Estonia, cultural, religious and national-patriotic events prevail, which was reported by 68.8% of the respondents. Community initiatives supporting adaptation and integration were also significant: 59.7% received informational or legal aid, 31.2% humanitarian assistance, 28.6% psychological support, and 54.5% attended Estonian language courses. Moreover, 40.3% participated in political actions and marches promoting Ukraine's interests in Estonia. The least popular activities were Ukrainian language courses (6.5%) and volunteering (3.9%). Besides, UFM are generally satisfied with Ukrainian NGOs in Estonia; more than 60% rated their activities at seven or higher on a ten-point scale.

The in-depth interview respondents estimate that up to 20% of UFM engage in Ukrainian civic activities. They believe that newcomers' level of involvement in community activities depends mostly on their available time and emotional capacity: many are eager to contribute, but their ability can be limited by more important things, such as learning Estonian and job seeking, which highlights the tension between survival needs and social participation during the adaptation process:

Forced migrants are quite open to public activity. Those who have the strength and motivation to get involved do come and offer their help. There are many such people. A lot of people come to weave camouflage nets. It's a simple activity. [...] But when people start learning Estonian, looking for a job, then of course, they have less energy and fewer resources (diaspora).

They don't get involved very actively. Maybe 20%. And it's not because people don't want to, but because they find themselves in a foreign country and face challenges: housing, work. What kind of civic participation can they think about? They can think about how to survive and get by. Maybe they would like to get involved, but they don't have the resources, because after the war everyone is already exhausted (forced migrant).

Overall, the main barriers identified in the study, which can be analyzed on several levels, are the following:

1. Individual level:

- psychological consequences of war trauma and the reluctance to engage in activities that may evoke painful memories of the war;
- limited time resources, as well as difficulties related to financial constraints and the process of adaptation to the host-country;
- lack of experience or understanding of civic activism and NGO activities, as well as a limited internalization of civic and volunteering practices common in European civil society;
- a sense of paternalism among some forced migrants who became accustomed to receiving humanitarian assistance and may not immediately recognize the need for personal civic contribution:

Some people who arrived at the beginning of the war became accustomed to receiving everything for free and may not immediately realize the need to contribute themselves. For some, this understanding comes with time, they eventually see that it's time to get involved in civic activities, but for others, it never does (forced migrant).

2. Social level:

- insufficient sense of belonging to Ukrainian culture and limited willingness or ability to communicate in Ukrainian;
- negative or exclusionary attitudes of some Ukrainian diaspora organizations towards newly arrived forced migrants;
- tensions within the Ukrainian diaspora in Estonia, including institutional fragmentation and rivalry between two umbrella organizations.

3. Structural level:

- the absence of Ukrainian civic organizations or institutionalized associations of Ukrainians in some of the initial cities or localities where forced migrants first arrived, which restricts opportunities for early engagement and networking;
- limited dissemination of information about the activities, initiatives and thematic focus of Ukrainian civic organizations in Estonia.

4. Political level or specifics of broader socio-political context:

- external pressure of the Russian minority: the fear of Russian-linked hostility deters public activity and puts geopolitical constraints on local civic life; civic engagement in Estonian regions which are close to Russian border becomes a politically risky act:

People have become afraid of being active. Because it's about safety in our region. For example, during a recent city celebration, many parents refused to let their children perform, here in our town. [...] many choose to hide in their niche so they won't be seen. The town is small, everyone knows that we're Ukrainians, and we're constantly being watched. This creates discomfort and discourages community activity. And those who are afraid don't come. [...] This is due to the ties with Russia, which almost the entire population of the town still maintains (diaspora).

Despite the barriers and challenges to the involvement of UFM in civic activism and community building in Estonia, the surveys also revealed the following motivating factors that encourage them to participate in civic activities:

- the desire to help forced migrants to adapt, having gone through this difficult experience themselves;
- the opportunity for self-realization, self-development, expansion of the network of contacts and social circle;
- the realization that there is greater strength and broader opportunities in unity;
- a way to receive psychological support and help, a sense of unity with like-minded Ukrainians,;
- an effective way of socialization, a sense of home and support;
- a way of preserving national identity and the Ukrainian language;
- a sense of responsibility for Ukraine, a desire to unite to help the Motherland and the Armed Forces of Ukraine;
- the positive attitudes of Estonians and their help offered sincerely.

Thus, the findings underscore civic activism not merely as participation, but as a coping and adaptation strategy: migrants engage to regain control over their circumstances, establish social networks and reconstruct a collective identity. Their motivations range from altruism (helping others to adapt) to psychological support and national pride. These reflect both instrumental and expressive dimensions of civic engagement. These factors of civic engagement prove that Ukrainian migrants' participation fosters bonding ties (within the Ukrainian community) and bridging ties (with Estonians), thus engagement becomes both an act of resilience and an assertion of belonging in a host society.

As to the institutional framework of the civic engagement of UFM, the surveys (both quantitative and qualitative) show that they not only engage in existing Ukrainian NGOs, but also create their own. For example, the findings indicate that almost 11% are already planning to start a new NGO, and additionally, 34.8% expressed interest in founding such an association but are hindered by a lack of relevant skills and knowledge in this area. It is noteworthy that UFM engage not only in the activities of Ukrainian diaspora associations, but also participate in other non-governmental organizations. According to the survey data, 27.7% of respondents reported such involvement.

When considering the perspectives of Ukrainian community building in Estonia and the effect of UFM in this process, it should be stressed that approximately 20% of UFM are already active in civic initiatives, while another 11% plan to create NGOs. This quantitative insight points to a nascent yet rapidly expanding civic infrastructure. Forced migration, though initially disempowering, has stimulated organizational innovation within the Ukrainian diaspora. The emergence of new associations and the revival of dormant ones testify to the capacity of crisis to reinvigorate collective identity and social solidarity. Crucially, this transformation

extends beyond the Ukrainian community; by engaging with Estonian institutions, migrants contribute to transnational civic spaces that transcend national borders. Their activities support Ukraine materially and symbolically, while simultaneously fostering integration and intercultural dialogue within Estonia. However, in our opinion, the sustainability of this momentum remains contingent on three key factors: (1) the economic integration of war migrants, (2) organizational cooperation, primarily between Ukrainian diaspora umbrella institutions and then with newly created NGOs, and (3) the sense of Ukrainian identity among forced migrants.

Conclusions

The data concerning the dynamics of Ukrainian forced migration to Estonia for the period 2022–2024 suggest a transition from the emergency reception of large refugee cohorts in 2022 to a more stable demographic and administrative pattern by 2024. The displaced Ukrainian community in Estonia has evolved into a more settled and demographically mature group, with a slight increase in male representation and elderly beneficiaries. These transformations point towards processes of community stabilization, adaptation to host-country conditions and potential shifts from temporary protection towards longer-term residence or integration frameworks.

Estonia's response to the arrival of UFM's has been characterized by a high degree of societal openness and state-led humanitarian solidarity. Both policy measures and public attitudes demonstrate a broadly positive and empathetic stance, rooted in shared historical experiences and collective memory. However, such a supportive environment faces friction from the Russian-speaking minority who, influenced by Kremlin narratives, exhibit attitudes of open hostility, discrimination and social exclusion towards Ukrainians. Besides, the preferential focus on UFM's has also produced certain perceptions of unequal treatment among other refugees.

The civic engagement of UFM's in Estonia demonstrates both significant potential and notable challenges. On the one hand, their participation in Ukrainian and Estonian civil society organizations reflects emerging forms of resilience, self-organization and community solidarity. Civic activism serves not only as a means of adaptation and psychological coping but also as a vehicle for preserving national identity and fostering integration into Estonian society. On the other hand, numerous structural and psychosocial barriers, such as limited information, a lack of institutional presence in certain regions, psychological trauma, issues concerning the use of the Ukrainian language, intra-diaspora tensions and geopolitical pressures, continue to hinder broader participation.

Despite these constraints, a growing interest in creating new NGOs and forming collaborative networks indicates promising prospects for the development of a more cohesive and dynamic Ukrainian community in Estonia. The long-term sustainability

of this civic revival, however, depends on addressing core challenges: ensuring migrants' economic stability, enhancing civic competence and strengthening cooperation within the Ukrainian diaspora and with Estonian institutions.

References

- Aleksynska, M. (2011). Civic participation of immigrants in Europe: Assimilation, origin, and destination country effects. *European Journal of Political Economy*, 27(3), 566–585. <https://doi.org/10.1016/j.ejpoleco.2010.12.004>
- Arvanitidis, P.A. (2017). The concept and determinants of civic engagement. *Human Affairs*, 27(3), 252–272. <https://doi.org/10.1515/humaff-2017-0022>
- Cappiali, M.T. (2015). *Activism and participation among people of migrant background: Discourses and practices of inclusiveness in four Italian cities*, https://www.academia.edu/18999629/Activism_and_Participation_Among_People_of_Migrant_Background_Discourses_and_Practices_of_Inclusiveness_in_Four_Italian_Cities
- Caselli, M. (2009). Integration, participation, identity: Immigrant associations in the province of Milan. *International Migration*, 47(3), 58–79. <https://doi.org/10.1111/j.1468-2435.2009.00530.x>
- Eurostat. (2025a). *Beneficiaries of temporary protection at the end of the month by citizenship, age and sex*. https://doi.org/10.2908/MIGR_ASYTPSM
- Eurostat. (2025b). *Beneficiaries of temporary protection by citizenship – per thousand persons*. https://doi.org/10.2908/MIGR_ASYTPSPOP
- Eurostat. (2025c). *Decisions granting temporary protection by citizenship, age and sex - quarterly data*. https://doi.org/10.2908/MIGR_ASYTPFQ
- Kasianczuk, M.H. (2022). Hromadski orhanizatsii ukrainskoi diaspori v Estonii [Non-governmental organizations of the Ukrainian diaspora in Estonia]. *Ukrainskyi Sotsium [Ukrainian Society]*, 2(81), 144–154. <https://doi.org/10.15407/socium2022.02.144> [in Ukrainian]
- Maidanik, I. (2025a). Civic engagement as a tool for (re)integration of forced migrants from Ukraine. *Demography and Social Economy*, 61(3), 25–40. <https://doi.org/10.15407/dse2025.03.025>
- Maidanik, I. (2025b). Civic engagement of Ukrainian forced migrants abroad: Insights and implications. *Bezpieczeństwo: Teoria i Praktyka [Security: Theory and Practice]*, 1, 237–249. <https://doi.org/10.48269/2451-0718-btip-2025-1-015>
- Minority Rights Group International. (n.d.). *Ukrainians and Belarusians in Estonia*. <https://minorityrights.org/communities/ukrainians-and-belarusians>
- Pajnik, M., Bajt, V. (2013). Civic participation of migrant women: Employing strategies of active citizenship. In F. Anthias, M. Kontos, M. Morokvasić (Eds.), *Paradoxes of integration: Female migrants in Europe* (pp. 97–116). Springer.
- Ploom, I., Šliwa, Z., Haas, M. (2025). Lessons identified from Ukraine: The bid for the Estonian total defence concept. *Journal on Baltic Security*, 11(1), 58–87. https://doi.org/10.57767/jobs_2025_004
- Statistics Estonia. (n.d.). *Population, 1 January by year, sex, county and ethnic nationality*. https://andmed.stat.ee/en/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV0222U/table/tableViewLayout2
- UNHCR. (2025). *Ukraine refugee situation*. <https://data.unhcr.org/en/situations/ukraine>

- Vogel, D., Triandafyllidou, A. (2005). Civic activation of immigrants: An introduction to conceptual and theoretical issues. https://www.researchgate.net/publication/237300734_Civic_activation_of_immigrants_-_An_introduction_to_conceptual_and_theoretical_issues
- Voicu, M., Rusu, I.A. (2012). Immigrants' membership in civic associations: why are some immigrants more active than others. *International Sociology*, 27(6), 788–806. <https://doi.org/10.1177/0268580912452172>
- Zaff, J.F., Hart, D., Flanagan, C.A., Youniss, J., Levine, P. (2010). Developing civic engagement within a civic context. In *Handbook of life-span development* (Vol. 2). Wiley. <https://doi.org/10.1002/9780470880166.hlsd002015>

Civic engagement of Ukrainian forced migrants in Estonia: Key challenges and perspectives

Abstract

This article examines the challenges and prospects of civic engagement among Ukrainian forced migrants (UFMs) in Estonia and their impact on Ukrainian community building based on quantitative and qualitative surveys conducted by the International Institute of Education, Culture and Diaspora Relations of Lviv Polytechnic National University in 2024, as well as secondary data analysis. The article also presents the evolving dynamics of Ukrainian migration following Russia's full-scale invasion of Ukraine. The findings reveal that Estonia's response has been marked by notable openness and solidarity, fostering favourable conditions for integration civic activism and community development. At the same time, migrants face structural and psychosocial barriers such as information deficits, intra-diaspora tensions, psychological exhaustion and Russian minority pressure. Despite these challenges, the emergence of new civic initiatives and NGOs demonstrates growing organizational potential and social resilience.

Keywords: temporary protection, forced migration, migrants' integration, migrants' civic engagement, Ukrainian diaspora

Author Contributions

Conceptualization: O.P.

Methodology: O.P.

Formal analysis: O.P.

Investigation: O.P.

Resources: O.P.

Writing – original draft: O.P.

Writing – review & editing: O.P.

Supplementary Materials

Not applicable.

Funding

This research received no external funding.

Ethics Approval Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Data sharing is not applicable to this article as no new data were generated or analyzed in this study.

Declaration of Generative AI Use

No generative artificial intelligence tools were used in the preparation of this manuscript.

Acknowledgments

Not applicable.

Conflict of Interest

Oksana Pyatkovska declares no conflict of interest.

