Studia Administracji i Bezpieczeństwa

Public Administration and Security Studies

2025
nr 19

Europe's Security in the Face of Crises and Challenges

Issue Editors
Tomasz Marcinkowski
Juliusz Sikorski

Akademia im. Jakuba z Paradyża
Gorzów Wielkopolski 2025

Redakcja informuje, że pierwotną wersją czasopisma jest wydanie papierowe

ISSN 2543-6961

Adres redakcji: Studia Administracji i Bezpieczeństwa
ul. Fryderyka Chopina 52, 66-400 Gorzów Wielkopolski
tel. 95 7216 061
e-mail: czasopismowaibn@gmail.com, strona internetowa: www.studia.administracji.i.bezpieczenstwa.ajp.edu.pl

TABLE OF CONTENTS

PART II: NEW FORMS OF CONFRONTATION

PART III: STATE SECURITY AND THE LEGAL AND INSTITUTIONAL FRAMEWORK

Part I:

Geopolitical Changes and Strategic Challenges for Europe

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 195–220

ISSN 2543-6961
e-ISSN 2720-3093

Marco Marsili
ORCID: 0000-0003-1848-9775
Cà Foscari University of Venice

Disinformation and Democratic Resilience in the European Union: Lessons from the Covid-19 Pandemic and Election Interference[1]

Dezinformacja i odporność demokratyczna w Unii Europejskiej: wnioski z pandemii COVID-19 i ingerencji w wybory

Abstract
This article investigates how the European Union has addressed the challenges posed by disinformation in times of crisis. It examines the EU's institutional and regulatory responses to digital threats, with a particular focus on the COVID-19 infodemic and foreign election interference. The article analyzes key policy initiatives, including the Code of Practice on Disinformation, the Digital Services Act, and the establishment of the European Digital Media Observatory. Drawing on the social amplification of risk framework and resilience theory, it evaluates the effectiveness of these measures in fostering democratic stability and media integrity. The findings highlight both achievements and ongoing vulnerabilities in the EU's strategy for countering information manipulation in a fragmented digital environment.

Keywords: disinformation; EU digital governance; COVID-19 infodemic; election interference; Code of Practice; Digital Services Act; media literacy; democratic resilience

Abstrakt
Artykuł analizuje, w jaki sposób Unia Europejska stawia czoła wyzwaniom związanym z dezinformacją w czasie kryzysów. Omawia instytucjonalne i regulacyjne reakcje UE na zagrożenia cyfrowe, ze szczególnym uwzględnieniem infodemii podczas pandemii COVID-19 oraz ingerencji zagranicznej w procesy wyborcze. Autor przedstawia kluczowe inicjatywy polityczne, takie jak Kodeks postępowania w sprawie dezinformacji, Akt o usługach cyfrowych (DSA) oraz utworzenie Europejskiego Obserwatorium Mediów Cyfrowych (EDMO). W oparciu o ramy teorii amplifikacji ryzyka społecznego i odporności instytucjonalnej, artykuł ocenia skuteczność tych środków w umacnianiu stabilności demokratycznej i integralności mediów. Wnioski podkreślają zarówno osiągnięcia, jak i istniejące słabości strategii UE wobec manipulacji informacją w zróżnicowanym środowisku cyfrowym.

Słowa kluczowe: dezinformacja; zarządzanie cyfrowe UE; infodemia COVID-19; ingerencja wyborcza; Kodeks postępowania; Akt o usługach cyfrowych; edukacja medialna; odporność demokratyczna

[1] This article constitutes Part I of a two-part study. It is complemented by "The European Union's Strategic Adaptations to Hybrid Conflicts and the Influence of External Actors", published as Part II in the thematic issue "Europe's Security in the Face of Crises and Challenges" of *Studia Administracji i Bezpieczeństwa*, vol. 19, no. 19, 2025.

Introduction

This article aims to examine the European Union's responses to disinformation as a strategic challenge to democratic governance. It focuses on two critical cases: the COVID-19 pandemic and foreign interference in electoral processes. Specifically, the study evaluates the policy instruments, institutional arrangements, and informational frameworks that the EU has mobilized to counter digital threats and enhance societal resilience.

In recent years, the European Union has found itself navigating through a storm of unprecedented crises. From the relentless waves of the COVID-19 pandemic to the geopolitical tremors caused by the war in Ukraine, the EU's resilience and adaptability have been put to the test. These crises have not only challenged the EU's institutional frameworks but have also reshaped its internal and external policies in profound ways.

The COVID-19 pandemic, which swept across the globe in late 2019, laid bare the vulnerabilities within the EU's public health systems. It underscored the urgent need for stronger coordination among member states, as the virus did not respect borders. Alongside the health crisis, a parallel pandemic of disinformation spread rapidly, undermining public trust in institutions and complicating efforts to manage the crisis effectively. Social media platforms became battlegrounds where false information thrived, challenging the EU to find innovative ways to combat this digital menace.

For instance, during the early stages of the pandemic, false claims about the virus's origins, treatments, and preventive measures proliferated online. The EU's response included launching the "EU vs Disinfo" campaign, which aimed to debunk myths and provide accurate information to the public. This initiative highlighted the importance of timely and transparent communication in combating disinformation. As Vice-President of the European Parliament Eva Kaili noted, "[a] strong European response against disinformation is crucial to ensure the protection of European values and democracy."[2]

As if the pandemic were not enough, the war in Ukraine erupted, posing significant challenges to the EU's security and foreign policy. This conflict, characterized by a blend of conventional military tactics and modern hybrid warfare—including cyber-attacks and disinformation campaigns—required the EU to respond with a multifaceted strategy. The war in Ukraine became a stark

[2] European Digital Media Observatory (EDMO), *United Against Disinformation: A Truly European Response*, EDMO, 26 September 2022, https://edmo.eu/edmo-news/united-against-disinformation-a-truly-european-response/ [date of access: 13.07.2025].

reminder of the complexities of contemporary conflicts and the need for comprehensive approaches that integrate military, political, and technological responses.

A real-life example of the EU's response to hybrid warfare can be seen in its support for Ukraine through the European Peace Facility, which provides funding for military equipment and training. Additionally, the EU has imposed sanctions on Russia, targeting key sectors of its economy to pressure it into ceasing its aggressive actions. These measures demonstrate the EU's commitment to a coordinated and robust response to hybrid threats. As Kaja Kallas, High Representative of the EU, emphasized, "[d]isinformation is a fundamental part of Russian military activities. We have to fight it. This is hybrid warfare."[3]

Disinformation, often disseminated through social media and other digital platforms, emerged as a critical threat to democratic processes and public trust. The EU's strategies to combat disinformation included regulatory measures, public awareness campaigns, and collaborations with technology companies. However, the effectiveness of these measures remains a topic of ongoing debate, as the digital landscape continues to evolve.

For example, the EU's *Code of Practice on Disinformation*, which involves major tech companies like Facebook, Google, and Twitter, aims to increase transparency and accountability in online platforms. This voluntary code encourages companies to take proactive steps in identifying and removing false content, thereby protecting the integrity of information shared online. As Lauri Tierala from the European University Institute stated, "[t]he creation of EDMO [European Digital Media Observatory] is a key element to work toward a deeper understanding of online disinformation, its mechanisms and actors, challenges, and impact on society."[4]

Hybrid conflicts, which combine traditional military tactics with cyber warfare and disinformation, represent a significant challenge to the EU's security. The war in Ukraine is a prime example of such a conflict, involving not only traditional military engagements but also cyber-attacks and information warfare. The EU's response to these hybrid threats requires a comprehensive approach that integrates various strategies to address the multifaceted nature of these conflicts.

Thomas Haldenwang, former president of Germany's federal domestic intelligence agency, highlighted the severity of these threats: "Russia is using the entire toolbox, from influencing political discussions to cyber-attacks on critical

[3] K. Kallas, *Ukraine: Speech by High Representative/Vice-President Kaja Kallas at the EP plenary on Russia's disinformation and historical falsification to justify its war of aggression*, 17 December 2024, https://www.eeas.europa.eu/eeas/ukraine-speech-high-representativevice-president-kaja-kallas-ep-plenary-russia's-disinformation-and_en/ [date of access: 13.07.2025].

[4] EDMO, *United Against Disinformation: A Truly European Response*.

infrastructure to sabotage on a significant scale."[5] This underscores the need for the EU to develop robust and adaptive strategies to counter these hybrid threats effectively.

2. Theoretical Framework

2.1 Crisis Management Theories

Crisis management is a critical field of study that examines how organizations, governments, and institutions respond to unexpected and disruptive events. Theories in this domain provide frameworks for understanding the processes and strategies involved in mitigating the impacts of crises. Several key theories are particularly relevant to the EU's responses to contemporary crises such as disinformation and hybrid conflicts.

One foundational theory in crisis management is the Crisis Life Cycle Theory**,** which outlines the stages of a crisis: pre-crisis, crisis response, and post-crisis.[6] This theory emphasizes the importance of preparedness and proactive measures in the pre-crisis stage, effective response strategies during the crisis, and recovery and learning in the post-crisis phase. The EU's approach to managing the COVID-19 pandemic, for instance, can be analyzed through this lens. The initial response involved rapid coordination among member states, the implementation of public health measures, and the dissemination of accurate information to counter disinformation.[7]

The Crisis Life Cycle Theory influences policy-making by emphasizing the need for comprehensive planning across all stages of a crisis. Policymakers are encouraged to develop robust preparedness plans, including early warning systems and stockpiling essential resources. During the crisis response phase, policies focus on rapid and coordinated actions to mitigate the impact. In the post-crisis phase, policies aim to evaluate the response and implement lessons learned to improve future preparedness. This cyclical approach ensures that policies are continuously refined and adapted based on past experiences.

The Crisis Life Cycle Theory can be applied to the EU's handling of the COVID-19 pandemic. In the pre-crisis stage, the EU focused on preparedness by

[5] L. Kayali, D. Banse, W. Büscher, U. Kraetzer, U. Müller, C. Schweppe, *Europe is under attack from Russia. Why isn't it fighting back?*, Politico, 25 November 2024, https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference/ [date of access: 13.07.2025].

[6] W.T. Coombs, *Ongoing Crisis Communication: Planning, Managing, and Responding*, Thousand Oaks 2007; S. Fink, *Crisis Management: Planning for the Inevitable*, New York 1986.

[7] European Commission, *EU Coronavirus Response Overview*, https://commission.europa.eu/strategy-and-policy/coronavirus-response/overview-commissions-response_en#:~:text=The%20Commission%20has%20mobilised%20more,the%20coronavirus%20and%20save%20lives [date of access: 13.07.2025].

stockpiling medical supplies and developing early warning systems. During the crisis response phase, the EU implemented public health measures, coordinated vaccine distribution, and launched information campaigns to counter disinformation. In the post-crisis phase, the EU is now focusing on recovery and learning, analyzing the effectiveness of its response to improve future crisis management strategies.

Another significant theory is the Contingency Theory**,** which posits that there is no one-size-fits-all approach to crisis management.[8] Instead, the effectiveness of a response depends on the specific context and nature of the crisis. This theory is particularly relevant to the EU's handling of hybrid conflicts, such as the war in Ukraine. The EU's response has involved a combination of military support, economic sanctions, and diplomatic efforts, tailored to the unique challenges posed by the conflict.[9]

The Contingency Theory impacts policy-making by highlighting the importance of context-specific responses. Policymakers are encouraged to assess the unique characteristics of each crisis and tailor their strategies accordingly. This theory supports the development of flexible policies that can be adjusted based on the evolving nature of the crisis. For example, the EU's varied responses to different crises, such as economic sanctions for geopolitical conflicts and public health measures for pandemics, reflect the principles of contingency theory.

The Contingency Theory is evident in the EU's response to the war in Ukraine. Recognizing that a one-size-fits-all approach would be ineffective, the EU tailored its response to the specific context of the conflict. This included providing military aid to Ukraine, imposing economic sanctions on Russia, and engaging in diplomatic efforts to de-escalate the situation. The EU's flexible and context-specific approach highlights the principles of contingency theory.

The Complexity Theory also offers valuable insights into crisis management. This theory suggests that crises are often complex and interconnected, requiring adaptive and flexible responses.[10] The EU's strategies to combat disinformation, for example, involve multiple stakeholders, including government agencies, technology companies, and civil society organizations. This collaborative approach

[8] L. Donaldson, *The Contingency Theory of Organizations*, Thousand Oaks 2001.

[9] M. Marsili, *Hybrid Warfare: Above or Below the Threshold of Armed Conflict?*, "Hungarian Defence Review" 2022, vol. 150, no. 1-2, p. ; M. Marsili, *Inside and beyond the Russo-Ukrainian War: The Pitfalls of the European Union*, [in:] *Newsletter Annual of the Academy of Yuste: Reflections on Europe and Ibero-America*, *vol. 3, year 2022, 1st ed.,* Cuacos de Yuste 2023, p. 429.

[10] A. Boin, L.K. Comfort, C.C. Demchak, *The Rise of Resilience: Crisis Response in the European Union*, Cambridge 2013.

reflects the complexity of the disinformation landscape and the need for coordinated efforts to address it effectively.[11]

The Complexity Theory influences policy-making by recognizing that crises are often interconnected and multifaceted. Policymakers are encouraged to adopt adaptive and flexible strategies that can respond to the dynamic nature of complex crises. This theory supports the development of policies that involve multiple stakeholders and sectors, fostering collaboration and coordination. For instance, the EU's approach to combating disinformation involves regulatory measures, partnerships with technology companies, and public awareness campaigns, reflecting the complexity of the issue.

The Complexity Theory is particularly relevant to the EU's strategies to combat disinformation. Disinformation is a complex issue involving multiple actors and platforms. The EU's response has been multifaceted, involving regulatory measures, collaborations with technology companies, and public awareness campaigns. This approach acknowledges the interconnected nature of the problem and the need for adaptive and flexible strategies.

The Resilience Theory shapes policy-making by emphasizing the need to build systems and institutions that can absorb shocks and recover from crises.[12] Policymakers are encouraged to develop policies that enhance the resilience of critical infrastructure, public health systems, and economic frameworks.[13] This theory is particularly relevant to the EU's efforts to enhance its institutional resilience in the face of ongoing and emerging crises. Initiatives such as the European Resilience Initiative aim to strengthen the EU's ability to withstand and adapt to various threats, from cyber-attacks to economic instability, and ensure that the Union is better prepared for future crises.[14] The initiative promotes cross-sectoral and cross-border crisis management, improving crisis communication, and combating disinformation. It also emphasizes the importance of sustainable, fair, and democratic transitions in response to crises. However, the effectiveness

[11] C. Wardle, H. Derakhshan. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe report DGI(2017)09, Strasburg 2017, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html [date of access: 13.07.2025].

[12] C.S. Holling, *Resilience and stability of ecological systems*, "Annual Review of Ecology and Systematics" 1973, vol. 4, no. 1, pp. 1–23.

[13] Ibidem.

[14] European Council/Council of the European Union, *The Council adopted conclusions on resilience and crisis response*, 23 November 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/11/23/the-council-adopted-conclusions-on-resilience-and-crisis-response/?utm_source=chatgpt.com [date of access: 13.07.2025].

of this initiative depends on continuous investment and political commitment from member states.[15]

Here are some notable examples of resilience policies implemented by the European Union.[16] The *Recovery and Resilience Facility* (RRF) is a central component of the EU's *NextGenerationEU* plan, designed to help member states recover from the economic and social impacts of the COVID-19 pandemic. The RRF provides financial support for reforms and investments that make economies and societies more sustainable, resilient, and prepared for the green and digital transitions. Member states submit national recovery and resilience plans outlining their proposed measures, which must allocate at least 37% of their budget to green initiatives and 20% to digital measures. The RRF has been praised for its flexibility and focus on green and digital transitions. However, its effectiveness varies across member states, depending on how well national plans are implemented and monitored.[17]

The *Union Civil Protection Mechanism* (UCPM) enhances cooperation among national civil protection authorities across Europe. It aims to improve disaster preparedness, increase public awareness, and enable quick, coordinated assistance during natural and man-made disasters. This mechanism has been crucial in responding to various crises, including wildfires, floods, and health emergencies. The UCPM has proven effective in enhancing cooperation and coordination among EU member states during disasters. It has facilitated rapid response and resource sharing during emergencies such as wildfires, floods, and health crises. The mechanism's ability to mobilize resources quickly and efficiently has been a significant strength, although challenges remain in ensuring consistent preparedness levels across all member states.[18]

In response to the energy market disruptions caused by geopolitical tensions, such as Russia's attack on Ukraine, the *REPowerEU Plan* aims to reduce the EU's dependence on Russian fossil fuels. It focuses on diversifying energy supplies, accelerating the rollout of renewable energy, and improving energy efficiency. This plan is part of the broader effort to enhance the EU's energy security and

[15] A. Kammer, *Europe's Choice: Policies for Growth and Resilience*, International Monetary Fund (IMF), 16 December 2024, https://www.imf.org/en/News/Articles/2024/12/15/sp121624-europes-choice-policies-for-growth-and-resilience [date of access: 13.07.2025].

[16] Council of the EU and the European Council, *How the EU responds to crises and builds resilience*, last review 19 November 2024, https://www.consilium.europa.eu/en/policies/eu-crisis-response-resilience/; European Commission, *The Recovery and Resilience Facility*, https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility_en [date of access: 13.07.2025].

[17] J. Sparf, E. Petridou, *Resilience in Practice: A Survey of Recent European Union Projects*, "RCR Working Paper Series" 2019, no. 4. p.

[18] European Commission, Directorate-General for Communication, *Building a Resilient and Future-Ready Democracy in the EU*, 20 March 2024, https://commissioners.ec.europa.eu/building-resilient-and-future-ready-democracy-eu-2024-03-20_en [date of access: 13.07.2025].

resilience. While the plan has made significant strides, its long-term success will depend on sustained efforts to improve energy efficiency and infrastructure.

These legislative acts aim to create a safer and more open digital space by regulating online platforms and digital services. The *Digital Services Act* (DSA)[19] focuses on increasing transparency and accountability of online platforms, combating illegal content, and protecting users' rights. The *Digital Markets Act* (DMA)[20] targets anti-competitive practices by large digital companies, promoting fair competition and innovation. These acts contribute to the resilience of the EU's digital ecosystem. The effectiveness of these acts will continue to evolve as they are fully implemented and enforced.

The *European Green Deal* is a comprehensive strategy to make the EU's economy sustainable by turning climate and environmental challenges into opportunities. It includes policies aimed at reducing greenhouse gas emissions, promoting clean energy, and fostering sustainable agriculture. The Green Deal also emphasizes the importance of building resilience to climate impacts through adaptation measures and disaster risk reduction.[21] The Green Deal's success is evident in the increased adoption of renewable energy and the EU's progress towards its climate goals. However, achieving these targets requires ongoing commitment and collaboration among member states.

These policies illustrate the EU's commitment to enhancing its resilience across various domains, from economic recovery and energy security to digital governance and environmental sustainability. By implementing these measures, the EU aims to better prepare for and respond to future crises, ensuring a more resilient and sustainable future for its member states. Overall, the EU's resilience policies have shown considerable effectiveness in addressing various crises and enhancing the Union'' capacity to withstand future shocks. While there are areas for improvement, particularly in ensuring consistent implementation and monitoring across member states, these policies have laid a strong foundation for a more resilient and sustainable Europe.

The *Social Amplification of Risk Framework* (SARF) is another important theory that examines how social processes can amplify or attenuate public perceptions

[19] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (*Digital Services Act*), PE/30/2022/REV/1, *OJ L 277, 27.10.2022, p. 1–102*, http://data.europa.eu/eli/reg/2022/2065/oj.

[20] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (*Digital Markets Act*), PE/17/2022/REV/1, *OJ L 265, 12.10.2022, p. 1–66,* http://data.europa.eu/eli/reg/2022/1925/oj.

[21] Council of the EU and the European Council, *How the EU responds to crises and builds resilience*.

of risk.[22] This framework is particularly relevant in the context of disinformation, where social media can significantly amplify the perceived severity of a crisis. Policymakers are encouraged to develop communication strategies that manage the amplification of risk through media and public discourse. This theory supports the creation of policies that promote transparency, accurate information dissemination, and public engagement. The EU's efforts to counter disinformation through public awareness campaigns and collaborations with social media platforms during the COVID-19 pandemic and in the context of the war in Ukraine can be seen as attempts to manage the social amplification of risk and provide reliable information to the audience.

In addition to these theories, the Network Theory highlights the importance of networks and relationships in crisis management.[23] This theory supports the creation of networks and partnerships that enhance the sharing of information and resources. Policymakers are encouraged to develop policies that facilitate coordination and cooperation across different organizations and sectors. The EU's response to the COVID-19 pandemic, for example, involved coordination between health authorities, governments, and international organizations. This networked approach facilitated the sharing of information and resources, enhancing the overall effectiveness of the response.

The Institutional Theory also provides valuable insights into how organizations adapt to crises. This theory suggests that institutions are influenced by their environments and must adapt to changing conditions to survive and thrive[24] Policymakers are encouraged to develop policies that promote institutional flexibility and adaptability. The theory supports the creation of new crisis management bodies, the implementation of innovative policies, and the continuous evaluation of institutional performance. The EU's institutional adaptations in response to the COVID-19 pandemic and the war in Ukraine, such as the establishment of new crisis management bodies and the implementation of new policies, reflect the principles of institutional theory.

Marco Marsili's extensive research on international relations and security, including his analysis of the EU's crisis management strategies,[25] further enriches

[22] R.E. Kasperson, O. Renn, P. Slovic, H.S. Brown et al., *The social amplification of risk: A conceptual framework*, "Risk Analysis" 1988, vol. 8, no. 2, pp. 177–187.

[23] R.S. Burt, *Brokerage and Closure: An Introduction to Social Capital,* New York 2005, M. S. Granovetter, *The Strength of Weak Ties*, "*American Journal of Sociology"* 1973*, vol. 78,* no. 6, pp. 1360–1380.

[24] J.W. Meyer, B. Rowan, *Institutionalized Organizations: Formal Structure as Myth and Ceremony*, "*American Journal of Sociology"* 1977, vol. *83*, no. 2, pp. 340–363, ; P.J. DiMaggio, W.W. Powell, *The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields*, "*American Sociological Review" 1983, vol. 48, no.* 2, pp. 147–160.

[25] M. Marsili, *Hybrid Warfare: Above or Below the Threshold of Armed Conflict?*, "Hungarian Defence Review" 2022, vol. 150, no. 1-2,pp. 36-48 .

our understanding of these theoretical frameworks. His work emphasizes the need for a holistic approach to crisis management that integrates multiple perspectives and disciplines.

In summary, crisis management theories provide essential frameworks for understanding and analyzing the EU's responses to contemporary crises. By applying these theories, we can gain deeper insights into the effectiveness of the EU's strategies and identify areas for improvement. The integration of theoretical perspectives with practical examples enriches our understanding of crisis management in the context of the EU's complex and dynamic environment.

2.2 Institutional Resilience in the EU

The European Union has faced numerous crises over the past decades, each testing the resilience of its institutions. From the financial crisis of 2008 to the COVID-19 pandemic, and the migration and climate crises, the EU's ability to adapt and respond effectively has been crucial. This section explores how the EU's institutional resilience has been demonstrated through various case studies, highlighting the lessons learned and the innovative approaches adopted, while also discussing future strategies for enhancing resilience.

During the financial crisis of 2008, the EU's response was multifaceted, involving significant policy shifts and the creation of new mechanisms. One notable example is the establishment of the *European Stability Mechanism* (ESM) in 2012. The ESM provided financial assistance to Eurozone countries in distress, ensuring stability and preventing the collapse of the Euro. This mechanism showcased the EU's ability to create robust financial safeguards and fostered greater economic integration among member states. The crisis underscored the importance of flexibility and adaptability in policy-making, as well as the need for strong institutional frameworks to manage economic shocks.

The COVID-19 pandemic posed an unprecedented challenge, requiring swift and coordinated action. The EU's response included the implementation of the *Coronavirus Response Investment Initiative* (CRII) and its extension, CRII+. These initiatives allowed for the reallocation of unused cohesion policy funds to support healthcare systems, SMEs, and labor markets. For instance, France utilized CRII/CRII+ flexibilities to mobilize additional funds for healthcare, significantly increasing its capacity to respond to the health crisis.[26] Moreover, the *Recovery and Resilience Facility* was established as part of the *NextGenerationEU* recovery plan.

[26] T. Kiss-Gálfalvi, C. Alcidi, A. Ounnas, E. Rubio, H. Crichton-Miller, D. Gojsic, *Lessons learned from the implementation of crisis response tools at EU level. Part 1: Assessing implementation and implications*, Brussels 2024.

This facility provided substantial financial support to member states, enabling them to implement reforms and investments aimed at fostering resilience and recovery. Italy, for example, leveraged RRF funds to enhance its digital infrastructure and healthcare system, demonstrating the EU's commitment to long-term resilience and innovation.[27] The pandemic highlighted the importance of collaboration and solidarity among member states, as well as the need for innovative and flexible funding mechanisms to enhance crisis response capabilities.

The migration crisis of 2015-2016 tested the EU's capacity to manage large-scale humanitarian challenges. The sudden influx of refugees and migrants, primarily from Syria, Iraq, and Afghanistan, required a coordinated and compassionate response. The EU implemented several measures, including the relocation and resettlement schemes, which aimed to distribute asylum seekers more evenly across member states. Germany's response, where the government, in collaboration with civil society organizations, provided extensive support to integrate refugees into the community, is a notable example.[28] This included language courses, vocational training, and employment opportunities, showcasing a comprehensive approach to integration.[29] The EU also established the *European Border and Coast Guard Agency* (Frontex) to enhance border management and ensure the safety and security of external borders.[30] The migration crisis underscored the need for a humanitarian approach in crisis management, shared responsibility among member states, and the importance of engaging local communities and civil society organizations in effectively integrating refugees and migrants.

The EU has also been at the forefront of global efforts to combat climate change, demonstrating resilience through proactive policies and initiatives. The *European Green Deal*, launched in 2019, aims to make Europe the first climate-neutral continent by 2050. This ambitious plan includes measures to reduce greenhouse gas emissions, promote renewable energy, and enhance energy efficiency.

---

[27] A. D'Alfonso, *Italy's National Recovery and Resilience Plan. Latest state of play*, "EPRS Brief" PE 698.847, April 2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698847/EPRS_BRI%282021%29698847_EN.pdf [date of access: 13.07.2025].

[28] Federal Office for Migration and Refugees, *Access to integration courses and vocational language courses for Afghan local staff and their family members*, https://www.bamf.de/SharedDocs/Anlagen/EN/AsylFluechtlingsschutz/info-zugang-integrations-berufssprachkurse-afghan-ortskraefte.pdf?__blob=publicationFile&v=5 [date of access: 13.07.2025].

[29] European Migration Network (EMN), *EMN Annual Report on Immigration and Asylum 2015*, Dublin/Brussels 2016,; https://emn.ie/files/p_20160816024328 2015emn_annual_report_on_immigration_and_asylum.pdf [date of access: 13.07.2025]; S. Niinistö, *Safer Together. Strengthening Europe's Civilian and Military Preparedness and Readiness,* Brussels 2024, https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf [date of access: 13.07.2025].

[30] Frontex, https://frontex.europa.eu.

One significant initiative under the Green Deal[31] is the *Just Transition Mechanism* (JTM), which supports regions and sectors most affected by the transition to a green economy.[32] For example, Poland, heavily reliant on coal, has received substantial funding to support the transition to renewable energy sources and create new economic opportunities.[33] This approach ensures that the transition is fair and inclusive, leaving no one behind. The climate crisis has highlighted the importance of proactive policy-making, inclusive transition strategies, and investment in renewable energy and innovative technologies to build resilience against climate change.

Technology plays a pivotal role in the EU's resilience strategies.[34] The integration of advanced technologies enhances the EU's capacity to respond to crises and build long-term resilience. For instance, the development of digital infrastructure and the promotion of digital skills are central to the EU's strategy for economic recovery and growth. The Digital Europe Programme aims to strengthen Europe's digital capabilities by investing in supercomputing, artificial intelligence, cybersecurity, and advanced digital skills.[35] These technological advancements not only support immediate crisis response but also contribute to the EU's long-term strategic autonomy and competitiveness.

However, the EU faces several challenges in its quest for future resilience. One significant challenge is the need for continuous innovation and investment in technology to keep pace with rapidly evolving threats and opportunities. Additionally, ensuring equitable access to technological advancements across all member states is crucial to prevent disparities and promote inclusive growth. The EU must also address the risks associated with technological dependencies and cybersecurity threats, which can undermine resilience efforts. Furthermore, the complexity

[31] European Commission, *The European Green Deal*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en [date of access: 13.07.2025].

[32] European Commission, *The Just Transition Mechanism: making sure no one is left behind*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/finance-and-green-deal/just-transition-mechanism_en [date of access: 13.07.2025].

[33] European Commission, *EU Cohesion Policy: €3.85 billion for a just transition toward climate neutral economy in five Polish regions*, 5 December 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7413 [date of access: 13.07.2025].

[34] European Commission, *Joint Communication to the European Parliament, The European Council, and the Council on "European Economic Security Strategy"*, JOIN(2023) 20 final, 20 June 2023; Expert Group of the Community for European Research and Innovation for Security Building resilience in the civil security domain based on research and technology, *Building resilience in the civil security domain based on research and technology*, Report of the CERIS Expert Group, Luxembourg 2024, doi:10.2837/02895 [date of access: 13.07.2025].

[35] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, PE/13/2021/INIT, *OJ L 166, 11.5.2021, p. 1–34,* http://data.europa.eu/eli/reg/2021/694/oj [date of access: 13.07.2025].

of coordinating responses across diverse member states with varying capacities and priorities remains a persistent challenge.[36]

Looking ahead, the EU's future resilience strategies will likely focus on further strengthening institutional frameworks, enhancing flexibility in policy-making, and fostering greater collaboration among member states. The lessons learned from past crises emphasize the need for continuous innovation and investment in sustainable development, digital transformation, and social cohesion. By building on these experiences, the EU can develop robust mechanisms that not only address immediate challenges but also pave the way for a more resilient and integrated future.

In conclusion, the EU's experience with various crises has demonstrated the importance of institutional resilience. By learning from past challenges and continuously evolving, the EU has been able to develop robust mechanisms that not only address immediate needs but also pave the way for a more resilient and integrated future.

2.3 Hybrid Conflicts and Disinformation

Hybrid conflicts and disinformation have emerged as significant threats to the stability and security of the European Union. These forms of conflict blend conventional and unconventional tactics, including cyber-attacks, economic pressure, and the spread of false information, to achieve strategic objectives without engaging in open warfare. This section examines the nature of hybrid conflicts and disinformation, their impact on the EU, and the strategies employed to counter these threats.

Hybrid conflicts are characterized by the use of a combination of military and non-military tools to achieve political goals. These tools can include cyber-attacks, economic coercion, and the manipulation of information to influence public opinion and destabilize societies. The concept of hybrid warfare blurs the lines between war and peace, creating a grey zone where traditional definitions of conflict no longer apply.[37] This ambiguity makes it challenging for states to respond effectively, as the origin and nature of the threat are often unclear.

Disinformation, a key component of hybrid conflicts, involves the deliberate spread of false or misleading information to deceive and manipulate public opinion. This tactic has been used extensively in recent years to influence elections,

[36] N. Behnke, S. Muller, *Challenges and Opportunities of Intergovernmental Coordination*, Brussels 2021, https://igcoord.eu/wp-content/uploads/2022/01/IGCOORDPB1final.pdf [date of access: 13.07.2025].

[37] J. Kelly, *How democracies can overcome the challenges of hybrid warfare and disinformation*, Barcelona 2022.

sow discord, and undermine trust in democratic institutions. The EU has been a target of disinformation campaigns, particularly from state and non-state actors seeking to weaken its cohesion and influence.[38]

One notable example of disinformation in the context of hybrid conflicts is the Russo-Ukrainian conflict. Marco Marsili's work highlights how disinformation and propaganda have been used to shape narratives and influence perceptions during this conflict.[39] The strategic use of social media, digital propaganda, and deepfakes has had a profound impact on the conflict's dynamics, demonstrating the power of information warfare in modern conflicts.

The EU has taken several steps to counter hybrid threats and disinformation. The establishment of the *European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE)[40] and the creation of the *East StratCom Task Force* (ESCTF or ESTF) are examples of initiatives aimed at enhancing the EU's resilience against these threats.[41] These bodies work to identify and expose disinformation, improve information sharing among member states, and develop strategies to counter hybrid threats.

Technology plays a crucial role in both the propagation and countering of disinformation. Advances in artificial intelligence and machine learning have enabled the creation of sophisticated disinformation campaigns, but they also offer tools for detecting and mitigating these threats. The EU's Digital Europe Programme aims to strengthen Europe's digital capabilities, including investments in cybersecurity and advanced digital skills, to enhance resilience against hybrid threats.

However, the EU faces several challenges in addressing hybrid conflicts and disinformation. The complexity of coordinating responses across diverse member states with varying capacities and priorities remains a persistent challenge. Additionally, the rapid evolution of technology means that disinformation tactics are constantly changing, requiring continuous innovation and adaptation in countermeasures.

Looking ahead, the EU's strategies for enhancing resilience against hybrid conflicts and disinformation will likely focus on strengthening institutional frameworks, fostering greater collaboration among member states, and investing in technological solutions. By building on existing initiatives and continuously

[38] *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*, eds. M. Regan, A. Sari, Oxford 2024 .

[39] M. Marsili, *The Russian Influence Strategy in Its Contested Neighbourhood*, [in:] *The Russian Federation in Global Information Warfare: Influence Operations in Europe and Its Neighborhood*, eds. H. Mölder, V. Sazonov, A. Chochia, T. Kerikmäe, Cham 2021, pp. 149-172.

[40] European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), https://www.hybridcoe.fi.

[41] *European Union External Action (EEAS)*, *Questions and Answers about the East StratCom Task Force*, 27 October 2021, https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en [date of access: 13.07.2025].

evolving to address new threats, the EU can develop robust mechanisms to protect its societies and democratic institutions from the destabilizing effects of hybrid conflicts and disinformation.

In conclusion, hybrid conflicts and disinformation represent significant challenges to the EU's security and stability. By understanding the nature of these threats and implementing comprehensive strategies to counter them, the EU can enhance its resilience and safeguard its democratic values.

3. The EU's Response to Disinformation

3.1 Overview of Disinformation Challenges

Disinformation poses a significant threat to the stability and integrity of democratic societies, and the European Union is no exception. The proliferation of false or misleading information, often spread through digital platforms and social media, has the potential to undermine public trust in institutions, influence elections, and exacerbate social divisions.[42] This subsection provides an overview of the key challenges associated with disinformation in the EU.

Disinformation is characterized by the deliberate creation and dissemination of false or misleading information with the intent to deceive.[43] Unlike misinformation, which is false information spread without malicious intent, disinformation is strategically crafted to manipulate public opinion and achieve specific political, economic, or social objectives. The digital age has amplified the reach and impact of disinformation, making it easier to spread and harder to control.

The sheer volume and speed at which disinformation can spread online present significant challenges. Social media platforms and digital communication tools enable the rapid dissemination of false information to large audiences, often outpacing efforts to verify and counteract it. Disinformation campaigns have become increasingly sophisticated, employing advanced technologies such as artificial intelligence and deepfakes to create highly convincing false content. These tactics make it difficult for individuals to discern truth from falsehood.

Disinformation is often tailored to exploit existing social, political, and cultural divisions within societies. By targeting specific groups with tailored messages, disinformation campaigns can exacerbate tensions and polarize communities. Persistent exposure to disinformation can erode public trust in traditional media,

[42] S.M. Maci, M. Demata, P. Seargeant, M. McGlashan, *The various dimensions of disinformation: An Introduction*, [in:] *The Routledge Handbook of Discourse and Disinformation*, eds. S.M. Maci, M. Demata, P. Seargeant, M. McGlashan, London 2023, pp. 1-13.

[43] M. Marsili, *The Russian Influence Strategy in Its Contested Neighbourhood,* ibid.; M. Marsili, *COVID-19 Infodemic: Fake News, Real Censorship. Information and Freedom of Expression in Time of Coronavirus*, "Europea" 2020, vol. 10, no. 2, p. 166-67.

government institutions, and democratic processes. This erosion of trust undermines the foundations of democratic societies and makes it more challenging to build consensus on important issues.

Disinformation is not confined by national borders. Foreign actors, including state and non-state entities, can launch disinformation campaigns that target multiple countries simultaneously, complicating efforts to coordinate responses at the national and EU levels.

The impact of disinformation has been evident in several high-profile cases. For instance, during the 2016 Brexit referendum, disinformation played a significant role in shaping public opinion and influencing the outcome of the vote. Similarly, the COVID-19 pandemic saw a surge in disinformation related to health measures, vaccines, and government responses, which hindered public health efforts and fueled skepticism.

Recognizing the severity of the disinformation threat, the EU has implemented a range of measures to address these challenges. Initiatives such as the *EU Code of Practice on Disinformation*, the *European Digital Media Observatory* (EDMO), and the *Rapid Alert System* aim to enhance cooperation, improve information sharing, and develop effective countermeasures. These efforts are complemented by public awareness campaigns and educational programs designed to improve media literacy and critical thinking skills among EU citizens.

Disinformation presents a multifaceted challenge that requires a comprehensive and coordinated response. By understanding the nature of disinformation and the key challenges it poses, the EU can develop and implement strategies to protect its democratic values and ensure the integrity of its information ecosystem.

3.2 Policy Measures and Strategies

The European Union has implemented a comprehensive set of policy measures and strategies to counter disinformation and protect its democratic processes. These measures are designed to address the multifaceted nature of disinformation, enhance the resilience of societies, and promote a secure and trustworthy information environment.

One of the cornerstone initiatives is the *EU Code of Practice on Disinformation*,[44] which was launched in 2018 and strengthened in 2022. This voluntary framework involves collaboration between the EU, online platforms, advertisers, and other stakeholders to combat the spread of disinformation. The Code sets out

[44] *EU Code of Practice on Disinformation*, October 2018, https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation [date of access: 13.07.2025].

commitments for signatories to improve transparency, disrupt advertising revenues for disinformation actors, and empower users with tools to identify and report false information.

The *Digital Services Act* (DSA), adopted in 2022, is another critical component of the EU's strategy. The DSA aims to create a safer digital space by establishing clear responsibilities for online platforms to tackle illegal content, including disinformation. It mandates platforms to implement measures such as content moderation, transparency reporting, and cooperation with fact-checkers and researchers.

The *European Digital Media Observatory* was established to support the fight against disinformation by fostering collaboration among fact-checkers, researchers, and media organizations.[45] EDMO provides a platform for sharing best practices, conducting research, and developing tools to detect and counter disinformation. It also plays a crucial role in enhancing media literacy and raising public awareness about the dangers of disinformation.

The *Rapid Alert System*, launched in 2019, is designed to facilitate real-time information sharing and coordination among EU member states in response to disinformation threats.[46] This system enables timely alerts about disinformation campaigns, allowing for coordinated responses and the dissemination of accurate information to the public.

The *European Democracy Action Plan*, introduced in 2020, outlines a comprehensive approach to strengthening democratic resilience and countering disinformation.[47] The plan includes measures to protect electoral processes, support independent media, and promote digital literacy. It emphasizes the importance of a whole-of-society approach, involving governments, civil society, and the private sector.

Technology plays a pivotal role in the EU's strategies to counter disinformation. Advances in artificial intelligence and machine learning are leveraged to detect and mitigate disinformation. For instance, automated systems are used to identify and flag false content, while AI-driven tools help analyze the spread and impact of disinformation campaigns. The EU's Digital Europe Programme

[45] European Digital Media Observatory (EDMO), *About Us*. https://edmo.eu/about-us/edmoeu/ [date of access: 13.07.2025].

[46] European Union, *Factsheet: Rapid Alert System*, Brussels March 2019, https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf [date of access: 13.07.2025].

[47] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*, COM(2020)790, 3 December 2020, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52020DC0790.

supports these technological advancements by investing in cybersecurity, digital skills, and innovative solutions.

Despite these efforts, the EU faces several challenges in its fight against disinformation. The rapid evolution of disinformation tactics, the complexity of coordinating responses across diverse member states, and the need for continuous innovation in technology are persistent issues. Additionally, ensuring equitable access to reliable information and fostering public trust remain critical challenges.

Looking ahead, the EU's strategies will likely focus on further strengthening institutional frameworks, enhancing international cooperation, and investing in research and innovation. By building on existing initiatives and continuously adapting to new threats, the EU can develop robust mechanisms to safeguard its democratic values and ensure a resilient information ecosystem.

The EU's policy measures and strategies represent a comprehensive and coordinated effort to counter disinformation. By leveraging technology, fostering collaboration, and promoting media literacy, the EU aims to protect its democratic processes and build a secure and trustworthy information environment.

3.3 Case Studies: COVID-19 and Election Interference

The COVID-19 pandemic and election interference represent two significant case studies that highlight the challenges and impacts of disinformation on democratic processes. This subsection examines these case studies, exploring how disinformation was used, the effects it had, and the measures taken to counter it.

The COVID-19 pandemic created a fertile ground for disinformation, with false information spreading rapidly about the virus, its origins, treatments, and government responses. Disinformation during the pandemic took various forms, including conspiracy theories, fake cures, and misleading information about vaccines.[48] This disinformation had serious consequences, undermining public health efforts, fueling vaccine hesitancy, and creating confusion and fear among the public.[49]

One notable example of COVID-19 disinformation was the spread of false claims about the virus being a bioweapon or a hoax. These claims were amplified by social media platforms and certain media outlets, leading to widespread mistrust in official health guidance and government measures.[50] Marco Marsili's work highlights how the infodemic of fake news during the pandemic led to real censorship issues and

[48] Pan American Health Organization (PAHO), *Understanding the Infodemic and Misinformation in the fight against COVID-19*, Washington, https://iris.paho.org/handle/10665.2/52052 [date of access: 13.07.2025].

[49] M. Marsili, *COVID-19 Infodemic: Fake News, Real Censorship. Information and Freedom of Expression in Time of Coronavirus,* ibid.*;* T.S. James, A. Clark, E. Asplund, *Elections During Emergencies and Crises: Lessons for Electoral Integrity from the Covid-19 Pandemic*, Stockholm 2024.

[50] Ibidem.

impacted freedom of expression.[51] The EU responded by launching public awareness campaigns, collaborating with social media companies to remove false content, and promoting accurate information through trusted sources.[52]

Election interference through disinformation has been a growing concern, particularly with the increasing use of digital platforms to influence public opinion.[53] Disinformation campaigns during elections aim to manipulate voter perceptions, suppress voter turnout, and undermine the legitimacy of the electoral process. The 2016 US presidential election and the Brexit referendum are prominent examples where disinformation played a significant role.[54]

In the context of the EU, the 2019 European Parliament elections saw coordinated disinformation efforts aimed at influencing voter behavior and sowing discord.[55] These efforts included the spread of false information about candidates, political parties, and the electoral process itself. Social media platforms were used to amplify divisive narratives and create confusion among voters.

Marco Marsili's analysis of the Russian influence strategy in its contested neighborhood provides a comprehensive understanding of how disinformation and propaganda have been used to shape narratives and influence perceptions during conflicts.[56] This work is particularly relevant in understanding the broader context of election interference and hybrid conflicts.

To counter election interference, the EU implemented several measures, including the establishment of the *Rapid Alert System* to facilitate real-time information sharing among member states, and the *European Digital Media Observatory* to support fact-checking and research efforts. Additionally, the *EU Code of Practice on*

---

[51] M. Marsili, *COVID-19 Infodemic: Fake News, Real Censorship. Information and Freedom of Expression in Time of Coronavirus,* op. cit..

[52] European Commission, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Tackling COVID-19 disinformation-Getting the facts right*, JOIN/2020/8, 10 June 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0008 [date of access: 13.07.2025]*;* European Commission, *Tackling online disinformation,* last update 15 October 2024), https://digital-strategy.ec.europa.eu/en/policies/online-disinformation [date of access: 13.07.2025].

[53] S.M. Maci, M. Demata, P. Seargeant, M. McGlashan, *The Routledge Handbook of Discourse and Disinformation,* ibid..

[54] J. Rose, *Brexit, Trump, and Post-Truth Politics*, "Public Integrity" 2017, vol. 19, no. 6, pp. 555-558; H. Allcott, M. Gentzkow, *Social media and fake news in the 2016 election*, "Journal of Economic Perspectives" 2017, vol. 31, no. 2, pp. 211-236; A. Bovet, H.A. Makse, *Influence of fake news in Twitter during the 2016 US presidential election*, "Nature Communications" 2019, vol. 10, no. 1, pp. 1-10.

[55] European Commission, *Commission Staff Working Document Accompanying the document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Report on the 2019 elections to the European Parliament*, SWD/2020/113, 19 June 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0113 [date of access: 13.07.2025].

[56] M. Marsili, *The Russian Influence Strategy in Its Contested Neighbourhood,* ibid.

Disinformation was strengthened in June 2022 to hold online platforms accountable for the spread of false information.[57]

The case studies of COVID-19 and election interference highlight several key lessons in the fight against disinformation. First, the importance of timely and accurate information dissemination cannot be overstated. Public trust in official sources is crucial for countering false narratives. Second, collaboration between governments, social media companies, and civil society is essential to effectively combat disinformation. Third, continuous monitoring and adaptation of strategies are necessary to address the evolving tactics of disinformation actors.

Marco Marsili and Joanna Wróblewska-Jachna's work on the digital revolution and artificial intelligence underscores the challenges posed by technological advancements in the context of disinformation.[58] Their analysis provides valuable insights into how AI and digital technologies can both contribute to and mitigate the spread of disinformation.

The COVID-19 pandemic and election interference provide valuable insights into the challenges posed by disinformation. By learning from these experiences and implementing robust measures, the EU can enhance its resilience against disinformation and protect its democratic processes.

3.4 Effectiveness and Limitations

The European Union has implemented various measures to counter disinformation, but assessing their effectiveness and understanding their limitations is crucial for refining these strategies. This subsection explores the successes and challenges of the EU's disinformation countermeasures.

The EU's efforts to combat disinformation have yielded several positive outcomes. The *EU Code of Practice on Disinformation* has improved transparency and accountability among online platforms. Signatories have taken steps to enhance the visibility of trustworthy content, disrupt advertising revenues for disinformation actors, and provide users with tools to identify and report false information.[59] The *Digital Services Act* has established clear responsibilities for online platforms, mandating measures such as content moderation and cooperation with fact-checkers.

The EDMO has fostered collaboration among fact-checkers, researchers, and media organizations, enhancing the detection and countering of disinformation.

[57] *The Strengthened Code of Practice on Disinformation,* ibid.

[58] M. Marsili, J. Wróblewska-Jachna, *Digital Revolution and Artificial Intelligence as Challenges for Today,* "*Media i Społeczeństwo"* 2024, vol. 20, no. 1, pp. 19-30.

[59] C. Colomina, H. Ánchez Margalef, R. Youngs, *The impact of disinformation on democratic processes and human rights in the world*, Brussels 2021..

The *Rapid Alert System* has facilitated real-time information sharing and coordination among EU member states, enabling timely responses to disinformation threats. Additionally, the *European Democracy Action Plan* has outlined comprehensive measures to protect electoral processes, support independent media, and promote digital literacy.

Despite these successes, the EU's disinformation countermeasures face several limitations and challenges. One significant challenge is the rapid evolution of disinformation tactics. Disinformation actors continuously adapt their strategies, employing sophisticated technologies such as artificial intelligence and deepfakes to create highly convincing false content. This constant evolution makes it difficult for countermeasures to keep pace.

The voluntary nature of the *EU Code of Practice on Disinformation* limits its enforceability. While signatories have made progress, the lack of mandatory compliance means that not all platforms adhere to the same standards.[60] The *Digital Services Act* aims to address this by imposing legal obligations, but its full impact will only be seen in the coming years.[61]

Coordinating responses across diverse member states with varying capacities and priorities is another persistent challenge. The complexity of the EU's political landscape can hinder the implementation of uniform and effective countermeasures. Ensuring equitable access to reliable information and fostering public trust are also critical challenges. Disinformation can erode trust in traditional media, government institutions, and democratic processes, making it harder to build consensus on important issues.

To enhance the effectiveness of its disinformation countermeasures, the EU must continue to innovate and adapt. Strengthening institutional frameworks and enhancing international cooperation are essential steps. Investing in research and innovation, particularly in the fields of artificial intelligence and cybersecurity, will help develop advanced tools for detecting and mitigating disinformation.

Promoting media literacy and critical thinking skills among EU citizens is crucial for building resilience against disinformation. Public awareness campaigns and educational programs can empower individuals to identify and reject false information. Additionally, fostering collaboration between governments, social media companies, and civil society will ensure a comprehensive and coordinated approach to combating disinformation.

[60] Ibidem.

[61] European Court of Auditors (ECA), *Special report: Disinformation affecting the EU: tackled but not tamed*, Brussels 2021.

Recently, both X (formerly known as Twitter) and Facebook (Meta) have decided to abandon their fact-checking system in the U.S., a move that has sparked considerable debate. Critics have long questioned the effectiveness and functionality of fact-checking on social media platforms. A recent article published in *Nature* argues that the impact of misinformation on social media is often overstated and that the business models of these platforms are more to blame for the spread of false information than the content itself.[62] The research suggests that only a small fraction of users are exposed to false and radical content, and it is primarily those who actively seek it out.[63] This perspective challenges the prevailing narrative that fact-checking alone can significantly mitigate the spread of misinformation, highlighting the need for a more comprehensive approach to addressing the root causes of the issue. The abandonment of fact-checking by the two major US social platforms, although limited to American territory, highlights once again the need for international coordination.

Announcing the abandonment of fact-checking on Facebook (Meta), co-founder, chairman and CEO of Meta Platforms and Facebook Mark Zuckerberg admitted that the program had inadvertently limited freedom of expression, effectively introducing a form of censorship.[64] Joel Kaplan, Chief Global Affairs Officer of Meta, dubbed the social media "Facebook jail", thus stressing the censorship on the platform that curtailed the freedom of speech and limited legitimate political debate.[65] This decision reflects ongoing debates about the balance between combating misinformation and preserving open discourse on social media platforms. Meta will replace human fact-checkers with "community notes" in the U.S., while the fact-checking initiative will stay in place in Europe.

While the EU has made significant strides in countering disinformation, ongoing challenges necessitate continuous adaptation and innovation. By building on existing initiatives and addressing the limitations of current measures, the EU can enhance its resilience against disinformation and protect its democratic values.

Conclusions

The European Union has made significant progress in responding to the challenges of disinformation, especially during acute crises such as the COVID-19 pandemic and during vulnerable electoral periods. Through a blend of voluntary measures and legally binding frameworks, including the *Code of Practice on Disinformation*

[62] C. Budak, B. Nyhan, D.M. Rothschild et al., *Misunderstanding the harms of online misinformation*, "Nature" 2024, vol. 630, pp. 45–53.
[63] Ibidem.
[64] J. Kaplan, *More Speech and Fewer Mistakes,* 7 January 2025, https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/ [date of access: 13.07.2025].
[65] Ibidem.

and the *Digital Services Act*, the EU has begun to assert a normative stance on digital responsibility and information integrity.

However, the fragmented implementation of these tools across Member States and the limited enforceability of voluntary commitments continue to present challenges. While the establishment of mechanisms like the European Digital Media Observatory reflects a growing awareness of the systemic nature of disinformation, a deeper integration of media literacy, independent oversight, and transnational coordination remains crucial.

Building a resilient European digital space will require not only robust regulation, but also adaptive governance and continuous engagement with civil society, academic institutions, and technology platforms. The case studies reviewed underscore the importance of maintaining both democratic openness and institutional vigilance in an era of rapidly evolving information threats.

Bibliography

1. Allcott H., Gentzkow M., *Social media and fake news in the 2016 election*, "Journal of Economic Perspectives" 2017, vol. 31, no. 2, pp. 211-236.
2. Behnke N., Muller S., *Challenges and Opportunities of Intergovernmental Coordination*, IGCOORD November 2021, https://igcoord.eu/wp-content/uploads/2022/01/IGCOORDPB1final.pdf.
3. Boin A., Comfort L.K., Demchak C.C., *The Rise of Resilience: Crisis Response in the European Union*, Cambridge 2013.
4. Bovet A., Makse H.A., *Influence of fake news in Twitter during the 2016 US presidential election*, "Nature Communications" 2019, vol. 10, no. 1, pp. 1-10.
5. Budak C., Nyhan B., Rothschild D.M. et al., *Misunderstanding the harms of online misinformation*, "Nature" 2024, vol. 630, pp. 45–53.
6. Burt R.S., *Brokerage and Closure: An Introduction to Social Capital,* Oxford 2005.
7. Colomina C., Ánchez Margalef H., Youngs R., *The impact of disinformation on democratic processes and human rights in the world*, Brussels 2021.
8. Coombs W.T., *Ongoing Crisis Communication: Planning, Managing, and Responding*, Thousand Oaks 2007.
9. D'Alfonso A., *Italy's National Recovery and Resilience Plan. Latest state of play*, "EPRS Brief" PE 698.847, April 2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698847/EPRS_BRI%282021%29698847_EN.pdf.
10. DiMaggio P.J., Powell W.W.*, The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Field*, "American Sociological Review" 1983, vol. 48, no. 2, pp. 147–160.
11. Donaldson L, *The Contingency Theory of Organizations*, Thousand Oaks 2001.
12. *EU Code of Practice on Disinformation*, October 2018, https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.
13. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), https://www.hybridcoe.fi.

14. European Commission, *Commission Staff Working Document Accompanying the document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Report on the 2019 elections to the European Parliament*, SWD/2020/113, 19 June 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0113.
15. European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*, COM(2020)790, 3 December 2020, https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52020DC0790.
16. European Commission, *EU Cohesion Policy: €3.85 billion for a just transition toward climate neutral economy in five Polish regions*, 5 December 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7413.
17. European Commission, *EU Coronavirus Response Overview*. https://commission.europa.eu/strategy-and-policy/coronavirus-response/overview-commissions-response_en#:~:text=The%20Commission%20has%20mobilised%20more,the%20coronavirus%20and%20save%20lives.
18. European Commission, *Joint Communication to the European Parliament, The European Council, and the Council on "European Economic Security Strategy"*, JOIN(2023) 20 final, 20 June 2023.
19. European Commission, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Tackling COVID-19 disinformation-Getting the facts right*, JOIN/2020/8, 10 June 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0008.
20. European Commission, *Tackling online disinformation*, last update 15 October 2024, https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.
21. European Commission, *The European Green Deal*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en.
22. European Commission, *The Just Transition Mechanism: making sure no one is left behind*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/finance-and-green-deal/just-transition-mechanism_en.
23. European Council/Council of the European Union, *How the EU responds to crises and builds resilience*, last review 19 November 2024, https://www.consilium.europa.eu/en/policies/eu-crisis-response-resilience/.
24. European Council/Council of the European Union, *The Council adopted conclusions on resilience and crisis response*, 23 November 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/11/23/the-council-adopted-conclusions-on-resilience-and-crisis-response/?utm_source=chatgpt.com.
25. European Court of Auditors (ECA), *Special report: Disinformation affecting the EU: tackled but not tamed*, Brussels 2021.
26. European Digital Media Observatory (EDMO), *About Us*, https://edmo.eu/about-us/edmoeu/.
27. European Digital Media Observatory (EDMO), *United Against Disinformation: A Truly European Response*. EDMO, 26 September 2022, https://edmo.eu/edmo-news/united-against-disinformation-a-truly-european-response/.
28. European Migration Network (EMN), *EMN Annual Report on Immigration and Asylum 2015*, Dublin/Brussels 2016, https://emn.ie/files/p_20160816024328 2015emn_annual_report_on_immigration_and_asylum.pdf.

29. *European Union External Action (EEAS), Questions and Answers about the East StratCom Task Force*, 27 October 2021, https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en.
30. European Union, *Factsheet: Rapid Alert System*, Brussels March 2019, https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf.
31. Expert Group of the Community for European Research and Innovation for Security Building resilience in the civil security domain based on research and technology, *Building resilience in the civil security domain based on research and technology*, Report of the CERIS Expert Group, Luxembourg November 2024.
32. Federal office for Migration and Refugees, *Access to integration courses and vocational language courses for Afghan local staff and their family members*, https://www.bamf.de/SharedDocs/Anlagen/EN/AsylFluechtlingsschutz/info-zugang-integrations-berufssprachkurse-afghan-ortskraefte.pdf?__blob=publicationFile&v=5.
33. Fink S., *Crisis Management: Planning for the Inevitable*, New York 1986.
34. Frontex, https://frontex.europa.eu.
35. Granovetter M.S., *The Strength of Weak Ties*, "American Journal of Sociology" 1973, vol. 78, no. 6, pp. 1360–1380.
36. Holling C.S., *Resilience and stability of ecological systems*, "Annual Review of Ecology and Systematics" 1973, vol. 4, no. 1, pp. 1–23.
37. HR Fraternity, *Resource Constraints: Meeting Stakeholder Needs in a Crisis*, https://www.hrfraternity.com/business-excellence/resource-constraints-meeting-stakeholder-needs-in-a-crisis.html.
38. *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*, eds. M. Regan M., A. Sari. A. (eds.), Oxford 2024.
39. James T.S., Clark A., Asplund E., *Elections During Emergencies and Crises: Lessons for Electoral Integrity from the Covid-19 Pandemic*, Stockholm 2024.
40. Kallas K.**,** *Ukraine: Speech by High Representative/Vice-President Kaja Kallas at the EP plenary on Russia's disinformation and historical falsification to justify its war of aggression*, 17 December 2024, https://www.eeas.europa.eu/eeas/ukraine-speech-high-representativevice-president-kaja-kallas-ep-plenary-russia's-disinformation-and_en/.
41. Kammer A., *Europe's Choice: Policies for Growth and Resilience*, International Monetary Fund (IMF), 16 December 2024, https://www.imf.org/en/News/Articles/2024/12/15/sp121624-europes-choice-policies-for-growth-and-resilience.
42. Kaplan J., *More Speech and Fewer Mistakes,* 7 January 2025, https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/.
43. Kasperson R.E., Renn O., Slovic P., Brown H.S. et al., *The social amplification of risk: A conceptual framework*, "Risk Analysis" 1988, vol. 8, no. 2, pp. 177–187.
44. Kayali L., Banse D., Büscher W., Kraetzer U., Müller U., Schweppe C., *Europe is under attack from Russia. Why isn't it fighting back?*, "Politico" 25 November 2024, https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference/.
45. Kelly J., *How democracies can overcome the challenges of hybrid warfare and disinformation*, Barcelona 2022.
46. Kiss-Gálfalvi T., Alcidi C., Ounnas A., Rubio E., Crichton-Miller H., Gojsic D., *Lessons learned from the implementation of crisis response tools at EU level. Part 1: Assessing implementation and implications*, Brussels 2024.

47. Maci S.M., Demata M., Seargeant P., McGlashan M., *The various dimensions of disinformation: An Introduction*, [in:] *The Routledge Handbook of Discourse and Disinformation*, eds. Maci, S.M., Demata, M., McGlashan, M., P. Seargeant, London 2023, pp. 1-13.
48. Marsili M., *Hybrid Warfare: Above or Below the Threshold of Armed Conflict?*. "Hungarian Defence Review" 2022, vol. 150, no. 1-2,pp. .
49. Marsili M., *COVID-19 Infodemic: Fake News, Real Censorship. Information and Freedom of Expression in Time of Coronavirus*, "Europea" 2020, vol. 10, no. 2, pp. 147-170.
50. Marsili M., *Inside and beyond the Russo-Ukrainian War: The Pitfalls of the European Union*, [in:] *Newsletter Annual of the Academy of Yuste: Reflections on Europe and Ibero-America*, vol. 3, year 2022, 1st ed., Cuacos de Yuste: 2023, pp. 429-445.
51. Marsili M., *The Russian Influence Strategy in Its Contested Neighbourhood*, [in:] *The Russian Federation in Global Information Warfare. Influence Operations in Europe and Its Neighborhood*, eds. H. Mölder, V. Sazonov, A. Chochia, T. Kerikmäe, Cham 2021, pp. 149-172.
52. Marsili M., Wróblewska-Jachna J., *Digital Revolution and Artificial Intelligence as Challenges for Today*, "*Media i Społeczeństwo"* 2024, vol. 20, no. 1, pp. 19-30.
53. Meyer J.W., Rowan B., *Institutionalized Organizations: Formal Structure as Myth and Ceremony,* "*American Journal of Sociology"* 1977, vol. *83, no.* 2, pp. 340–363.
54. Niinistö S., *Safer Together. Strengthening Europe's Civilian and Military Preparedness and Readiness,* Brussels 2024.
55. Pan American Health Organization (PAHO), *Understanding the Infodemic and Misinformation in the fight against COVID-19*, Washington 2020, https://iris.paho.org/handle/10665.2/52052.
56. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, PE/13/2021/INIT, *OJ L 166, 11.5.2021, p. 1–34,* http://data.europa.eu/eli/reg/2021/694/oj.
57. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (*Digital Markets Act*), PE/17/2022/REV/1, *OJ L 265, 12.10.2022, p. 1–66 ,* http://data.europa.eu/eli/reg/2022/1925/oj.
58. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (*Digital Services Act*), PE/30/2022/REV/1, *OJ L 277, 27.10.2022, p. 1–102*, http://data.europa.eu/eli/reg/2022/2065/oj.
59. Rose J., *Brexit, Trump, and Post-Truth Politics*, "Public Integrity" 2017, vol. 19, no. 6, pp. 555-558.
60. Sparf J., Petridou E., *Resilience in Practice: A Survey of Recent European Union Projects*, "RCR Working Paper Series" 2019, no. 4.
61. *Strengthened Code of Practice on Disinformation*, 16 June 2022, https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.
62. *The Routledge Handbook of Discourse and Disinformation*, eds. S.M. Maci S.M., M. Demata M., M. McGlashan M., P. Seargeant P. (eds.), London 2023.
63. Wardle C., Derakhshan H., *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe report DGI(2017)09, Strasbourg 2017, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 221–238

ISSN 2543-6961
e-ISSN 2720-3093

Juliusz Sikorski
ORCID: 0000-0002-0579-0158-0002-0579-0158
The Jacob of Paradies University in Gorzów Wielkopolski

Proxy Sources in Cognitive Warfare: The Hidden Architecture of Russian Influence Operations in Central Europe

Źródła pośredniczące w wojnie kognitywnej: ukryta architektura rosyjskich operacji wpływu w Europie Środkowej

Abstract
The article analyzes the role of proxy sources – indirect, ostensibly independent sources and conduits of content – as key components of Russian influence operations in Central Europe conducted within the logic of cognitive warfare. Drawing on reports by NATO StratCom COE, Cardiff University, and the ICCT, as well as documented actions by regulators including the European Union, it reconstructs the mechanics of information laundering, delineates a typology and chains of content flow (placement → layering → integration), and presents case studies (Ghostwriter, NewsFront) alongside an analysis of environmental conditions in Poland and the broader region. The conclusions propose indicators for identifying "proxies" and offer policy and institutional recommendations (prebunking, distribution-network audits, intermediary accountability). The article situates proxy sources within the broader architecture of Russian cognitive warfare, which aims to shape not only what audiences think, but how they think and make decisions. The findings are evidence-informed and derive from a qualitative review of secondary data.

Keywords: cognitive warfare, proxy sources, information laundering, disinformation, propaganda, NewsFront, Ghostwriter, Central Europe, Poland, NATO StratCom

Abstrakt
Artykuł analizuje rolę proxy sources, pośrednich, pozornie niezależnych źródeł i nośników treści, jako kluczowych komponentów rosyjskich operacji wpływu w Europie Środkowej realizowanych w logice walki kognitywnej. W oparciu o raporty NATO StratCom COE, Cardiff University, ICCT oraz udokumentowane działania regulatorów, w tym Unii Europejskiej, dokonano w nim rekonstrukcji mechaniki prania informacji (information laundering), opisano typologię i łańcuchy przepływu treści (lokowanie → warstwowanie → integracja), a także przedstawiono studia przypadków (Ghostwriter, NewsFront) oraz środowiskowe uwarunkowania Polski i regionu. We wnioskach przedstawiono wskaźniki identyfikacji „proxy" oraz rekomendacje polityczne i instytucjonalne (prebunking, audyt sieci dystrybucji, odpowiedzialność pośredników). Artykuł lokuje zjawisko proxy sources w szerszej architekturze rosyjskiej wojny kognitywnej, której celem jest kształtowanie nie tylko tego, co myślą odbiorcy, lecz jak myślą i podejmują decyzje. Ustalenia mają charakter evidence-informed i wynikają z przeglądu jakościowego danych zastanych.

Słowa kluczowe: wojna kognitywna, proxy sources, pranie informacji (information laundering), dezinformacja, propaganda, NewsFront, Ghostwriter, Europa Środkowa, Polska, NATO StratCom

1. Introduction: from propaganda and disinformation to cognitive warfare

Contemporary Russian information influence targeting Central Europe has evolved from classic propagandistic and disinformation techniques toward practices that the military and scholarly literature designate as cognitive warfare. These activities are designed to interfere with the cognitive processes of individuals and collectives, with entrenched interpretive schemas, and with decision-making mechanisms.[1] The literature emphasizes that cognitive warfare "strikes at trust as the social binder" and precedes or accompanies the kinetic phase, preparing the adversary's decision-making environment. In the NATO Review's analytical framing, the battlespace in this type of confrontation is the human mind, and the objective is not only to modify what audiences think, but also how they think and act.[2]

In this context, proxy sources constitute the covert supporting structures of propaganda-disinformation operations. They appear as ostensibly local media outlets, think tanks, blogs, news agencies, and not infrequently as private profiles and micro-influencers. Through overlapping layers of intermediation, they conceal the provenance of the message and lower audiences' threshold of skepticism. They render narratives more concrete by locally anchoring them, while simultaneously serving as content suppliers for channels regarded as at least relatively more credible (mainstream media, political actors, the commentariat).[3] Within such structures, the mechanism known as information laundering is most fully realized.[4]

---

[1] See: F. du Cluzel, *Cognitive Warfare*, Voltairenet, 22 January 2021, pp. 26-27, https://www.voltairenet.org/IMG/pdf/20210122_cognitive_warfare.pdf?utm_source=chatgpt.com [date of access: 29.08. 2025]; Ch. Deppe, G. S. Schaal, *Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept*, "Frontiers in Big Data" 2024, vol. 7, article 1452129, pp. 1-2 https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full [date of access: 29.08.2025]..

[2] K. Cao, S. Glaister, A. Pena, D. Rhee, W. Rong, A. Rovalino, S. Bishop, R. Khanna, J. Singh Saini, *Countering Cognitive Warfare: Awareness and Resilience*, "NATO Review" 20 May 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [date of access: 29.08. 2025].

[3] U.S. Department of State, Global Engagement Center (GEC), *Pillars of Russia's Disinformation and Propaganda Ecosystem,* https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf [date of access: 31.08. 2025]; J. Sikorski, *Źródła pośredniczące (proxy sources) w komunikacji politycznej jako narzędzie walki informacyjnej* [Proxy sources in political communication as a tool of information warfare], [in:] *Komunikowanie polityczne i publiczne w nowych mediach: wybrane przykłady* [Political and Public Communication in New Media: Selected Examples], eds. A. Grzechynka, K. Szmyd, Kraków 2025, pp. 166-187; idem, *Online analytics portal as an information warfare tool of the Russian Federation and its impact after 24 February 2022: case study: RuBaltic.ru*., "Sõjateadlane (Estonian Journal of Military Studies)" 2023, vol. 23, pp. 188-190.

[4] ADMM Cybersecurity & Information CoE (ACICE), *Update on the Information Domain – Information Laundering (Issue 05/24), May 2024*, pp. 1-4, https://www.acice-asean.org/files/may_24_info.pdf [date of access: 29.08. 2025]..

2. Methodology

The aim of this article is to determine the role and operating mechanics of proxy sources – intermediary, ostensibly independent content carriers – within Russian influence operations in Central Europe in the logic of cognitive warfare; to present their typology and the sequencing of narrative flows; to specify indicators for their identification; and to formulate policy-institutional recommendations, with particular emphasis on Poland and its broader Central European environment (in particular the Baltic and Visegrad states).

The study is situated within Critical Security Studies (a constructivist-post-positivist variant with poststructuralist inspirations), which foregrounds the constitutive role of language and discourse in constructing "security problems" and in reproducing or contesting power relations. In this sense, the article draws on the conceptual vocabulary developed by Peoples and Vaughan-Williams and other CSS scholars, treating security not as a fixed condition but as an effect of practices of (in) securitization and meaning-making. At the same time, it engages with the emerging literature on information/technology and warfare that conceptualizes contemporary conflicts as taking place in hybrid, techno-communicative environments shaped by algorithmization, platform logics, and dataveillance practices. By bringing these two strands together, the article adopts a critical perspective on the infrastructural conditions that allow cognitive influence and symbolic violence to be "scaled" through intermediary sources rather than focusing solely on overt propaganda outlets.

The novelty of the approach is threefold. First, it proposes to treat proxy sources as *structural* components of Russian cognitive warfare rather than as merely marginal or auxiliary channels. Second, it links the concept of information laundering to a concrete taxonomy of intermediaries and to empirically documented case studies (Ghostwriter, NewsFront), thus moving beyond purely conceptual treatments. Third, it integrates an analysis of the regional techno-regulatory environment (including DNS-level interventions and sanctions) with a methodology-oriented discussion of how indicators of proxy activity can be operationalized in practice. Taken together, these elements position the article at the intersection of Critical Security Studies, disinformation research, and the emerging debate on cognitive warfare.[5]

The article poses three research questions:

RQ1. What role do proxy sources play in the process of "information laundering," and to what extent do they facilitate the "legalization" of content within mainstream messaging in Central and Eastern Europe?

[5] C. Peoples, N. Vaughan-Williams, *Critical Security Studies: An Introduction – 3rd edition*, Abingdon–New York 2021, pp. 6, 104, 182-183, 197-198.

RQ2. Which indicators best distinguish proxy sources from ordinary content replicators?

RQ3. Under what linguistic–institutional conditions are proxy sources most effective in Poland and the broader Central European region (in particular the Baltic and Visegrad states)?

These questions form an integrated research design. RQ1 focuses on the *functions* of proxies within narrative flows; RQ2 operationalizes this perspective into observable *indicators* that allow proxies to be distinguished from ordinary content aggregators; and RQ3 links both layers to the *contextual conditions* that either facilitate or constrain the effectiveness of proxy sources in Poland and its regional environment. Together, they structure the subsequent empirical sections of the article (architecture of the ecosystem, case studies, regional frameworks, and methodological implications).

On this basis, the following three hypotheses are formulated:

H1. The presence of proxy sources increases the likelihood that a narrative will progress through the sequence placement → layering → integration and enter the mainstream.

H2. Persistent "link bridges"[6] to recognizable hubs, close temporal coincidences, and multilingual replication are key markers of proxy sources.

H3. The effectiveness of proxy sources increases when local linguistic intermediaries are present and verification/response mechanisms within the media ecosystem are weak.

The hypotheses correspond directly to the research questions: H1 mirrors RQ1 by specifying the expected effect of proxies on narrative progression; H2 translates RQ2 into a testable set of diagnostic cues; and H3 provides an empirically oriented answer to RQ3 concerning the enabling conditions of proxy effectiveness. Although a short article format imposes limits on the level of disaggregation, keeping this 3+3 structure makes it possible to maintain an analytically clear distinction between mechanisms (H1), markers (H2), and contextual conditions (H3), while still treating them as parts of a single, coherent research design.

[6] Link bridges are auxiliary, typically low-quality websites created solely to redirect traffic to a target site. This is a so-called black-hat SEO technique, contrary to Google's guidelines, and subject to penalties such as ranking demotion or even removal from the index. Google Search Central, *Spam policies for Google web search*, "Google for Developers" 10 June 2025, https://developers.google.com/search/docs/essentials/spam-policies [date of access: 30.09. 2025]; B. White, *An update on doorway pages*, "Google Search Central Blog" 16 March 2015, https://developers.google.com/search/blog/2015/03/an-update-on-doorway-pages [date of access: 30.09.2025]; Google Support, *Manual actions report,* "Search Console Help" [n.d.], https://support.google.com/webmasters/answer/9044175 [date of access: 30.09.2025]; Google Search Central, *Link best practices for Google*, "Google for Developers" 4 Feb. 2025, https://developers.google.com/search/docs/crawling-indexing/links-crawlable [date of access: 30.09.2025].

Verification of the hypotheses and answers to the research questions were achieved through a qualitative review of the relevant literature and documented case studies. Methodological triangulation – combining cross-linguistic comparisons, reconstruction of citation and link chains, and narrative frame analysis – was used to enhance the reliability of the findings and to ensure that the proposed indicators are robust across different sources and sub-regions of Central Europe.

3. "Proxy sources" and information laundering: definitions, mechanics, indicators

In the NATO StratCom COE's framing, information laundering denotes a process whereby false or misleading content is systematically introduced into circulation via a network of intermediaries so as to obscure the provenance of the message and lend it an appearance of credibility.[7] In turn, at a meeting of ministers responsible for cybersecurity and information from Association of Southeast Asian Nations (ASEAN) member states, it was noted that initiation of this process most often occurs in closed environments (forums, niche channels), from which – using multiple coordinated accounts and platforms – the message gradually permeates mainstream media communications and, through selective fact-picking, contextual manipulation, and the instrumental use of statements by political actors, becomes commingled with credible news until it is fully integrated into the information ecosystem.[8]

In the scholarly literature, the sequence of information laundering comprises three stages:

1. Placement – the initial insertion of content into the public sphere (e.g., on a quasi-portal or blog),
2. Layering – cascading repetitions across related channels, often with references to statements by politicians or to "alternative" media; and
3. Integration – uptake by mainstream media or entry into official debates, which confers a distinctive "quality stamp."[9]

As current findings indicate, these phases may overlap, and the "legalization" of content can result both from an intentional plan and from the opportunistic dynamics of platforms.[10]

---

[7] NATO Strategic Communications Centre of Excellence (NATO StratCom COE), *Information Laundering in Germany*, p. 4, https://stratcomcoe.org/publications/information-laundering-in-germany/23 [date of access: 31.08. 2025].

[8] Ibidem; ACICE, *Update on the Information Domain…*, op. cit., pp. 1-4.

[9] Ibidem.

[10] RESET: Digital for Good, *The Ghostwriter Campaign. A Multi-Vector Information Operation: Attempts to Control Its Influence & the Limitations of Current Countermeasures*, London 2023, pp. 20-22, https://www.reset.tech/publications/the-ghostwriter-campaign-report/ [date of access: 31.08. 2025].

In these processes, proxy sources play a distinctive role, betraying their function through recurrent "link bridges" to a narrow set of hubs (including Sputnik/RT, NewsFront, and the Strategic Culture Foundation), synchronization of publications at short temporal intervals, formulaic multilingual translations, and regular "reciprocal citations" among the same entities (so-called legitimization loops.)[11]

4. The Architecture of the Russian Information Ecosystem and the Role of "Proxies"

International analyses conducted by NATO, the Global Engagement Center (GEC), and the International Centre for Counter-Terrorism (ICCT) consistently indicate that Russian information operations function within an ecosystem that links official state channels with an extensive network of "shell" institutions and intermediaries. The multiplicity of facades plays a crucial role here – ranging from entities masquerading as think tanks, through quasi-news agencies, to simple blogs. The dense web of their covert and ambiguous connections disperses responsibility and complicates the attribution of message sources.[12] From the perspective of cognitive warfare, this mechanism increases the likelihood of reaching diverse audience segments (including experts, military personnel, and activists), while, through "local" intermediaries, it helps to overcome cultural and linguistic barriers.[13]

A variety of entities can be classified as proxy sources. These include quasi-news agencies and "shell" think tanks. Examples of such entities are NewsFront, a quasi-news agency based in the occupied Crimea, and the Strategic Culture Foundation (SCF), a supposedly independent platform for global analysis whose involvement and connections (including with the Foreign Intelligence Service [SVR]) have been identified in both European and U.S. sanction documents.[14]

---

[11] NATO StratCom COE, *Russia's Footprint in the Nordic-Baltic Information Environment: Report 2016/2017*, project director: E. Lange-Ionatamišvili; research team: I. Bērziņa, M. Cepurītis, D. Kaljula, I. Juurvee, Riga 2018, pp. 54-55, 76-77; J. Gallacher, M. Heerdink, *Measuring the effect of Russian Internet Research Agency information operations in online conversations*, "Defence Strategic Communications" 2019, vol. 6, pp. 155-198; T. P. Gerber, J. Zavisca, *Does Russian Propaganda Work?* "The Washington Quarterly" 2016, 39(2), pp. 79-98.

[12] Ch. Deppe, G. S. Schaal, *Cognitive warfare: a conceptual analysis…*, op. cit., pp. 1-3.

[13] F. du Cluzel, *Cognitive warfare…*, op. cit., p. 7; Ch. Deppe, G. S. Schaal, *Cognitive warfare…*, op. cit., pp. 5-8.

[14] Council of the European Union (CEU), *Council Implementing Regulation (EU) 2022/260 of 23 February 2022 implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine*, "Official Journal of the European Union" 23 Feb. 2022, L 42 I/11; United States. Department of the Treasury. Office of Foreign Assets Control, *Notice of OFAC Sanctions Actions*, Federal Register 20 Apr. 2021, vol. 86, no. 74, p. 20598, 20600-20601 (FR Doc. 2021–08087), https://www.govinfo.gov/content/pkg/FR-2021-04-20/pdf/2021-08087.pdf [date of access:]; M. Leitenberg, *Russian disinformation related to biological weapons, 1998–2021*, annex to: M. Leitenberg, *False allegations of biological-weapons from Putin's Russia*, "The Nonproliferation Review" 2020, vol. 27, nr 4-6, p. 77; supplemental material (appendix),. [do czego appendix?]

The selection of examples used in this article follows a purposive logic. Entities such as NewsFront, the Strategic Culture Foundation, and related "shell" outlets have been repeatedly identified in high-quality analytical reports by NATO StratCom COE, the U.S. State Department's Global Engagement Center, and the International Centre for Counter-Terrorism as central hubs in the Russian disinformation and propaganda ecosystem. They appear not only as content producers but also as organizers of distribution chains that systematically rely on intermediary platforms and local amplifiers. Focusing on these actors makes it possible to trace relatively well-documented chains of content flow – from overt state-linked nodes to ostensibly independent intermediaries – and to illustrate how proxies operate at the intersection of official messaging, social media operations, and cyber-enabled techniques.

These also include intermediaries embedded within the target linguistic environment, as multilingualism is a prerequisite for effectively reaching intended audiences. For instance, NewsFront distributes content in multiple languages, combining a consistent core narrative with localized elements (e.g., anti-immigration slogans in messages aimed at German-speaking audiences, or anti-elitist themes in the English-language version). This mechanism is designed to reinforce the impression of "native media," which are more likely to be cited by politicians and journalists. Their role also involves the multiplication of narratives and the introduction of such narratives into public discourse.[15]

5. Case Studies: The Role of "Proxies" in Credibilizing Narratives

It appears that one of the best-documented examples of the use of proxy sources in disinformation and propaganda campaigns is Operation "Ghostwriter", reconstructed in a 2023 report by Cardiff University. The study revealed the multi-vector nature of the operation, which combined hacking techniques (such as defacement and account takeovers), impersonation of public officials, and the publication of fabricated "articles" on quasi-news portals and blogs that were subsequently systematically amplified. It was established that the campaign's activity dates back to at least 2016, with its initial area of focus being NATO's presence in the Baltic states. Around 2019/2020, the operation's vector expanded to include Poland.

In this context, a significant role was played by the right-wing portal "Niezależny Dziennik Polityczny" (NDP), known for its pro-Kremlin sympathies. The fabricated stories often revolved around recurring narrative frames: questioning the reliability and professionalism of NATO troops deployed in the region, suggesting

[15] See: NATO StratCom COE, *Information Laundering in Germany*, op. cit.; NATO StratCom COE, *Russia's footprint in the Nordic-Baltic information environment…*, op. cit., pp. 6, 32-46, 54, 57, 59, 69, 75-78.

internal fractures within the Alliance, and portraying Polish authorities as subservient to Washington. In several cases documented by investigative outlets and official communications, forged letters or alleged "leaks" were published on quasi-portals, then quickly republished by a network of small websites and social media profiles, which lent them an appearance of independent corroboration. An analysis of the distribution of content published on NDP indicated that dissemination occurred primarily through a network of interconnected social media accounts, especially on Facebook.[16]

The mechanism of dissemination operated as follows: after the publication of fabricated materials on institutional websites,[17] hyperlinks to the alleged "articles" were massively propagated – among others through portals such as lewy.pl, prawy.pl, and podlasie24.pl – which allowed them to achieve significant reach and engagement, while being simultaneously replicated on external platforms (e.g., The Duran, Verity Weekly).[18] A recurrent motif in these texts was the suggestion that the presence of Allied troops undermined local security or that alleged misconduct by soldiers was being deliberately covered up by authorities. Another notable feature was the persistence of some links on Twitter even after the original posts had been removed. Despite the later deletion of NDP accounts on certain platforms, traces of distribution and video materials remained accessible, confirming the durability of the informational contamination effect. Polish intelligence services publicly pointed to the connections between NDP and Russian intelligence activities, emphasizing the risks associated with the continued circulation of such content.[19]

[16] RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 2-4, 6, 9-10, 24.

[17] On April 22, 2020, a cyberattack targeted the website of the War Studies University (Akademia Sztuki Wojennej), during which a forged letter was published, allegedly authored by the commandant, Gen. Ryszard Parafianowicz, calling on Polish soldiers to "rebel" against the "American occupying forces." Subsequently, spoofed emails (impersonating, among others, a former Civic Platform MP and an American journalist) were sent to NATO institutions and Polish government agencies, containing links to the fabricated document. The material was replicated in English on the The Duran website and as "news" on Polish portals lewy.pl, prawy.pl, and podlasie24.pl (which later claimed to have been hacked). The message was further amplified by accounts linked to NDP. The War Studies University warned about the breach the same day on Twitter, and analyses by intelligence services and fact-checkers were published the following day. See: Rzecznik Ministra Koordynatora Służb Specjalnych [Spokesperson for the Minister Coordinator of Special Services], *Atak dezinformacyjny na Polskę [PL/EN]*. Gov.pl – Służby specjalne [*Disinformation attack on Poland* [PL/EN]. Gov.pl – Special Services], April 23, 2020, https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske [date of access: 30.09.2025).

[18] A. Gielewska, *Russia-related accounts and a cyberattack in Poland*, https://vsquare.org/russia-related-accounts-and-a-cyberattack-in-poland/ [date of access: 30.09.2025]; Digital Forensic Research Lab (DFRLab), *Cyber-enabled disinformation campaign targeted U.S.-Poland alliance,* https://dfrlab.org/2020/06/24/cyber-enabled-disinformation-campaign-targeted-u-s-poland-alliance/ [date of access: 30.09. 2025).

[19] RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 6-7; Pełnomocnik Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP [Government Plenipotentiary for the Security of the Information Space of the Republic of Poland], *Rosyjska sieć kłamstw [Russia's web of lies]*, czy to jest źródło internetowe? 2023, pp. 16-17; K. Kuśmirek, *Działania informacyjne Federacji Rosyjskiej w 2023 roku [Information activities of the Russian Federation in 2023]*, "Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30, pp. 90, 347.

A second representative example of the use of proxies is NewsFront, which serves both as a distribution hub and as a kind of narrative "framework." In European Union documents, NewsFront is identified not only as a media outlet but also as an organizer of content flows, directly linked to undermining Ukraine's territorial integrity and destabilizing the region. Operationally, it functions as a "wholesaler" of ready-made narratives, easily adaptable for local "packaging" and distribution. Typical storylines include portraying the EU as being in permanent crisis, questioning the legitimacy of sanctions against Russia, or depicting Ukraine and NATO as aggressive actors responsible for escalation. Once supplied by central "hubs" (such as NewsFront), the introduction of these narratives into national information spaces is carried out by smaller proxies – niche portals, blogs, and social media channels – that increase the likelihood of the messages infiltrating mainstream discourse.[20]

6. "Proxy Sources": Taxonomy, Patterns, Tactics

"Proxy sources" are communication channels formally operating outside state structures, which integrate official messaging, state media, social media operations, and the cyber component, multiplying narratives and giving them an appearance of grassroots authenticity[21]. Based on the Global Engagement Center (U.S. Department of State) framework regarding the pillars of Russian propaganda and disinformation, at least four types of such intermediaries can be distinguished:

1. Semi-official periodicals with an academic façade (e.g., Strategic Culture Foundation, New Eastern Outlook), which serve to legitimize state narratives,
2. Ideologically driven quasi–think tanks (e.g., Katehon, Geopolitica.ru), providing meta-narratives and interpretative frameworks,
3. External amplifiers with a "Western face" (e.g., Global Research), which "launder" the message through cross-publications; and
4. Operational content distributors (e.g., NewsFront, SouthFront), conducting rapid diffusion campaigns.[22]

This perspective is reinforced by the European Union's sanctions framework, which identifies not only the "faces of propaganda" (including Margarita Simonyan, Maria Zakharova, Vladimir Solovyov), but also the operators (e.g., Konstantin Knyrik/NewsFront), online executors (such as the Internet Research Agency), and financial enablers (Bank Rossii, PSB, VEB.RF).[23]

[20] Ibidem, p. 6; CEU, *Council Implementing Regulation (EU) 2022/260*…, op. cit., pp. 8-9.
[21] GEC, *Pillars of Russia's Disinformation and Propaganda Ecosystem*..., op. cit., pp. 7, 11-13.
[22] Ibidem, pp. 14-60.
[23] CEU, *Council Implementing Regulation (EU) 2022/260 of 23 February 2022*…, op. cit., L 42 I, L 42 I/10–L 42 I/14.

In turn, an analysis of the mechanics by which proxy sources operate makes it possible to identify four recurring operational patterns:

1. Building interlingual bridges: the same thesis is rapidly translated and distributed in successive language versions (e.g., EN→DE→PL), with each iteration accompanied by a subtle shift of emphasis (for instance, moving from a focus on "health security" toward "individual freedom" or from "sanctions" toward "economic self-harm"). NATO StratCom COE's studies of information laundering in Germany and the Nordic-Baltic region repeatedly documented identical or near-identical articles appearing across multiple language versions within short intervals, often citing each other as "independent" sources.
2. An amalgam of facts and opinions: combining genuine quotations with an overlaid interpretation, often through misappropriation or the use of misleading language, repeatedly documented in the recommendations of the ADMM Cybersecurity & Information Centre of Excellence (ACICE). In this pattern, seemingly neutral factual statements (e.g., about troop movements or parliamentary debates) are embedded in a narrative frame that suggests hidden motives, conspiracies, or imminent threats, without making explicit factual claims that could be easily disproven.[24]
3. Cyclical activation of "boosters": coordinated, short-term publication of convergent content across several affiliated portals and Telegram/Facebook channels generates a reach impulse (burst) and artifacts of "perceptual consensus." The Ghostwriter campaign provides concrete examples: shortly after the appearance of a forged letter or statement on a quasi-portal, a wave of small sites and social media accounts would circulate similar headlines or commentaries, creating the impression that "everyone is talking about it," even though the content originated from a single operation.
4. "Recycling" scandals: returning to previously fabricated or debunked stories (e.g., the "Lisa 2.0" case in Germany) in new political–media contexts reactivates emotions and keeps the narratives in circulation. Here, minor modifications (such as changing the location, alleged victim, or institutional actor) give the impression of a "new" case, while the underlying storyline – for example, that authorities allegedly conceal crimes or that migrants are systematically protected from accountability – remains stable. Such recycling has been observed both in the German-language and Central European information spaces.[25]

[24] ACICE stands for ADMM Cybersecurity & Information Centre of Excellence, a regional cooperation center operating at the ASEAN Defense Ministers' Meeting. Established in June 2021, its mission is to support information exchange and build defense capabilities in ASEAN against cyberattacks and disinformation. ASEAN, *About ADMM*, 28 April, 2025, https://admm.asean.org/index.php/about-admm/about-admm.html [date of access: 6.10.2025]; ACICE, *Update on the Information Domain*..., op. cit., p. 2.

[25] Ibidem, pp. 2-4.

The "Ghostwriter" practice further illustrates the coupling of information tactics with the cyber component. Account and website takeovers (the compromise of digital identity) are combined with publishing materials through proxy channels and subsequent amplification on social media. In turn, giving messages an appearance of "authenticity" by impersonating recognizable newsrooms or public offices increases their perceived credibility and strengthens the distribution leverage of both the content "wholesalers" and the local intermediaries responsible for further disseminating the message.[26]

7. Cognitive Warfare: Where Do Proxies "Touch" the Mind?

In the scholarly literature, cognitive warfare – described as a maximalist concept – extends classical understandings of the battlespace to encompass mental and social dimensions.[27] From this perspective, so-called proxy sources function as "cognitive adapters." First, they reduce cognitive dissonance by appealing to the audience's group identity ("this is written by our people"), for example when quasi-portals such as NDP use national symbols and local references to present narratives aligned with Kremlin interests as "patriotic" or "pro-sovereignty." Second, they enhance the credibility of the message by layering intermediaries, which lends information an appearance of ubiquitous presence ("everyone is writing about this"), as seen in the cascading republication of Ghostwriter-related forgeries across minor websites and social media accounts. Third, they activate heuristics of authority, consensus, and availability, thereby lowering the cognitive cost of critically verifying content – for instance, when English-language narratives originating from NewsFront are reproduced by ostensibly independent Western-facing portals and then cited back in national debates as "foreign expert opinions."

Findings from Innovation Hub[28] analyses indicate that the key objective of activities in the realm of cognitive warfare is trust. Its erosion leads to lasting changes in how sources are assessed, thereby increasing the susceptibility of individuals and collectives to manipulation.[29] Empirical observations from the Nordic-Baltic region further suggest that these processes resulted in measurable fluctuations in the perceived risks associated with NATO's presence, migration phenomena, and the narrative of "discrimination against Russian speakers."[30]

[26] RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 2-4, 9-10.

[27] Ch. Deppe, G. S. Schaal, *Cognitive warfare: a conceptual analysis…*, op. cit., pp. 1-3.

[28] The Innovation Hub (IH) is an open community and collaborative platform run by NATO Allied Command Transformation (ACT), bringing together military and civilian experts to collaboratively identify challenges and develop ideas and solutions for the Alliance (including a community, online platform, knowledge base, and the NATO Innovation Challenge). NATO Allied Command Transformation, *Innovation Hub*, https://www.act.nato.int/activities/innovation-hub/ [date of access: 30.09.2025).

[29] F. du Cluzel, *Cognitive warfare…*, op. cit., pp. 7, 27.

[30] NATO StratCom COE, *Russia's footprint in the Nordic-Baltic…*, op. cit., pp. 5-6, 29-30, 35-38, 45-46, 59.

The case studies discussed in this article support this interpretation. In the Ghostwriter operation, the combination of hacked accounts, forged documents, and proxy websites produced a layered structure in which each intermediary appeared to confirm the others, thereby strengthening the perception that "many independent outlets" were reporting the same allegations. In the NewsFront ecosystem, multilingual channels and local proxies provided a similar effect: narratives framed centrally were adapted to national contexts, cited by fringe actors, and occasionally picked up by mainstream outlets as "controversial but relevant views." In both cases, proxies did not simply increase technical reach; they altered how audiences processed information, making disinformation more cognitively "fluent" and less likely to be questioned.

8. Poland and Central Europe: Institutional Frameworks and Resilience Practices

On the day Russia launched its full-scale invasion of Ukraine, CZ.NIC, the Czech association managing the .cz domain registry,[31] after consultations with the competent services, temporarily removed 8 disinformation domains from the DNS. A mechanism for the periodic review of domains was also introduced, along with a time limit on blocking that – if continued beyond three months – requires a decision by the competent authority. Additionally, a public register of domains excluded from the DNS was created, as well as pages listing administratively withdrawn names.[32] As it turned out, such infrastructural interventions (DNS, national registries) can effectively disrupt the content supply chain from intermediaries, provided they are accompanied by transparency and a clear legal basis.[33] In line with these practices, EU sanctions targeting entities that organize the "wholesaling" of narratives (e.g., NewsFront) likewise produced a significant chilling effect and made platform moderation easier.[34]

Thus, the neutralization of proxy sources is possible within the framework of the rule of law, provided that actions are transparent and based on clear legal principles. Unfortunately, reviews of the activities of the vast majority of Western states indicate that there are still significant deficiencies in the areas of rapid attribution and transnational coordination of responses to disinformation and propaganda campaigns.[35]

[31] *About association*, https://www.nic.cz/page/351/ [date of access: 6.10. 2025].

[32] Compare the mechanics of "wholesalers" and local intermediaries: RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 5-6, 9-10, 14-15; NATO StratCom COE, *Russia's footprint in the Nordic-Baltic information environment…*, op. cit., pp. 5, 7, 74; CZ.NIC, *Annual Report 2022*, Prague2023, pp. 7, 26, 75-76, https://www.nic.cz/files/nic/230821_CZNIC_vyrocni_zprava_2022_EN.pdf [date of access: 13.09.2025].

[33] CZ.NIC, *Annual Report 2022*…, op. cit., pp. 5, 26, 74-76.

[34] CEU, *Council Implementing Regulation (EU) 2022/260…*, op. cit., pp. 3-4, 11, 13.

[35] V. Witkowska, V. Krátka Špalková, *Czech Republic: Echoes of Discontent – Far-Right Populism and the Disinformation Dilemma*, [in:] *Russia and the Far-Right…*, op. cit., pp. 253-255.

Against this backdrop, Poland fits into a broader Central European pattern: while there is a strong and enduring consensus on EU and NATO membership, certain soft points of vulnerability remain. These are formed by political and social circles that, for ideological or opportunistic reasons, amplify pro-Kremlin narratives – particularly in the areas of security, energy, and migration. Analyses by the International Centre for Counter-Terrorism (ICCT) indicate that some of these circles function as "narrative laboratories," where specific forms of language and storytelling are tested. Subsequently, often through proxy channels, these narratives permeate the wider public discourse.[36]

Although historical and cultural conditions make Poland a difficult environment for openly pro-Russian initiatives, the risk has not disappeared. Radical communication channels on both ends of the political spectrum, sharing elements of the pro-Kremlin repertoire, function as "proxy nests" and facilitate the transfer of content from "narrative wholesalers" (e.g., NewsFront) into the Polish infosphere, where – under favorable conditions – they undergo further legitimization and diffusion.[37]

9. Methodology for Detecting and Limiting the Influence of Proxy Sources

Effectively mitigating the impact of informational intermediaries requires the integration of network analytics, temporal sensitivity, and content assessment across a multilingual environment. Drawing on the patterns reconstructed in the preceding sections – in particular the sequence placement → layering → integration, the role of legitimization loops, and the regional experiences of DNS-level and sanctions-based interventions – this section translates the article's findings into a set of methodological guidelines for detecting and limiting the influence of proxy sources. In other words, it presents the *practical* implications of the answers to RQ1–RQ3 and of the qualitative verification of H1–H3, outlining how the proposed indicators can inform audits, editorial policies, and regulatory measures in Poland and Central Europe.[38]

[36] P. Witkowski, *Poland: Ex Oriente Lux*, [in:] *Russia and the Far-Right: Insights from Ten European Countries*, eds. K. Rekawek, T. Renard, B. Molas (ed.), The Hague 2024, pp. 305-306, 310-311, 318-319.

[37] For an overview of the limited room for openly pro-Russian initiatives in Poland, rooted in specific historical and cultural conditions, and of the role of fringe far-left and far-right actors and media as key vectors of pro-Kremlin narratives, see: Ł. Wenerski, M. Kacewicz, *Russian soft power in Poland: The Kremlin and pro-Russian organizations*, Budapest 2017, pp. 8-9; A. Yeliseyeu, V. Laputska et al., *Major Pro-Kremlin Disinformation Narratives and Their Transmitters in Poland, Czechia, and Slovakia*, https://www.amo.cz/wp-content/uploads/2023/06/AMO_Pro-Russian-Narratives-in-Czech-Republic-Slovakia-and-Poland.pdf, M. Zadorożna, M. Butuc, *Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war*, "*Security and Defence Quarterly" 2024, no.* 46(2), pp. 47-65; P. Witkowski, *Poland: Ex Oriente Lux*…, op. cit., pp. 305-311, 317-319.

[38] The report identifies the following as "behavioral signatures" of the Ghostwriter campaign: 1. a cyber component preceding the influence phase (gaining access to websites/profiles), 2. a typical focus on

In addition, the audit should also encompass multilingual replication pathways. A typical marker in this regard consists of identical articles appearing in two or three languages within intervals of several hours or days, as well as content indicators – that is, stable narrative frameworks (e.g., "NATO = a threat," "discrimination against Russian speakers," "the EU in collapse") – whose persistent presence has been demonstrated in studies conducted by NB8 NATO StratCom.[39]

The preventive layer should be based on prebunking and so-called "resilience headers," understood as pre-agreed editorial and institutional guidelines that reduce the information system's vulnerability to "content laundering." The ACICE recommendations emphasize, among other things, the avoidance of language that facilitates the legitimization of messages of uncertain provenance, as well as the practice of coordinated silence during periods of heightened sensitivity.[40] A model example in this context remains the response of the electoral commission to the "Macron Leaks" case.[41]

Transferring such measures to the Polish and regional context would require agreed-upon operational protocols among newsrooms, public administration, and platforms, including clear escalation procedures and shared risk lexicons.

The final component of the detection methodology is the response sphere involving platforms and regulators. This includes the mapping of network nodes and the whitelisting of reliable sources (with clearly defined qualification criteria and an appeal mechanism), and – where appropriate and proportionate – short-term

the military thread and targets in Central and Eastern Europe, 3. frequent use of fabricated content provoking official denials, 4. hybrid distribution (inauthentic accounts, email spoofing, impersonation + use of compromised but real websites and accounts), 5. strict "scheduling" of important events (visits, exercises), rarely ad hoc reactions. See: RESET: Digital for Good, *The Ghostwriter Campaign…*, op. cit., pp. 5-7, 8, 10-12, 16-17.

[39] NB8 NATO StratCom – an initiative of eight Nordic-Baltic countries (Denmark, Finland, Iceland, Norway, Sweden, Estonia, Latvia, Lithuania) cooperating in the area of NATO strategic communications, including a coherent alliance narrative, coordination of information and psychological activities, and countering disinformation, including in cooperation with the NATO StratCom Centre of Excellence in Riga. See: NATO StratCom COE, *Russia's Footprint…*, op. cit., pp. 4-5, 54-55, 57, 59, 65-66, 69, 76-77.

[40] ACICE, *Update on the Information Domain…*, op. cit., pp. 4-5.

[41] On Saturday, May 6, 2017, the state Electoral Campaign Control Commission called on the media and citizens not to publish or disseminate leaked materials during the election silence period, reminding them of the possible legal consequences. Following the appeal, "Le Monde," among others, announced that it would not report on the content until the end of the vote. See: E. Schultheis, *The Macron Leaks Probably Came Too Late to Change the French Election*, "The Atlantic" 6 May 2017, https://www.theatlantic.com/international/archive/2017/05/france-macron-leak-hack/525738/ [date of access: 6.10.2025]; J.-B. Vilmer Jeangène, *The "Macron Leaks" Operation: A Post-Mortem*, Washington, DC, Paris2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf [date of access: 6.10.2025]; K. Willsher, *French media warned not to publish Emmanuel Macron leaks*, "The Guardian" 6 May 2017, https://www.theguardian.com/world/2017/may/06/french-warned-not-to-publish-emmanuel-macron-leaks [date of access: 6.10.2025]; REUTERS, *France warns against republishing hacked Macron campaign emails, 6 May 2017*, https://www.reuters.com/article/world/france-warns-against-republishing-hacked-macron-campaign-emails-idUSL9N1GD01N/ [date of access: 6.10.2025].

distribution measures at the level of DNS, hosting, and advertising systems, all based on transparent criteria and appeal procedures. The CZ.NIC experience demonstrates that transparency and the temporary nature of interventions increase public acceptance and reduce the risk of excessive interference, while also serving as an effective tool for disrupting the content supply chains of intermediaries.[42]

10. Conclusions

The aim of this article was to reconstruct the role and operational mechanics of proxy sources in Russian influence operations in Central Europe, with particular emphasis on the sequence of "information laundering" (placement → layering → integration) and the identification of indicators for detecting narrative intermediaries. The research design combined a qualitative review of secondary data with illustrative case studies (Ghostwriter, NewsFront) and an analysis of the regional institutional environment in Poland and its broader Central European context. Methodologically, the study relied on triangulation: cross-linguistic comparisons, reconstruction of citation and link chains, and narrative frame analysis were used to capture both the structural and contextual dimensions of proxy activity.

With regard to RQ1, concerning the role of proxy sources in information laundering, the analysis supports H1. Based on the literature and existing data, it has been shown that proxy sources serve as latent structural carriers, masking the origin of messages and increasing their perceived credibility through legitimization by layers of intermediation. The Ghostwriter campaign and the NewsFront ecosystem illustrate how intermediaries make it more likely that narratives will progress from initial placement on quasi-portals to layering across multiple minor outlets and, ultimately, integration into mainstream debates. Proxies thus do not merely replicate content; they facilitate the transition between phases in the laundering process.

In answering RQ2, which asked about indicators that distinguish proxies from ordinary content replicators, the findings support H2. The most useful markers were found to be: (1) recurrent "link bridges" to a fixed pool of diffusion nodes (e.g., NewsFront, SCF), (2) short-window temporal coincidences of publications across multiple channels, and (3) multilingual replications maintaining a stable narrative core with local shifts in emphasis. The identification of legitimization loops (A→B→C→A) and "boosters" operating in coordinated bursts further refines this picture. Taken together, these indicators can inform practical procedures for detecting and cutting off distribution streams without relying solely on content-based assessments.

[42] CZ.NIC, *Annual Report 2022*…, op. cit., pp. 7, 26, 45, 75-76.

As for RQ3, addressing the linguistic–institutional conditions under which proxy sources are most effective in Poland and the broader Central European region, the evidence lends support to H3. The key enabling factors are the presence of local linguistic intermediaries, who lend the message an appearance of "nativeness," and institutional gaps such as weak editorial verification standards, limited cross-border coordination, and the absence of agreed escalation protocols among newsrooms, platforms, and public authorities. At the same time, regional experiences – notably DNS-level interventions by CZ.NIC and EU sanctions targeting narrative "wholesalers" like NewsFront – indicate that it is possible to effectively limit the influence of proxies within the framework of the rule of law, provided that actions are transparent, proportionate, and accompanied by clear appeal mechanisms.

The qualitative nature of this article, based on secondary data, implies certain limitations. It cannot provide statistically generalizable estimates of the scale of proxy activity, nor does it exhaust the diversity of actors and narratives involved in Russian influence operations in Central and Eastern Europe. Nevertheless, the findings point to several promising directions for future research: network–temporal audits on defined datasets; quantitative measurements of delays between the placement, layering, and integration phases and estimation of "legalization" thresholds; comparative analyses across different languages and audience segments; and evaluation of the effectiveness of regulatory and platform interventions in cutting off "narrative wholesalers."

Building on the results, the article proposes an integrated approach to strengthening resilience against proxy sources. It combines (1) prebunking and "resilience headers" – i.e., agreed editorial guidelines standardizing the presentation of disinformation-related risks; (2) distribution network audits aimed at detecting legitimization loops and linguistic bridges; and (3) transparent, time-limited infrastructural interventions targeting diffusion nodes that act as intermediaries. A resilience ecosystem designed in this way – coherent, measurable, and coordinated – increases the likelihood of neutralizing intermediary sources before their messages reach the phase of mainstream integration, thereby addressing the core objective of cognitive warfare: the contestation and capture of trust.

Bibliography

1. ADMM Cybersecurity & Information Centre of Excellence (ACICE). *Update on the Information Domain — Issue 05/24 (May) Information Laundering*. ASEAN Defence Ministers' Meeting Cybersecurity & Information Centre of Excellence (ACICE), 01 May 2024, https://www.acice-asean.org/files/may_24_info.pdf.

2. ASEAN Defence Ministers' Meeting. *About the ASEAN Defence Ministers' Meeting* [online]. ASEAN Defence Ministers' Meeting (ADMM), 28 April 2025, https://admm.asean.org/index.php/about-admm/about-admm.html.
3. Cao K., Glaister S., Pena A., Rhee D.i, Rong W., Rovalino A., Bishop S., Khanna R., Saini J. S., *Countering Cognitive Warfare: Awareness and Resilience*. *NATO Review*, *20 May 2021*, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.
4. Council of the European Union (CEU), *Council Implementing Regulation (EU) 2022/260 of 23 February 2022 implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine*, "Official Journal of the European Union" 23 Febr. 2022 L 42..
5. CZ.NIC, *About association*, https://www.nic.cz/page/351/.
6. CZ.NIC, *Annual Report 2022*, https://www.nic.cz/files/nic/230821_CZNIC_vyrocni_zprava_2022_EN.pdf.
7. Deppe C., Schaal G. S., *Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept*, "Frontiers in Big Data" 2024, vol. 7, art. 1452129, https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full.
8. Digital Forensic Research Lab (DFRLab), *Cyber-enabled disinformation campaign targeted U.S.-Poland alliance*, https://dfrlab.org/2020/06/24/cyber-enabled-disinformation-campaign-targeted-u-s-poland-alliance/.
9. Du Cluzel F., *Cognitive Warfare*, https://www.voltairenet.org/IMG/pdf/20210122_cognitive_warfare.pdf.
10. Gielewska A., *Russia-related accounts and a cyberattack in Poland*, https://vsquare.org/russia-related-accounts-and-a-cyberattack-in-poland/.
11. Google Search Central, *Link best practices for Google*. *Google for Developers*, *4 Febr. 2025*, https://developers.google.com/search/docs/crawling-indexing/links-crawlable?hl=pl.
12. Google Search Central, *Spam policies for Google web search*. *Google for Developers, 10 June 2025*, https://developers.google.com/search/docs/essentials/spam-policies.
13. Google Support, *Manual actions report*. *Search Console Help*, https://support.google.com/webmasters/answer/9044175.
14. Kuśmirek K, *Działania informacyjne Federacji Rosyjskiej w 2023 roku [Information activities of the Russian Federation in 2023]*, "Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30 .
15. Leitenberg M., *Russian disinformation related to biological weapons, 1998–2021*. Annex to: Leitenberg M., *False allegations of biological weapons from Putin's Russia*, "The Nonproliferation Review" 2020, vol. 27, no. 4-6, appendix.
16. NATO Strategic Communications Centre of Excellence (NATO StratCom COE), *Russia's Footprint in the Nordic-Baltic Information Environment: Report 2016/2017*, project director: E. Lange-Ionatamišvili; research team: I. Bērziņa, M. Cepurītis, D. Kaljula, I. Juurvee, Riga 2018.
17. NATO Strategic Communications Centre of Excellence, *Information Laundering in Germany, 2019/2020*, Riga 2020.
18. Pełnomocnik Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP [Government Plenipotentiary for the Security of the Information Space of the Republic of Poland]. *Rosyjska sieć kłamstw [Russia's web of lies]*, 2023 źródło internetowe?.
19. Peoples C., Vaughan-Williams N., *Critical Security Studies: An Introduction – 3rd edition,* Abingdon–New York, 2021.

20. RESET: Digital for Good, *The Ghostwriter Campaign. A Multi-Vector Information Operation: Attempts to Control Its Influence & the Limitations of Current Countermeasures*, London2023, https://www.reset.tech/publications/the-ghostwriter-campaign-report/.
21. REUTERS, *France warns against republishing hacked Macron campaign emails*, *6 May 2017,* https://www.reuters.com/article/world/france-warns-against-republishing-hacked-macron-campaign-emails-idUSL9N1GD01N/.
22. Rzecznik Ministra Koordynatora Służb Specjalnych [Spokesperson for the Minister-Coordinator of Special Services], *Atak dezinformacyjny na Polskę[Disinformation Attack on Poland]*. https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske.
23. Schultheis E., *The Macron Leaks Probably Came Too Late to Change the French Election*, *"The Atlantic"* 6 May 2017, https://www.theatlantic.com/international/archive/2017/05/france-macron-leak-hack/525738/.
24. Sikorski J., *Źródła pośredniczące (proxy sources) w komunikacji politycznej jako narzędzie walki informacyjnej [Proxy sources in political communication as a tool of information warfare]*, [in:] *Komunikowanie polityczne i publiczne w nowych mediach: wybrane przykłady [Political and public communication in new media: selected examples],* eds. A. Grzechynka, K. Szmyd,. Kraków 2025.
25. Sikorski J., *Online analytics portal as an information warfare tool of the Russian Federation and its impact after 24 February 2022: case study: RuBaltic.ru*., "*Sõjateadlane (Estonian Journal of Military Studies)*" 2023, vol. 23.
26. United States Department of State, Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem*, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.
27. United States Department of the Treasury, Office of Foreign Assets Control, *Notice of OFAC Sanctions Actions*, "Federal Register" 20 April 2021 vol. 86, no. 74, (FR Doc. 2021–08087), https://www.govinfo.gov/content/pkg/FR-2021-04-20/pdf/2021-08087.pdf.
28. Vilmer J. J., *The "Macron Leaks" Operation: A Post-Mortem*, Washington, DC, Paris 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf.
29. Wenerski Ł., Kacewicz M., *Russian soft power in Poland: The Kremlin and pro-Russian organizations*, Budapest 2017.
30. White B., *An update on doorway pages*, "Google Search Central Blog" 16 March 2015, https://developers.google.com/search/blog/2015/03/an-update-on-doorway-pages.
31. Willsher K., *French media warned not to publish Emmanuel Macron leaks*, "The Guardian" 6 May 2017, https://www.theguardian.com/world/2017/may/06/french-warned-not-to-publish-emmanuel-macron-leaks.
32. Witkowska V., Krátka Špalková V., *Czech Republic: Echoes of Discontent – Far-Right Populism and the Disinformation Dilemma*,[in:] *Russia and the Far-Right: Insights from Ten European Countries*, eds.. K. Rekawek, T. Renard, B. Molas, The Hague2024.
33. Witkowski P., *Poland: Ex Oriente Lux,* [in:] *Russia and the Far-Right: Insights from Ten European Countries,* eds. K. Rekawek, T. Renard, B. Molas, . The Hague 2024.
34. *Yeliseyeu A., Laputska V. ., Havlíček P. , Nemečkayová N., Dubóczi P., Ružičková M., Major Pro-Kremlin Disinformation Narratives and Their Transmitters in Poland, Czechia, and Slovakia*, https://www.amo.cz/wp-content/uploads/2023/06/AMO_Pro-Russian-Narratives-in-Czech-Republic-Slovakia-and-Poland.pdf.
35. Zadorożna M., Butuc M., *Russian disinformation in Moldova and Poland in the context of the Russo-Ukrainian war*, "*Security and Defence Quarterly" 2024,* 46(2).

Part III:

State Security and the Legal and Institutional Framework

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 241–253

ISSN 2543-6961
e-ISSN 2720-3093

Roman Martyniuk
ORCID: 0000-0003-4469-7762
National University "Ostroh Academy"
Oleksii Datsiuk
ORCID: 0000-0003-2293-6371
National University "Ostroh Academy"
Mykola Romanov
ORCID: 0000-0002-1086-9485
National University "Ostroh Academy"

The Law of Ukraine "On National Security of Ukraine" dated June 21, 2018. Some Problematic Aspects

Ustawa Ukrainy „O bezpieczeństwie narodowym Ukrainy" z dnia 21 czerwca 2018 r. Wybrane problematyczne aspekty

Abstract
The Law of Ukraine "On National Security of Ukraine" dated June 21, 2018, establishes a number of the most important institutions in the field of national security and defense, individual elements of the mechanism for ensuring national security and defense capability of the Ukrainian state, and defines the structure of the security and defense sector of Ukraine. Along with the relevant provisions of the Constitution of Ukraine, it forms the regulatory basis of Ukrainian legislation in the field of national security and defense. In view of this, the shortcomings of the Law become of paramount importance, including cases of terminological inconsistency and uncertainty, problems associated with consolidating the scope and competence of subjects of the security and defense sector, attempts to fill gaps in constitutional regulation, and the lack of regulation of certain fundamental issues.

Keywords: national security and defense of the state, national interests, national values, security and defense sector, security forces, defense forces, constitution, law.

Abstrakt
Ustawa Ukrainy „O bezpieczeństwie narodowym Ukrainy" z dnia 21 czerwca 2018 r. ustanawia szereg kluczowych instytucji w sferze bezpieczeństwa narodowego i obrony, określa wybrane elementy mechanizmu zapewniania bezpieczeństwa narodowego oraz zdolności obronnej państwa ukraińskiego, a także definiuje strukturę sektora bezpieczeństwa i obrony Ukrainy. Wraz z odpowiednimi postanowieniami Konstytucji Ukrainy tworzy ona podstawę normatywną ukraińskiego ustawodawstwa w dziedzinie bezpieczeństwa narodowego i obrony. W konsekwencji, szczególnego znaczenia nabierają mankamenty tej ustawy, w tym przypadki niekonsekwencji i niejednoznaczności terminologicznej, problemy związane z utrwaleniem zakresu działania oraz kompetencji podmiotów sektora bezpieczeństwa i obrony, próby wypełniania luk w regulacji konstytucyjnej, jak również brak unormowania niektórych kwestii fundamentalnych.

Słowa kluczowe: bezpieczeństwo narodowe i obrona państwa, interesy narodowe, wartości narodowe, sektor bezpieczeństwa i obrony, siły bezpieczeństwa, siły obrony, konstytucja, ustawa.

Introduction

The Verkhovna Rada of Ukraine adopted the Law of Ukraine "On National Security of Ukraine" on June 21, 2018. Developing the provisions of the Constitution of Ukraine on national security and defense of the state, the Law establishes the foundations and principles of national security and defense of Ukraine as well as the goals and principles of state policy in the field of national security and defense; it establishes a number of the most important institutions in this area, individual elements of the mechanism for ensuring national security and defense capability of the Ukrainian state, and defines the structure of the security and defense sector of Ukraine.

A valuable feature of the Law is the consolidation of fundamental national interests of Ukraine in it, such as, in particular, comprehensive integration into the European space and membership in the European Union and the North Atlantic Treaty Organization. These and other national interests of Ukraine are formulated taking into account the vital material, intellectual and spiritual values of man, society, and the state. The normative definition of the national interests of Ukraine as fundamental social values causes systematic and purposeful activity of all subjects of the security and defense sector to ensure their real guarantee.

Terminological inconsistencies

The Law of Ukraine "On National Security of Ukraine" establishes a certain system of terms that should form the conceptual basis of legislation in the field of national security and defense. A notable feature of the Law is the rejection of the terminology inherited from the Soviet past and the use of terms established in the Western professional environment. For example, the term "military organization of the state", used in the Law of Ukraine "On the Fundamentals of National Security of Ukraine" dated June 19, 2003[1] and the Law of Ukraine "On Democratic Civilian Control over the Military Organization and Law Enforcement Bodies of the State" dated June 19, 2003,[2] in the Law of Ukraine "On National Security of Ukraine" is replaced by the term "security and defense sector". At the same time, the Law of Ukraine "On National Security of Ukraine" does not establish the definition of some terms used in it, and some terms are used in different variations. This causes a number of complications related to both understanding these terms and finding

[1] On the Fundamentals of National Security of Ukraine: Law of Ukraine dated June 19, 2003, no. 964-IV. Bulletin of the Verkhovna Rada of Ukraine 2003, no. 39, art. 351.

[2] On democratic civilian control over the military organization and law enforcement agencies of the state: Law of Ukraine dated June 19, 2003, no. 975-IV. Bulletin of the Verkhovna Rada of Ukraine 2003, no. 46, art. 366.

an answer to their correlation. The Law, in particular, uses the concepts of national values of Ukraine and democratic values of society. Since the Law does not define these concepts, they appear as self-evident. If the concept of "democratic values of society" is broad and its content does not give rise to significant discussions, then the concept of "national values of Ukraine" is fundamentally more specific and requires a normative definition. The concept of "social and state (national) values of Ukraine" is used in various semantic contexts in the Law of Ukraine "On the Basic Principles of State Policy in the Sphere of Establishing Ukrainian National and Civic Identity" dated December 13, 2022.[3] However, the current Ukrainian legislation does not contain a definition of the concept of "national values of Ukraine". This circumstance raises the question of how the concept of "national values of Ukraine" correlates with another concept enshrined in the Law – "national interests of Ukraine".[4] The concept of "national interests of Ukraine" itself is used in the Law in two variations: as "national interests of Ukraine" and as "fundamental national interests of Ukraine". If, according to Part 1 of Article 1 of the Law, "national interests of Ukraine" are "vital interests of a person, society and the state",[5] then what is the difference between them and "fundamental national interests of Ukraine"?

The Law defines the concepts of "security forces" and "defense forces", thus delimiting the relevant systems of bodies. However, the criteria for delimiting the security forces and defense forces in the Law are not clearly defined.[6] As a result, law enforcement and intelligence agencies, according to the Law, belong to both the security forces and the defense forces.

The problem of the balance between leadership and coordination functions in the field of national security and defense

The Law of Ukraine "On National Security of Ukraine" contains Article 13 entitled "Leadership in the Spheres of National Security and Defense", which enshrines the system of powers of the President of Ukraine in the sphere of national security and defense. Thus, Article 13 associates the leadership function in the sphere of national security and defense only with the person of the President of Ukraine. Here, both ignoring the role of other leading entities in the sphere of national

[3] On the Basic Principles of State Policy in the Sphere of Promoting Ukrainian National and Civic Identity: Law of Ukraine dated December 13, 2022, no. 2834-IX. Bulletin of the Verkhovna Rada of Ukraine 2023, no. 46, art. 116.

[4] *Analysis of the Law of Ukraine "On National Security of Ukraine",* https://www.helsinki.org.ua/articles/analiz-zakonu-ukrajiny-pro-natsionalnu-bezpeku-ukrajiny/[date of access: 01.02.2025].

[5] On national security of Ukraine: Law of Ukraine dated June 21, 2018, no. 2469-VIII. Bulletin of the Verkhovna Rada of Ukraine 2018, no. 31, art. 241.

[6] M. Sungurovskyi, *Critical comments on the draft law "On National Security"*, https://razumkov.org.ua/statti/khtos-mozhe-kazaty-iaku-systemu-bezpeky-buduiemo [date of access: 01.02.2025].

security and defense and an attempt to reduce the role of the President of Ukraine in the sphere of national security and defense to the leadership function are obvious. It is obvious that the President of Ukraine performs not only the function of supreme leadership, but also the function of coordination in the sphere of national security and defense. The functions and powers of the National Security and Defense Council of Ukraine, which, in accordance with Article 107 of the Constitution of Ukraine, "is a coordinating body on national security and defense issues under the President of Ukraine,"[7] are derived from the functions and powers of the President of Ukraine in the field of national security and defense and are means of ensuring these functions and powers. The coordination activities of the President of Ukraine in the field of national security and defense are aimed primarily at the system of executive bodies. The President of Ukraine influences the process of ensuring the national security and defense capability of Ukraine through the governing body in this system – the Cabinet of Ministers of Ukraine. The President of Ukraine exercises such influence on government activities in the field of national and defense not directly, but through the National Security and Defense Council of Ukraine. In essence, the National Security and Defense Council of Ukraine plays the role of a mediator in the mechanism of interaction between the President of Ukraine and the system of executive bodies in the field of national security and defense. Carrying out current control over the activities of executive bodies in the field of national security and defense, the National Security and Defense Council of Ukraine "shall submit relevant conclusions and proposals to the President of Ukraine" (Clause 2 of Part 1 of Article 4 of the Law of Ukraine "On the National Security and Defense Council of Ukraine" dated March 5, 1998).[8]

In the Law of Ukraine "On National Security of Ukraine", the coordinating role of the National Security and Defense Council of Ukraine in the field of national security and defense is reflected in Article 14 under the title "Coordination in the Fields of National Security and Defense". However, no other subjects are mentioned in Article 14 about coordinating activities in the field of national security and defense. In general, according to the approach applied in the Law of Ukraine "On National Security of Ukraine", leadership and coordination in the field of national security and defense appear as two functions, which are separately performed by two separate subjects – the President of Ukraine and, accordingly, the National Security and Defense Council of Ukraine.

[7] Constitution of Ukraine: Law of Ukraine of June 28, 1996, no. 254/96-vr. Bulletin of the Verkhovna Rada of Ukraine 1996, no. 30, art. 141.

[8] On the National Security and Defense Council of Ukraine: Law of Ukraine dated March 5, 1998, no. 183/98-VR. Bulletin of the Verkhovna Rada of Ukraine 1998, no. 35, art. 237.

The functions of leadership and coordination in the field of national security and defense are actually performed by a number of subjects of power, in addition to the President of Ukraine and the National Security and Defense Council of Ukraine. Part 1 of Article 15 of the Law of Ukraine "On National Security of Ukraine" states that "the powers of the Ministry of Defense of Ukraine include ... coordinating the activities of state bodies and local self-government bodies in preparing the state for defense in accordance with the established procedure."[9] According to Part 8 of Article 15 of the Law, "[t]he Minister of Defense of Ukraine shall exercise leadership over the Ministry of Defense of Ukraine, military-political and administrative leadership over the Armed Forces of Ukraine."[10] According to Part 3 of Article 18 of the Law, the Cabinet of Ministers of Ukraine, through the Minister of Internal Affairs of Ukraine, directs and coordinates the activities of the National Police of Ukraine, the National Guard of Ukraine, the State Border Service of Ukraine, the State Emergency Service of Ukraine and the State Migration Service of Ukraine. The leadership role of the Minister of Defense of Ukraine in relation to the Armed Forces of Ukraine is discussed in Part 1 of Article 8 of the Law of Ukraine "On the Armed Forces of Ukraine" dated March 25, 1992.[11] The leading role of the Minister of Internal Affairs of Ukraine in relation to the National Guard of Ukraine is discussed in Part 1 of Article 6 of the Law of Ukraine "On the National Guard of Ukraine" dated March 13, 1992.[12] The Cabinet of Ministers of Ukraine and the Minister of Internal Affairs of Ukraine as entities that direct and coordinate the activities of the police are discussed in Part 2 of Article 1 of the Law of Ukraine "On the National Police" dated July 2, 2015,[13] etc.

Taking into account the fact that the functions of leadership and coordination in the sphere of national security and defense are closely interconnected, it is advisable to allocate a special section in the Law of Ukraine "On National Security of Ukraine" under the title "Leadership and Coordination in the Sphere of National Security and Defense",[14] enshrining comprehensively and systematically in it the mechanism of leadership and coordination in the sphere of national

[9] On national security of Ukraine: Law of Ukraine dated June 21, 2018, no. 2469-VIII. Bulletin of the Verkhovna Rada of Ukraine 2018, no. 31, art. 241.

[10] Ibid.

[11] On the Armed Forces of Ukraine: Law of Ukraine dated March 25, 1992, no. 1934-XII. Bulletin of the Verkhovna Rada of Ukraine 1992, no. 9, art. 108.

[12] On the National Guard of Ukraine: Law of Ukraine dated March 13, 1992, no. 876-VII. Bulletin of the Verkhovna Rada of Ukraine 2014, no. 17, art. 594.

[13] On the National Police: Law of Ukraine dated July 2, 2015, no. 580-VIII. Bulletin of the Verkhovna Rada of Ukraine 2015, no. 40-41, art. 379.

[14] O. Nesterenko, *The system of subjects of ensuring national security and defense of Ukraine*, "Law and Security" 2020, no. 2 (77), p. 34.

security and defense. Such a mechanism should coordinate the competence in the sphere of national security and defense of the relevant entities, ensuring their effective interaction.

Participation of the Ukrainian people in ensuring national security

Part 1 of Article 17 of the Constitution of Ukraine enshrines the provision that "the protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian people."[15] Thus, Part 1 of Article 17 emphasizes the role of the Ukrainian people in protecting the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security. The declarative nature of Part 1 of Article 17 of the Constitution of Ukraine is obvious, since the possibility of its real implementation directly depends on the legislative consolidation of the mechanism for its implementation. However, the Law of Ukraine "On National Security of Ukraine" does not establish such a mechanism.

Composition of the security and defense sector

In Part 16 of Article 1 of the Law of Ukraine "On National Security of Ukraine" the concept of the security and defense sector is defined. The peculiarity of this definition is that the concept itself establishes the composition of the security and defense sector. According to Part 16 of Article 1 of the Law, the security and defense sector is "a system of state authorities, the Armed Forces of Ukraine, other military formations established in accordance with the laws of Ukraine, law enforcement and intelligence agencies, special-purpose state authorities with law enforcement functions, civil defense forces, the defense-industrial complex of Ukraine, the activities of which are under democratic civilian control and, in accordance with the Constitution and laws of Ukraine, are functionally aimed at protecting the national interests of Ukraine from threats, as well as citizens and public associations who voluntarily participate in ensuring the national security of Ukraine."[16] At the same time, the Law of Ukraine "On National Security of Ukraine" contains a separate Article 12 entitled "Composition of the Security and Defense Sector". Part 1 of Article 12 establishes that "the security and defense sector of Ukraine consists of four interrelated components: security forces; defense forces; defense-industrial complex; citizens and public associations who voluntarily participate in ensuring

[15] Constitution of Ukraine: Law of Ukraine of June 28, 1996, no. 254/96-vr. Bulletin of the Verkhovna Rada of Ukraine 1996, no. 30, art. 141.

[16] On national security of Ukraine: Law of Ukraine dated June 21, 2018, no. 2469-VIII. Bulletin of the Verkhovna Rada of Ukraine 2018, no. 31, art. 241.

national security."[17] Specifying the composition of the security and defense sector, Part 2 of Article 12 establishes that "the security and defense sector includes: the Ministry of Defense of Ukraine, the Armed Forces of Ukraine, the State Special Service of Transport, the Ministry of Internal Affairs of Ukraine, the National Guard of Ukraine, the National Police of Ukraine, the State Border Service of Ukraine, the State Migration Service of Ukraine, the State Emergency Service of Ukraine, the Security Service of Ukraine, the Anti-Terrorist Center under the Security Service of Ukraine, the Court Security Service, the State Security Department of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Apparatus of the National Security and Defense Council of Ukraine, the intelligence agencies of Ukraine, the central executive body that ensures the formation and implementation of the state military-industrial policy."[18] Thus, Part 2 of Article 12 narrows the composition of the security and defense sector compared to Clause 16 of Part 1 of Article 1 and Part 1 of Article 12 of the Law. In fact, Part 2 of Article 12 of the Law includes only certain state authorities (state bodies) or their structural divisions in the list of subjects of the security and defense sector. This list does not include either subjects of the defense-industrial complex, or citizens and public associations that voluntarily participate in ensuring national security and defense capability of the state.

Among the subjects of the security and defense sector listed in Part 2 of Article 12 of the Law of Ukraine "On National Security of Ukraine", the President of Ukraine is not mentioned, in particular. The President of Ukraine as a leading subject of the security and defense sector is mentioned in Article 13 of the Law "Leadership in the Spheres of National Security and Defense". Therefore, it is impossible to understand why the President of Ukraine as a subject of the security and defense sector is not mentioned in Part 2 of Article 12 of the Law. The list of subjects of the security and defense sector given in Part 2 of Article 12 of the Law also does not mention the Cabinet of Ministers of Ukraine, the National Security and Defense Council of Ukraine, etc.

Part 2 of Article 12 of the Law of Ukraine "On National Security of Ukraine" does not mention such subjects of the security and defense sector as citizens of Ukraine and their associations who voluntarily participate in ensuring the national security and defense capability of Ukraine. According to the Law, foreign citizens who serve in the Armed Forces of Ukraine or carry out volunteer activities for the benefit of the Armed Forces of Ukraine are also not subjects of the security and defense sector.

[17] Ibid.
[18] Ibid.

Public associations and citizens who voluntarily participate in ensuring the national security and defense capability of the state as separate subjects of the security and defense sector are directly mentioned in Clause 16 of Part 1 of Article 1 of the Law, which defines the concept of the security and defense sector, and in Part 1 of Article 12 of Section IV of the Law "Security and Defense Sector", which defines the composition of the security and defense sector. The consolidation in the Law of Ukraine "On National Security of Ukraine" of the status of citizens and public associations that voluntarily participate in ensuring the national security and defense capability of Ukraine as subjects of the security and defense sector is necessary at least in view of the provisions of Part 1 of Article 17 of the Constitution of Ukraine that "the protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian people."[19] Citizens and public associations that voluntarily participate in ensuring the national security and defense capability of the state are important participants in the process of ensuring the national security and defense capability of Ukraine. This is clearly demonstrated by the circumstances of the modern Russian-Ukrainian war at its initial stage, when Ukrainian civil society actively opposed the Russian occupation by creating its own armed formations (volunteer battalions) and providing them with comprehensive assistance. At the same time, the activities of both the units themselves, created on the popular initiative, and the public organizations that facilitated them, were outside the scope of legal regulation.[20] Despite this, the role of civil society institutions in ensuring national security and defense capability of Ukraine is not properly reflected in the Law of Ukraine "On National Security of Ukraine". It is noteworthy that in the Concept for the Development of the Security and Defense Sector of Ukraine, approved by the decision of the National Security and Defense Council of Ukraine dated March 4, 2016, public organizations were recognized as active participants in the process of developing the security and defense sector (Chapter IV "The Role and Place of Society in the Development of the Security and Defense Sector".)[21]

[19] Constitution of Ukraine: Law of Ukraine of June 28, 1996, no. 254/96-vr. Bulletin of the Verkhovna Rada of Ukraine 1996, no. 30, art. 141.

[20] I. Doronin, *Legal problems of the participation of the Ukrainian people in ensuring national security*, [in:] *Education and science in the sphere of national security: problems and priorities of development: materials of the VI International Scientific and Practical Conference (Ostroh, May 17, 2024),* eds. M. S. Romanov, R. S. Martyniuk, E. M. Balashov, Ostroh ouse of the National University "Ostroh Academy", 2024, p. 16.

[21] On the decision of the National Security and Defense Council of Ukraine dated March 4, 2016, On the Concept of Development of the Security and Defense Sector of Ukraine: Decree of the President of Ukraine dated March 14, 2016, no. 92/2016, "Official Gazette of Ukraine" 2016, no. 23, art. 898.

The list of subjects of the security and defense sector specified by the Law of Ukraine "On National Security of Ukraine" does not mention local self-government bodies. Local self-government bodies play a significant role in ensuring national security, especially under the conditions of martial law or a state of emergency. The activities of local self-government bodies as subjects of the security and defense sector are regulated, in particular, in the Law of Ukraine "On Local Self-Government in Ukraine" dated May 21, 1997. Article 38 of this act enshrines detailed provisions on the powers of local self-government bodies to ensure security in the territory of the relevant territorial community.[22] It is also noteworthy that local self-government bodies were defined as "subjects of ensuring national security" in Article 4 of the Law of Ukraine "On the Fundamentals of National Security of Ukraine".[23]

Part 2 of Article 12 of the Law of Ukraine "On National Security of Ukraine" contains the following provision: "Other state bodies and local self-government bodies shall carry out their functions to ensure national security in cooperation with bodies that are part of the security and defense sector."[24] Thus, in accordance with the cited provision, local self-government bodies shall carry out certain functions to ensure national security. However, despite this, the Law of Ukraine "On National Security of Ukraine" does not mention them in the list of subjects of the security and defense sector.

It is obvious that the list of subjects of the security and defense sector, even reflected in general in the Law of Ukraine "On National Security of Ukraine", is not exhaustive. In reality, the circle of subjects that ensure the national security and defense capability of Ukraine, in addition to the Ukrainian people, also includes the Verkhovna Rada of Ukraine, the Constitutional Court of Ukraine, the State Bureau of Investigation, the Antimonopoly Committee of Ukraine, the National Anticorruption Agency, the Independent Anticorruption Commission, the National Agency of Ukraine for the Identification, Search and Management of Assets Obtained from Corruption and Other Crimes, people's deputies of Ukraine, and civil society institutions.

It is seen that all subjects that ensure the national security and defense capability of Ukraine can be divided into several groups. The first group is formed by state authorities, which, given their competence and staffing, directly ensure the national security and defense capability of Ukraine. These are such bodies as the

[22] On local self-government in Ukraine: Law of Ukraine dated May 21, 1997, no. 280/97-VR. Bulletin of the Verkhovna Rada of Ukraine 1997, no. 24, art. 170.

[23] On the Fundamentals of National Security of Ukraine: Law of Ukraine dated June 19, 2003, no. 964-IV. Bulletin of the Verkhovna Rada of Ukraine 2003, no. 39, art. 351.

[24] On national security of Ukraine: Law of Ukraine dated June 21, 2018, no. 2469-VIII. Bulletin of the Verkhovna Rada of Ukraine 2018, no. 31, art. 241.

Armed Forces of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, the National Guard of Ukraine, etc. The second group is formed by state authorities that ensure the national security and defense capability of Ukraine indirectly, in the process of exercising their "titular" functions and powers. These are such state authorities as the Verkhovna Rada of Ukraine, the Constitutional Court of Ukraine, etc. The third group is formed by state authorities that perform leadership and coordination functions in the field of national security and defense. These are such state authorities as the President of Ukraine, the Cabinet of Ministers of Ukraine, the National Security and Defense Council of Ukraine, etc. The fourth group is formed by entities that ensure the national security and defense capability of Ukraine in interaction with entities of the first group. With this approach, the entities of the fourth group are formed by the Ukrainian people in general and civil society institutions.

Attempts to fill the gaps in constitutional regulation

The Law of Ukraine "On National Security of Ukraine" contains Article 13 under the title "Leadership in the Spheres of National Security and Defense", which relatively comprehensively regulates the competence of the President of Ukraine in the sphere of national security and defense. From the point of view of legal technique, namely the level of its detail, Article 13 differs markedly from many other significantly generalized norms of the Law. According to Article 13 of the Law of Ukraine "On National Security of Ukraine", the role and place of the President of Ukraine in the sphere of national security and defense are that he exercises supreme leadership in this sphere over the system of bodies that ensure the national security and defense capability of Ukraine. According to Article 13, the leadership of the President of Ukraine in the sphere of national security and defense has the meaning of a basic authority, the implementation of which is subordinate to the entire system of powers of the President of Ukraine in the sphere of national security and defense, defined by the Law. The composition of Article 13 testifies that the powers of the President of Ukraine listed therein are derived from his leadership role in the sphere of national security and defense and are exercised by the Head of State in the process of leadership in the mentioned sphere.[25] Such a legal position, unfortunately, is not reflected in the Constitution of Ukraine, where there is no separate and integral regulation of the powers of the President of Ukraine in the sphere of national security and defense. A number

[25] O. Kotliarenko, *Characteristics of the content and scope of the powers of the President of Ukraine as the Supreme Commander-in-Chief of the Armed Forces of Ukraine*, "Analytical and Comparative Law" 2022, no. 2, pp. 52-58.

of the powers of the President of Ukraine in the sphere of national security and defense are defined indirectly in the Constitution, through the constitutional fixation of his other powers. This obvious flaw in the constitutional regulation of the status of the President of Ukraine as a guarantor of state sovereignty and territorial integrity of Ukraine provokes a discretionary form of implementation of his constitutional functions in the sphere of national security and defense. Another consequence of the absence of a separate and integral regulation of the powers of the President of Ukraine in the sphere of national security and defense in the Constitution of Ukraine is their "dispersion" among many laws.[26] Article 13 of the Law of Ukraine "On National Security of Ukraine" is designed to compensate for the shortcomings of the constitutional consolidation of the competence of the President of Ukraine in the field of national security and defense. However, it is noteworthy that the conditionality of part of the powers of the President of Ukraine, enshrined in Article 13 of the Law, by his constitutional powers in the field of national security and defense is not obvious.[27] It should be expected that the issue of the constitutionality of the provisions of Article 13 of the Law of Ukraine "On National Security of Ukraine" will be resolved by the body of constitutional jurisdiction in the process of their application.

Conclusions

Taking into account the role of the Law of Ukraine "On National Security of Ukraine" as a fundamental act in the system of legislation regulating legal relations in the field of national security and defense, it is necessary to define all the basic concepts used in this act. The law should avoid terminological inconsistency or ambiguity.

The Law of Ukraine "On National Security of Ukraine" must clearly adhere to the priorities of legal regulation in the field of national security and defense, outlined in the Constitution of Ukraine. Although the Ukrainian people and civil society institutions are mentioned in separate provisions of the Law that determine the composition of the security and defense sector, they are not endowed with any specific powers of the subjects of the security and defense sector. Without establishing any mechanisms for the participation of the Ukrainian people and civil society institutions in ensuring national security and defense capability of the state, the Law of Ukraine "On National Security of Ukraine" essentially ignored their importance as subjects of the security and defense sector. Thus, given the

[26] V. Topolynskyi, A. Ostapenko, *Historical and legal analysis of the legislative consolidation of the powers of the Supreme Commander-in-Chief of the Armed Forces of Ukraine*, "Law and Society" 2022, no. 4, p. 56.

[27] Analysis of the Law of Ukraine "On National Security of Ukraine", https://www.helsinki.org.ua/articles/analiz-zakonu-ukrajiny-pro-natsionalnu-bezpeku-ukrajiny/ [date of access: 01.02.2025].

provisions of Part 1 of Article 17 of the Constitution of Ukraine that ensuring the national security of Ukraine is "a matter of the entire Ukrainian people," the Law of Ukraine "On National Security of Ukraine" should have defined the main mechanisms for the participation of the Ukrainian people in ensuring national security and defense capability of the state.

Part 2 of Article 12 of the Law of Ukraine "On National Security of Ukraine" limits the range of subjects of the security and defense sector only to subjects of government authority. In addition, the list of these subjects is incomplete. It is necessary to define clearly, consistently and exhaustively the range of subjects of the security and defense sector in the Law of Ukraine "On National Security of Ukraine". The powers of state authorities, whose role in ensuring national security and defense capability of the Ukrainian state is decisive, must be directly enshrined in the Law. It is seen that among all subjects of government authority that directly or indirectly ensure national security and defense capability of Ukraine within the limits of their competence, it is necessary to define in the Law of Ukraine "On National Security of Ukraine", given its goals and nature, the role of such higher state bodies as the President of Ukraine, the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine, the Constitutional Court of Ukraine, the Supreme Court of Ukraine in the sphere of national security and defense. It is necessary to regulate in detail and holistically the powers of its leading subjects in the field of national security and defense – the President of Ukraine and the Cabinet of Ministers of Ukraine. The role of other security and defense sector entities in ensuring the national security and defense capability of Ukraine can be defined more generally in the Law of Ukraine "On National Security of Ukraine".

References

1. *Analysis of the Law of Ukraine "On National Security of Ukraine"*, https://www.helsinki.org.ua/articles/analiz-zakonu-ukrajiny-pro-natsionalnu-bezpeku-ukrajiny/.
2. Constitution of Ukraine: Law of Ukraine of June 28, 1996, no. 254/96-vr. Bulletin of the Verkhovna Rada of Ukraine 1996, no. 30, art. 141.
3. Doronin I., *Legal problems of the participation of the Ukrainian people in ensuring national security*, [in:] *Education and science in the sphere of national security: problems and priorities of development: materials of the VI International Scientific and Practical Conference (Ostroh, May 17, 2024),* eds.. M. S. Romanov, R. S. Martyniuk, E. M. Balashov, Ostroh ouse of the National University "Ostroh Academy", 2024,.
4. Kotliarenko O., *Characteristics of the content and scope of the powers of the President of Ukraine as the Supreme Commander-in-Chief of the Armed Forces of Ukraine*, "Analytical and Comparative Law" 2022, no. 2,.
5. Nesterenko O., *The system of subjects of ensuring national security and defense of Ukraine*, "Law and Security" 2020, no. 2 (77),.

6. On democratic civilian control over the military organization and law enforcement agencies of the state: Law of Ukraine dated June 19, 2003, no. 975-IV. Bulletin of the Verkhovna Rada of Ukraine 2003, no. 46, art. 366.
7. On local self-government in Ukraine: Law of Ukraine dated May 21, 1997, no. 280/97-VR. Bulletin of the Verkhovna Rada of Ukraine 1997, no. 24, art. 170.
8. On national security of Ukraine: Law of Ukraine dated June 21, 2018, no. 2469-VIII. Bulletin of the Verkhovna Rada of Ukraine 2018, no. 31, art. 241.
9. On the Armed Forces of Ukraine: Law of Ukraine dated March 25, 1992, no. 1934-XII. Bulletin of the Verkhovna Rada of Ukraine 1992, no. 9, art. 108.
10. On the Basic Principles of State Policy in the Sphere of Promoting Ukrainian National and Civic Identity: Law of Ukraine dated December 13, 2022, no. 2834-IX. Bulletin of the Verkhovna Rada of Ukraine 2023, no. 46, art. 116.
11. On the decision of the National Security and Defense Council of Ukraine dated March 4, 2016, "On the Concept of Development of the Security and Defense Sector of Ukraine": Decree of the President of Ukraine dated March 14, 2016, no. 92/2016, "Official Gazette of Ukraine" 2016, no. 23, art. 898.
12. On the Fundamentals of National Security of Ukraine: Law of Ukraine dated June 19, 2003, no. 964-IV. Bulletin of the Verkhovna Rada of Ukraine 2003, no. 39, art. 351.
13. On the National Guard of Ukraine: Law of Ukraine dated March 13, 1992, no. 876-VII. Bulletin of the Verkhovna Rada of Ukraine 2014, no. 17, art. 594.
14. On the National Police: Law of Ukraine dated July 2, 2015, no. 580-VIII. Bulletin of the Verkhovna Rada of Ukraine 2015, no. 40-41, art. 379.
15. On the National Security and Defense Council of Ukraine: Law of Ukraine dated March 5, 1998, no. 183/98-VR, Bulletin of the Verkhovna Rada of Ukraine 1998, no. 35, art. 237.
16. Sungurovskyi M., *Critical comments on the draft law "On National Security",* https://razumkov.org.ua/statti/khtos-mozhe-kazaty-iaku-systemu-bezpeky-buduiemo.
17. Topolynskyi V., Ostapenko A., *Historical and legal analysis of the legislative consolidation of the powers of the Supreme Commander-in-Chief of the Armed Forces of Ukraine*, "Law and Society" 2022, no. 4, pp. 54-61.

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 255–272

ISSN 2543-6961
e-ISSN 2720-3093

Maria Hapunik
ORCID: 0000-0002-4522-0563
University of Białystok

Police Cooperation as a Response to European Union Security Threats

Współpraca policyjna jako odpowiedź na zagrożenia bezpieczeństwa Unii Europejskiej

Abstract
This paper examines the rapidly evolving police cooperation within the European Union, which represents a crucial and essential response to emerging internal security threats. This article focuses on developments since 2022, examining enhanced legal and operational frameworks, including Europol's expanded mandate, the role of the European Multidisciplinary Platform Against Criminal Threats (EMPACT), and the integration of innovative technologies such as artificial intelligence (AI) and advanced biometric systems. The research demonstrates the indispensability of police cooperation in addressing organized crime, cybercrime, migration crisis management, and hybrid threats. Furthermore, the study identifies that the effectiveness of police cooperation is directly contingent upon the interoperability of information systems, mutual trust among EU member states, and response capabilities to contemporary challenges, while maintaining robust standards for fundamental rights protection and citizen privacy.

Keywords: police cooperation, EU security, cross-border crime, cybercrime, artificial intelligence, biometric data

Abstrakt
Niniejszy artykuł analizuje dynamicznie rozwijającą się współpracę policyjną w ramach Unii Europejskiej, która stanowi kluczową i niezbędną odpowiedź na pojawiające się zagrożenia dla bezpieczeństwa wewnętrznego. Tekst koncentruje się na zmianach zachodzących od 2022 r., obejmujących wzmocnione ramy prawne i operacyjne, w tym rozszerzony mandat Europolu, rolę Europejskiej Wielodyscyplinarnej Platformy Przeciwko Zagrożeniom Przestępczym (EMPACT) oraz integrację innowacyjnych technologii, takich jak sztuczna inteligencja (AI) i zaawansowane systemy biometryczne. Przeprowadzone badania wskazują na nieodzowność współpracy policyjnej w przeciwdziałaniu przestępczości zorganizowanej, cyberprzestępczości, w zarządzaniu kryzysami migracyjnymi oraz w reagowaniu na zagrożenia hybrydowe. Ponadto w artykule stwierdzono, że skuteczność współpracy policyjnej jest bezpośrednio uzależniona od interoperacyjności systemów informacyjnych, wzajemnego zaufania między państwami członkowskimi UE oraz zdolności reagowania na współczesne wyzwania, przy jednoczesnym utrzymaniu wysokich standardów ochrony praw podstawowych i prywatności obywateli.

Słowa kluczowe: współpraca policyjna, bezpieczeństwo UE, przestępczość transgraniczna, cyberprzestępczość, sztuczna inteligencja, dane biometryczne

Introduction

The fundamental duty of every state, and in the context of the European Union (EU), the common objective of member states, is to ensure internal security. The threat landscape is undergoing dynamic changes associated with the evolving cross-border nature of organized crime, cybercrime, and increasingly complex hybrid threats, against which traditional EU response mechanisms are becoming insufficient. Police cooperation in the EU, consisting of coordinated actions by the member states' law enforcement agencies which constitutes a fundamental response to these challenges, has been evolving in recent years toward increasingly integrated and innovative solutions.

The analyzed period from 2022 is characterized by a series of events that have significantly influenced the priorities and dynamics of police cooperation. Russia's aggression against Ukraine, ongoing since February 24, 2022, has not only sparked discussions about geopolitical security but has also revealed the need for effective countermeasures against conflict-related crimes such as arms trafficking, money laundering, human trafficking, and cyberattacks. Furthermore, the conflict between Iran and Israel, which began on June 13, 2025, has impacted attempts to destabilize functioning of the European Union and weakened the sense of security in member states. In this context, there are concerns about the intensification of organized crime, particularly in the area of arms trafficking, as well as increased radicalization among young people.

The ongoing migration crisis at the EU borders, unfolding in the background of these events, remains one of the most important reasons for strengthening coordinated actions in the field of border management and combating human trafficking. The phenomenal development of artificial intelligence and advanced digital technologies, utilized by both criminal perpetrators and law enforcement agencies, creates new challenges in personal data protection and in the area of inalienable fundamental human rights.

In the research process, the source base primally consists of normative acts, and the method of institutional – law analysis has been used. Sources of EU law and Polish generally applicable law have been examined. Reports of EU agencies have been also analysed. Within research process, mainly normative acts currently applicable, adopted after 2022 have been analysed. Ongoing research was conducted with consideration of the research objective. The research objective has both cognitive and practical value. The aim of the research was to identify and present, in a systematic and comprehensive manner, the necessity of cooperation between police forces and EU Member States in the use of new technologies.

1. Origins of Police Cooperation in the European Union

Police cooperation in the European Union has evolved from initial, loose forms of interstate cooperation, which were primarily based on bilateral agreements, to today's highly institutionalized system. The beginnings of cooperation were primarily associated with the Schengen Agreement,[1] followed by the establishment of Europol[2] in 1995; these two actions formed the foundations of a common security space. Treaty on the Functioning of the European Union signed in Lisbon (TFEU),[3] which entered into force in 2009, introduced the Area of Freedom, Security and Justice (AFSJ) as one of the main areas of policies of member states, significantly strengthening the legal basis and competencies of the Union in the scope of police cooperation, making it transnational in nature. Nowadays, the processes of integration and strengthening of police cooperation tools are characterized by greater intensity, which is a direct response to the rapidly changing security environment.

Data derived from analysis concerning the most serious threats, based on information exchange, or cross-checks, are collected in Europol's EU-SOCTA report (EU Serious and Organised Crime Threat Assessment). This report serves to inform and activate European law enforcement agencies to combat serious and organized crime across all the EU. The EU SOCTA 2025 report highlighted the necessity for deeper police cooperation and the need for continued commitment to protecting EU societies. Since the previous report in 2021, "Europol's support for member states' law enforcement has evolved toward a more targeted and effective operational approach, consolidating a more integrated model of EU police cooperation."[4] Europol participates in complex criminal investigations at the European level, conducting activities through operational task forces. Looking ahead, Europol's primary objective "is to provide an even more extensive response to internal security threats, strengthen Europol's role as a centre of knowledge and excellence, reinforce dedicated operational teams in the crime areas of greatest concern to EU member states, and further develop innovative potential for the purposes of law enforcement."[5]

[1] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. Schengen.1990.06.19 (OJ EU.L.2000.239.19).

[2] Europol – The European Police Office, headquartered in The Hague. The Europol Convention was signed on 26 July 1995, and the office began operations on 1 July 1999. Europol is a law enforcement agency tasked with increasing security in Europe by providing assistance to law enforcement agencies in EU Member States.

[3] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 (Journal of Laws of 2009, No. 203, item 1569).

[4] Europol, *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, Luxembourg 2025, p. 7; https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf [date of access: [7.07.2025].

[5] Ibidem.

As part of Europol's EU SOCTA report, published on March 18, 2025, recommendations were developed for setting priorities in combating serious and organized crime at the level of EU policy. The report assesses all threats across areas of crime under Europol's mandate, including criminal entities, criminal infrastructure, and geographical scope, taking into account the driving factors and impact of organized crime. The 2025 report developed recommendations indicating priorities for EU government services, noting that "organized crime is becoming increasingly globalized, digital, and adaptive, requiring an unprecedented level of cooperation and information sharing from law enforcement at the European level."[6]

Consequently, presenting the key aspects and mechanisms of police cooperation in the European Union, with particular emphasis on evolution and introduced innovations, aims to demonstrate how the EU adapts its tools and strategies to effectively respond to security threats. The EU SOCTA methodology is based on qualitative and quantitative analysis methods, and specific indicators have been established to identify the most dangerous criminal phenomena in the EU. Intensive analyses are conducted to establish priorities in police service operations.

Furthermore, EU SOCTA 2025 identified key threats that should be treated as the EU priorities in combating organized crime over the next four years in the context of EMPACT – European Multidisciplinary Platform Against Criminal Threats. EMPACT is an EU instrument, adopted in 2010, aimed at fighting and preventing the most serious crimes facing the Union. This initiative optimizes EU services at national levels, encouraging the use of their own resources and joint strengthening of efforts.

On April 1, 2025, in Strasbourg, a new Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions regarding Protect EU was issued: European Internal Security Strategy,[7] based on the unwavering promise of maintaining the peace. The Document identified security as the foundation upon which European freedoms are built, along with "democracy, rule of law, fundamental rights, competitiveness, and prosperity."

The main premise of the new actions is close strategic and operational cooperation between the Commission, member states, and the EU agencies, which will be based on new methods of information sharing and regular comprehensive analysis and assessment of threats. Another action planned by the European

[6] EU Serious and Organised Crime Threat Assessment (EU-SOCTA), https://www.europol.europa.eu/publications-events/main-reports/socta-report [date of access:17.07.2025].

[7] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on ProtectEU: European Internal Security Strategy, COM/2025/148 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148 [date of access:19.07.2025].

Commission is the development of new tools for law enforcement agencies, aimed at strengthening resilience against hybrid threats, enhancing cybersecurity, limiting access to tools and assets used in criminal activities, and providing special protection for transportation hubs and ports.

There are also plans to tighten regulations aimed at combating organized crime and take measures to prevent the recruitment of European youth into criminal groups. The European Internal Security Strategy announces the introduction of a comprehensive counter-terrorism programme, preventing radicalization through securing cyberspace and public spaces, and eliminating financing channels. The response to threats will include development of operational cooperation through partnerships with key regions, such as Latin America and the Mediterranean region.

Furthermore, special attention should be paid to the planned transformation of Europol into an operational law enforcement agency in 2026, the strengthening of Eurojust, and the expansion of the role and tasks of Frontex.

2. Legal Foundations of Police Cooperation in the European Union

The objective of police cooperation and judicial cooperation in criminal matters is to guarantee the security of European Union citizens through the prevention and combat of crime, racism, and xenophobia. This matter is regulated by Title V of the Treaty on the Functioning of the European Union in Chapters I, IV, and V. The cooperation, which serves the EU's internal security, involves collaboration between national police forces, as well as between national administrative authorities, such as customs services and national judicial authorities.[8] This cooperation is implemented with the participation of the European Union Agency for Criminal Justice Cooperation (Eurojust), the European Union Agency for Law Enforcement Cooperation (Europol), and the European Judicial Network.

Police cooperation in the European Union is based on a complex legal system that is continuously developed and adapted to new needs. The foundation is established by the provisions of the Treaty on the Functioning of the European Union (TFEU), particularly Articles 87-89, which define the objectives and scope of police cooperation and Europol's role. However, it is derived law – regulations, directives, and decisions – that specifies concrete mechanisms and instruments of action.

Currently, the development of EU law in the area of internal security is extremely intensive, resulting in a series of key acts that have redefined the framework for law enforcement operations in Europe. After 2022, the EU legal acts were adopted that strengthen police cooperation.

[8] An official website of the UE, *Police and criminal justice cooperation*, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM: police_judicial_cooperation [date of access:20.07.2025].

First, it is necessary to mention Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794[9] regarding Europol's cooperation with private parties, the processing of personal data by Europol to support criminal investigations, and Europol's role in research and innovation. This act significantly expanded Europol's competencies, enabling it to, among other things, more efficiently process large datasets (Big Data) to support cross-border investigations, expand cooperation with private entities (e.g., online platforms in removing terrorist content or content related to sexual abuse of children), and strengthen Europol's role in research and development of innovative technologies, such as artificial intelligence, for law enforcement purposes. The new regulations also introduced a more robust framework for supervising data processing, responding to privacy concerns.

Directive (EU) 2023/977[10] of the European Parliament and of the Council of 10 May 2023 on information exchange between member states' law enforcement authorities is another key instrument aimed at streamlining and harmonizing operational information exchange processes. The Directive introduced the requirement of establishment of a single point of contact for each member state, an obligation of prompt response to requests for information (within strictly defined timeframes, such as 8 hours in urgent cases), and established standard format for data exchange. These changes were aimed at overcoming bureaucratic barriers and accelerating the flow of data crucial for effective crime prevention.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 is a breakthrough legal act that establishes harmonized rules on artificial intelligence and amends Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), and has become known as the AI Act. While full implementation of the AI Act provisions will begin in 2026, certain provisions (Chapters I and II) have been in effect since February 2025, including those concerning prohibited practices of high-risk AI systems.

The EU legislator, acting with awareness of implementing the most far-reaching regulatory measures regarding AI technology development and use, which is

[9] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794 as regards Europol's cooperation with private entities, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, https://eur-lex.europa.eu/eli/reg/2022/991/oj [date of access:18.07.2025].

[10] Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, http://data.europa.eu/eli/dir/2023/977/oj [date of access:18.07.2025].

prohibition, designed Article 5 of the act (concerning prohibitions) on artificial intelligence, striving to define the scope of prohibition as precisely as possible.[11] The Act is fundamental in determining how the EU law enforcement authorities will use AI technologies, above all, biometric recognition systems. The AI Act, introduces strict conditions for the use of AI in real-time remote biometric identification in public places, permits such use only under strictly defined circumstances, such as searching for victims of a crime, prevention of specifically identified and imminent terrorist threats, or searching for suspects or perpetrators of serious crimes. This highlights the constant and intense tension between the need for security and the protection of fundamental rights.

Furthermore, the European legislator has introduced several legal acts supporting police cooperation and regulating topics such as: migration, border management, and security management through regulations concerning: Entry/Exit System (EES)[12]; European Travel Information and Authorization System (ETIAS)[13]; European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)[14]; Schengen Information System (SIS)[15]; Visa Information System (VIS)[16]; Eurodac.[17]

---

[11] J. Kozłowski, *Akt w sprawie sztucznej inteligencji w praktyce – charakterystyka unijnej regulacji opartej na ryzyku*, „Europejski Przegląd Sądowy" 2024, no. 12, pp.s 20-25.

[12] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

[13] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.

[14] Regulation (EU) 2019/816 setting up a centralised system for the identification of Member States holding conviction information on non-EU nationals and stateless persons (ECRIS-TCN) (UE) 2018/1726.

[15] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

[16] Regulation (EU) 2021/1134 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA in order to reform the Visa Information System (OJ L 248, 13.7.2021).

[17] Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac' for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council.

The regulations establishing interoperability frameworks entered into force on June 11, 2019,[18] enabling the creation of the European Search Portal, shared biometric matching service, Common Identity Repository, Multiple-Identity Detector, and Central Repository for Reporting and Statistics. Simultaneously, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) was established[19]. The agency is responsible for designing changes in the EU and Schengen border management and the registration process for third-country nationals crossing these borders.

The issue of biometric data has been particularly controversial and was also the subject of complaints before the Court of Justice of the European Union, resulting in a ruling C-205/21.[20] In this ruling, dated January 26, 2023, the CJEU determined that Police are authorized to process biometric and genetic data, within proper regulatory limitations. The use of new technologies is essential given the escalation of tensions in the Middle East and the war in Ukraine, which are directly linked to various threats, including the influx of illegal migrants through Belarus.

The processing of personal data, including sensitive data, by various EU Agencies and member state police forces has become a permanent element in combating threats, while the EU legislator maintains parallel efforts to uphold high standards of human rights, democracy, and rule of law within the Union. The aforementioned new legal frameworks, complementing existing regulations on information systems, create a comprehensive legal ecosystem designed to support police cooperation throughout the EU.

Cross-border police cooperation is largely based on the provisions of the Schengen Convention Implementing Agreement, which enabled the implementation

[18] Regulation (EU) 2019/817 on establishing a framework for interoperability between EU information systems in the area of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726, (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA and Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the area of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 . Report from the Commission to the European Parliament and the Council on the state of preparations for the full implementation of the interoperability regulations pursuant to Article 78(5) of Regulation (EU) 2019/817 and Article 74(5) of Regulation (EU) 2019/818, https://eur-lex.europa.eu/legal content/PL/ALL/?uri=COM%3A2025%3A162%3AFIN [date of access:(2./7./025])

[19] Report from the Commission to the European Parliament and the Council on the state of preparations for the full implementation of the interoperability regulations pursuant to Article 78(5) of Regulation (EU) 2019/817 and Article 74(5) of Regulation (EU) 2019/818, https://eur-lex.europa.eu/legal content/PL/ALL/?uri=COM%3A2025%3A162%3AFIN [date of access: (2./7./025])

[20] OPINION OF ADVOCATE GENERAL PITRUZZELLA delivered on 30 June 2022 (1) Case C-205/21 Criminal proceedings against V.S., third party: Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranataprestapnost, https://curia.europa.eu/juris/document/document.jsf;jsessionid=F7224E-4F7A500191A56E89B120053942?text=&docid=261934&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=16808143 [date of access: (2.07.2025]r

of its mechanisms and instruments. The EU legal acts concerning police cooperation are either linked to Schengen or derive from its legal acquis. Furthermore, through bilateral agreements and arrangements between Schengen area member states, selected issues concerning instruments, scope of cooperation, and the possibility of establishing permanent structure for police cooperation in border regions have been regulated.[21] Examples include the Agreement between the Government of the Republic of Poland and the Government of the Federal Republic of Germany on cooperation between police, border, and customs services, signed in Zgorzelec on May 15, 2014 (Journal of Laws of 2015, item 939), and the Agreement between the Republic of Poland and the Czech Republic on cooperation in border matters, signed in Prague on May 25, 1999 (Journal of Laws 2002 No. 195, item 1644).

Police cooperation in the European Union is also guided by the development of the EU substantive criminal law. In the current legal framework, provisions of Title V, Part III of the TFEU are particularly significant in this context, including Article 83(1), which establishes a closed catalogue of crime areas considered particularly serious and with a cross-border dimension, for which the Union has competence to harmonize national law through defining minimum definitions of prohibited acts and possible criminal sanctions.[22]

The closed catalogue of specified crimes was established in the Treaty of Lisbon; however, through a unanimous Council decision a provision was made for its expansion if future crime developments justify such action.[23] This provision opens the possibility for changes, particularly when considering and analysing new emerging forms of technological, social, and cultural threats.

3. Selected Forms of EU Police Cooperation

In June 2022, the Council of the European Union adopted a recommendation on operational police cooperation.[24] It established standards concerning operational cooperation for police officers operating in another EU member state or officers participating in joint operations. Rules regarding cross-border pursuits and cross-border surveillance were established.

[21] M. Róg, *Bilateral cooperation between the Polish and Lithuanian police (in the light of agreements and understandings)*, "Society and Politics" 2019, no. 3, pp. 303-316.

[22] A. Grzelak, *Expanding the list of offences in Article 83(1) TFEU – grounds, procedure and proposal to include hate crimes in the scope of harmonisation of European Union criminal law*, "Europejski Przegląd Sądowy" 2025, no. 6, pp. 4-10.

[23] Ibidem.

[24] Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation (Dz.U-.UE L z dnia 13.06.2022 r.), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32022H0915 [date of access: 15.07.2025].

The recommendation also included a list of crimes in relation to which cross-border pursuit and cross-border surveillance are permissible, frameworks for joint police operations, the establishment of a platform to support joint patrols and other joint operations, while ensuring secure communications and access to information, as well as joint police education with the goal of establishing a European police culture.

International police cooperation is conducted based on governmental and departmental legal acts, as well as documents enabling local cooperation in border areas.[25] Cooperation primarily consists of information exchange, which is the foundation of effective police collaboration. Currently, we can observe further modernization and development of key information systems, which constitute a vital lifeline of European security:

1. Schengen Information System[26] (SIS II): As the EU's largest information exchange system, SIS II underwent significant improvements following extensive modernization in 2022. New categories of alerts were introduced concerning persons wanted for entry or residence ban, vehicles, aircraft and boats, as well as objects related to terrorist offenses. The capabilities for entering and exchanging biometric data (fingerprints, facial images) were strengthened, which is crucial and essential for rapid person identification. According to the 2023 Ministry of Interior Affairs and Administration regulation,[27] Polish Police effectively uses SIS II to verify fingerprint data and images, which directly translates to crime detection and prevention capabilities.
2. European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN), that launched in 2023, is a system enabling judicial and police authorities to access information about convictions issued against third-country nationals and stateless persons throughout the Union. This represents an important enhancement in fighting cross-border crime, particularly in the context of border and migration management, as previously access to this type of data was partial.
3. European Travel Information and Authorization System (ETIAS), which will be fully operational in 2026, will introduce preliminary security

[25] *Współpraca międzynarodowa*, https://info.policja.pl/inf/wspolpraca-miedzynarod/72445,Wspolpraca-miedzynarodowa.html [date of access:(16.07.2025])

[26] The legal basis for the creation of the Schengen Information System (SIS) is three regulations of the European Parliament and of the Council: Regulation 2018/1862, 2018/1861 and 2018/1860.

[27] Regulation of the Minister of Internal Affairs and Administration of 3 March 2023 on the procedure for handing over to the Police persons or objects found as a result of access to SIS data, the procedure in cases of disclosure of misappropriated identity and the method and procedure of cooperation between authorities and the SIRENE office (Journal of Laws of 2023, item 427).

screening for visa-exempt third-country nationals, aiming to identify potential threats before their arrival at the border. The Entry/Exit System (EES), becoming fully operational in October 2025, will begin automating the entry and exit of third-country nationals crossing external Schengen borders, replacing traditional passport stamping and collecting biometric data (fingerprint data and facial biometric data). Both systems, managed by eu-LISA, significantly enhance the monitoring and identification capabilities in the border area, which is invaluable in counteracting illegal migration and crime. When fully operational, the capabilities of the systems will revolutionise the work of state authorities, including the Police.

4. Shared Biometric Matching Service (sBMS): In pursuit toward interoperability, sBMS enables simultaneous searching of biometric data across multiple databases (SIS, VIS, Eurodac, EES, ETIAS). The service enables fingerprint matching and first-time facial recognition. sBMS contains approximately 400 million biometric templates, aiming for precision during person identification and verification, enhancing border security and EU border controls. The launch of this new service coincides with the adaptation of the Visa Information System (VIS), which is now ready to interact with the Entry/Exit System (EES).[28] The system was launched on May 19, 2025. The shared biometric matching tool represents an important step needed to reduce the time required for identity verification and multiple identity detection, which is critical in combating current EU security threats.

The heart of police cooperation in the European Union is Europol – the European Union Agency for Law Enforcement Cooperation – which serves as a centre for multidimensional coordination. Europol's strengthened mandate from 2022, established by the aforementioned Regulation 2022/991, has enabled the Agency to operate even more effectively. Europol supports member states in analysing large datasets, which is crucial and irreplaceable in detecting complex criminal networks. Furthermore, Europol's creation of "threat maps" (SOCTA) and setting strategic priorities for the EU (EMPACT) serves as a starting point for coordinated and targeted police actions in the EU. The Agency is also the main AI development and implementation institution for law enforcement purposes, while ensuring its use complies with AI Act requirements and personal data protection principles.

[28] News article 19 May 2025 Directorate-General for Migration and Home Affairs, Commission announces launch of the shared biometric matching service, https://home-affairs.ec.europa.eu/news/commission-announces-launch-shared-biometric-matching-service-2025-05-19_en?prefLang=pl&etrans=pl [date of access: 23.07.2025].

Interpol,[29] the International Criminal Police Organization, assists law enforcement agencies in combating all forms of crime, bringing together 195 member states and is responsible for cooperation through a network of Police liaison officers operating in European Union countries, i.e., France, Spain, Lithuania, Germany, Croatia, Hungary, and Italy, as well as non-EU countries, i.e., Great Britain, Norway, Georgia, Turkey, Ukraine, the United States of America, and cooperation with foreign liaison officers accredited in Poland. It provides direct access to police databases concerning missing and wanted persons, fingerprint cards, DNA profiles, stolen vehicles and documents, etc.[30] Interpol continuously introduces innovations, keeping pace with contemporary policing challenges by utilizing new technologies, such as artificial intelligence, which can pose a security threat but can also serve as a police tool and source of evidence.[31] Interpol is an integral part of police cooperation worldwide and in Europe. It has been working towards international security for 100 years, evolving and introducing innovations to its security services.

In the Polish Police, the contact point and location where all international police information exchange channels converge – Single Point of Contact (SPOC) – is the International Police Cooperation Bureau of the National Police Headquarters. This unit coordinates and supervises all activities within international non-operational, operational, and training cooperation.

Another strategic and operational mechanism for coordinating EU internal security actions is EMPACT (European Multidisciplinary Platform Against Criminal Threats). This is an initiative led by the EU member states to identify, prioritize, and respond to threats posed by organized and serious international crime.[32] In the EMPACT policy cycle for the years 2025-2029, adopted by the EU Council in June 2025, seven priority threat areas were identified, including high-risk organized crime, cybercrime, human trafficking and migrant smuggling, drug trafficking, financial crime, as well as firearms and explosives-related crimes and environmental crimes.

EMPACT conducts Joint Action Days (JADs), which involve Europol, Frontex, Eurojust, and national law enforcement authorities. EMPACT provides a comprehensive approach, combining strategic analysis with specific operational activities to achieve measurable results in combating cross-border crime.

[29] CONSTITUTION OF THE INTERNATIONAL CRIMINAL POLICE ORGANIZATION-INTERPOL file:///C:/Users/752050/Downloads/01%20E%20Constitution_2024.pdf [date of access:23.07.2025].

[30] *Who we are*, https://www.interpol.int/ [date of access: 23.07.2025].

[31] *NTERPOL – Five actions for a safer world,* https://www.interpol.int/Who-we-are/What-is-INTERPOL2/INTERPOL-Five-actions-for-a-safer-world [date of access: 23.07.2025].

[32] *EMPACT fighting crime together*, An official website of the UE, https://home-affairs.ec.europa.eu/policies/internal-security/law-enforcement-cooperation/empact-fighting-crime-together_en [date of access: 23.07.2025].

In 2023, as a result of EMPACT, cooperation with non-EU partners was strengthened to combat criminal activity in the Western Balkans, Latin America, and in the context of Russia's aggressive war against Ukraine, but there were also many other achievements:

- 15,644 investigations initiated (over 7,500 victims identified and secured),
- 13,871 arrests made,
- €797 million confiscated (in assets and money),
- 197 tons of drugs seized,
- 821 high-risk criminal networks identified,
- 155 high-value targets revealed.

In 2024, under EMPACT:

- 6,635 investigations initiated,
- 13,575 criminals arrested,
- 5,024 victims identified and secured,
- €1.05 billion in assets and money seized,
- 1,941 firearms and 222 kg of explosives confiscated,
- 85 tons of drugs seized,
- 73 high-value targets were identified.[33]

Joint Investigation Teams (JITs) represent one of the most advanced forms of operational cooperation. The legal basis for establishing JITs within Member States' cooperation is founded on Article 13 of the 2000 Convention on Mutual Legal Assistance[34] and the 2002 Framework Decision concerning JITs.[35] These frameworks enable law enforcement authorities from different Member States to establish joint teams for conducting specific cross-border investigations, particularly in cases involving terrorism, organized crime, or cybercrime.

JITs, comprising of prosecution, law enforcement officials, and judges, are established for a specified duration, typically ranging from 12 to 24 months, deemed necessary for the successful completion of investigations.[36] Following the establishment of a JIT, police officers from various EU states, as team members, can directly exchange information and evidence, collaborate in real-time, and conduct joint operations. JITs facilitate the presence of police officers during investigative procedures in the territory of another state, resulting in the exchange of technical expertise and human resources.

[33] Ibidem.

[34] COUNCIL ACTof 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01).

[35] COUNCIL FRAMEWORK DECISION of 13 June 2002 on joint investigation teams (2002/465/JHA).

[36] European Union Agency for Criminal Justice Cooperation, Joint investigation teams, https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams [date of access: 23.07.2025].

Direct contact and communication enable JIT members to build personal relationships and trust, which translates into more brisk and efficient cooperation.[37] Eurojust (The European Union Agency for Criminal Justice Cooperation) plays a pivotal role in supporting and coordinating JITs by providing legal and financial assistance.[38] In collaboration with the Prosecutor's Office of the International Criminal Court, Eurojust actively supports handling cases of international scope by teams, representing a precedent-setting example of cooperation in the prosecution of international crimes.

Effective management of external borders is another crucial domain for EU internal security, with the European Border and Coast Guard Agency (Frontex) playing a central role. The most recent modification to Frontex's legal framework was implemented through the enactment of Regulation (EU) 2019/1896 of 13 November 2019 concerning the European Border and Coast Guard (OJ L 295, 14.11.2019). Hundreds of officers from the EU Member States participate in operations along and beyond the European Union's external borders, executing tasks related to border protection, combating cross-border crime, and facilitating return operations.[39]

During the period 2022-2025, Frontex significantly enhanced its operational capabilities by increasing the number of permanent corps officers, developing advanced surveillance technologies (including drones and satellites), and intensifying joint operations along the EU's external land and maritime borders. In the context of increased migratory pressure on the EU's eastern border and Mediterranean routes, Frontex's cooperation with national border services and police forces has become increasingly strategic.

According to preliminary data collected by Frontex in the first half of 2025, the number of illegal border crossing incidents at the European Union's borders decreased by 20% to 75,900, primarily due to significant drop in numbers along the Eastern Mediterranean and West African routes.[40]

4. Training and Capacity Building for Police Cooperation

Non-operational cooperation among Member States' police forces represents another significant aspect of the EU law enforcement collaboration. This primarily

[37] Ibidem.

[38] European Union Agency for Criminal Justice Cooperation, Joint investigation teams (Eurojust), https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/eurojust_pl [date of access: 23.07.2025].

[39] *Who we are*, https://www.frontex.europa.eu/about-frontex/who-we-are/tasks-mission/?etrans=pl [date of access: 22.07.2025].

[40] *EU external borders: Irregular crossings drop by 20% in first half of 2025*, 10.07.2025, https://www.frontex.europa.eu/media-centre/news/news-release/eu-external-borders-irregular-crossings-drop-by-20-in-first-half-of-2025-CUpZ5o [date of access: 23.07.2025].

encompasses training exchange and cooperation with other police institutions from the EU Member States, facilitated through EU agencies and bodies. The European Union Agency for Law Enforcement Training (CEPOL – Collège Européen de Police) extends its activities beyond the Union, particularly to Eastern Partnership countries (Azerbaijan, Armenia, Georgia, Belarus, Moldova, and Ukraine). CEPOL is responsible for developing the competencies of law enforcement officers within the EU.

During 2022-2025, CEPOL intensified its training programs, focusing on emerging threats and technologies. The training curriculum encompasses cybercrime (e.g., digital forensics, countering ransomware), hybrid threats (combating disinformation, critical infrastructure protection), counter-terrorism (including online radicalization), and the application of artificial intelligence in investigations. Investment in officer education is crucial to ensure that the Member States law enforcement agencies possess the necessary skills to combat evolving forms of crime. Consequently, the utilization of the EU funds by Member States' police forces for training and equipment acquisition represents a significant development.

Non-operational cooperation also encompasses the development of the EU legislation and familiarization with legislative solutions implemented in other Member States. Professional and personal contacts within this domain are equally important, as they foster interpersonal trust, eliminate prejudice, and dismantle harmful stereotypes.

Conclusion

Contemporary police cooperation would be impossible without the dynamic development and implementation of new technologies. Biometric data (facial images, fingerprints, and behavioural biometrics) has become fundamental for rapid and unambiguous identification. Systems such as sBMS and the development of AI-based analytical tools within Europol and eu-LISA enable automatic data comparison from various sources, identification of criminal behaviour patterns, and threat prediction. AI is also employed in analysing open-source information during Open Source Intelligence (OSINT) operations, in combating terrorist content and online child exploitation materials.

The EU AI Act will ensure technological development within clearly defined legal and ethical frameworks while protecting the fundamental rights of citizens and residents within the Union. Surely, police cooperation in the European Union continues to face numerous challenges that shape its developmental trajectory. Primarily, the protection of personal data and fundamental rights presents a significant challenge, with the balance between security and freedom remaining a persistent concern.

European Court of Justice rulings, such as those concerning biometric data collection (C-205/21 of 2023) and the legality of fingerprint collection in identity documents (C-61/22 of 2024), are clearly setting the boundaries of permissible intervention and require Member States to align national regulations with EU requirements.

Regarding system interoperability, challenges remain concerning the full integration of national databases with EU systems. Differences in system architecture, data standards, and national procedures hinder smooth information exchange. The level of trust between Member States' law enforcement authorities may still constitute a barrier, stemming from differences in legislation, operational procedures, and concerns about national sovereignty. Further development of a common police cooperation culture should be pursued through officer exchange programs and joint training initiatives.

EU national police forces must rapidly adapt to new criminal modus operandi, necessitating contemporary legal frameworks and EU investment in research and development. Effective police cooperation requires substantial financial and human resources as implementing innovative technologies, complex information systems, and joint operations is costly and requires consistent and adequate funding from national and the EU budgets.

In the years to come, we can expect the development of police cooperation with third countries, particularly EU neighbours and regions that are sources of criminal activity. This appears crucial in combating terrorism, organized crime, and illegal immigration. Given the increasing complexity of financial crimes and money laundering, the EU will place greater emphasis on developing capabilities in tracking financial flows and effectively recovering criminal assets.

Police cooperation within the European Union constitutes an appropriate response to complex and cross-border internal security threats that represents a dynamic and continuously evolving mechanism. The period since 2022 has brought significant reinforcement of legal and operational frameworks, responding to the necessity of adaptation to an evolving security landscape, marked by the war in Ukraine, destabilization in the Middle East, the migration crisis, and phenomenal technological advancement. The strengthening of Europol's mandate, EMPACT's development, information exchange through modernized systems, while pursuing full interoperability, is the appropriate representation of steps toward building an integrated and effective European security space.

In conclusion, police cooperation in the EU undergoes continuous development and is characterized by multidimensionality, encompassing a broad spectrum of operational tools and mechanisms. In the face of multiple global security threats

that do not respect national borders, decisive and well-coordinated action by all Member States' police forces remains a sine qua non condition for ensuring the protection of Union citizens. The development of this cooperation, while maintaining parallel respect for democratic values and human rights, will be paramount for the future of the European area of freedom, security, and justice.

Bibliography:

1. Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.
2. Council Framework Decision of 13 June 2002 on joint investigation teams (2002/465/JHA).
3. Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States.
4. Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, http://data.europa.eu/eli/dir/2023/977/oj.
5. Grzelak A., *Expansion of the catalogue of crimes in Article 83(1) TFEU – prerequisites, procedure and proposal to include hate crimes within the scope of EU criminal law harmonisation*, "European Legal Studies" 2025, no. 6, strony?.
6. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_pl.
7. OPINION OF ADVOCATE GENERAL PITRUZZELLA delivered on 30 June 2022 (1) Case C-205/21 Criminal proceedings against V.S., third party: Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranataprestapnost
8. https://curia.europa.eu/juris/document/document.jsf;jsessionid=F7224E4F7A500191A56E89B120053942?text=&docid=261934&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=16808143.
9. https://eur-lex.europa.eu/legalcontent/PL/ALL/?uri=COM%3A2025%3A162%3AFIN.
10. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32022H0915.
11. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM: police_judicial_cooperation.
12. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/eurojust_pl.
13. https://home-affairs.ec.europa.eu/news/commission-announces-launch-shared-biometric-matching-service-2025-05-19_en?prefLang=pl&etrans=pl.
14. *EMPACT fighting crime together*, https://home-affairs.ec.europa.eu/policies/internal-security/law-enforcement-cooperation/empact-fighting-crime-together_en.
15. https://info.policja.pl/inf/wspolpraca-miedzynarod/72445,Wspolpraca-miedzynarodowa.html.
16. *European Union Agency for Criminal Justice Cooperation, Joint investigation teams*, https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams.
17. https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
18. *EU Serious and Organised Crime Threat Assessment (EU-SOCTA)*, https://www.europol.europa.eu/publications-events/main-reports/socta-report.
19. https://www.frontex.europa.eu/about-frontex/who-we-are/tasks-mission/?etrans=pl.
20. https://www.frontex.europa.eu/media-centre/news/news-release/eu-external-borders-irregular-crossings-drop-by-20-in-first-half-of-2025-CUpZ5o.

21. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on ProtectEU: European Internal Security Strategy, COM/2025/148 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148.
22. Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. Schengen.1990.06.19 (OJ L 239, 2000).
23. Kozłowski J., *Akt o sztucznej inteligencji – charakterystyka unijnej regulacji opartej na ryzyku*, "Europejski Przegląd Sądowy" 2024, no. 12
24. Regulation (EU) 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726, (EU) 2018/1861 and Decisions 2004/512/EC and 2008/633/JHA, and Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.
25. Regulation of the Minister of Interior and Administration of 3 March 2023 on the procedure for transferring persons or objects found as a result of SIS data access, procedures for handling cases of revealed identity theft, and the method and procedure of cooperation between authorities with the SIRENE bureau (Journal of Laws 2023, item 427).
26. Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, https://eur-lex.europa.eu/eli/reg/2022/991/oj.
27. Róg M., *Bilateral Police Cooperation between Poland and Lithuania (in light of agreements and arrangements)*, "Society and Politics" 2019, no. 3.
28. Report from the Commission to the European Parliament and the Council on the state of preparation for the full implementation of the Interoperability Regulations pursuant to Article 78(5) of Regulation (EU) 2019/817 and Article 74(5) of Regulation (EU) 2019/818.
29. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon on 13 December 2007 (Journal of Laws of 2009, No. 203, item 1569).
30. Regulation (EU) 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018).
31. Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017).
32. Regulation (EU) 2018/1240 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018).

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 273–286

ISSN 2543-6961
e-ISSN 2720-3093

Robert Siuciński
ORCID: 0000-0002-4952-4695
Uniwersytet Łódzki

Administrative procedures adopted in the EU Regulation 2024/3015 on prohibiting products made with forced labour on the Union market: The most recent EU response to human rights violations

Procedury administracyjne przyjęte w rozporządzeniu UE 2024/3015 w sprawie zakazu produktów wytwarzanych z wykorzystaniem pracy przymusowej na rynku unijnym: najnowsza odpowiedź UE na naruszenia praw człowieka

Abstract
The new EU Regulation 2024/3015 on prohibiting products made with forced labour on the Union market was published in the Official Journal of the European Union on December 12, 2024, and shall apply from December 14, 2027 (except for the several enumerated articles which apply from December 13, 2024). The author puts forward the hypothesis that the regulation fits into the global trend to combat the use of a widespread forced labour in the world. Other acts adopted in this context include e.g.: the Fighting Against Forced Labour and Child Labour in Supply Chains Act (Canada), the Uyghur Forced Labor Prevention Act (United States), the Modern Slavery Act 2015 (United Kingdom) and the Modern Slavery Act (Australia). The aim of this paper is to analyse and critically assess the administrative procedures adopted in the EU regulation, assuming that particular attention will be paid to "investigations", "decisions", and "enforcement" issues. The author tests the hypothesis that the regulation fits into the third generation administrative procedures.

Keywords: administrative procedure, forced labour, products made with forced labour, the EU Regulation on prohibiting products made with forced labour on the Union market, the lead competent authority

Abstrakt
Nowe rozporządzenie UE 2024/3015 w sprawie zakazu produktów wytwarzanych z wykorzystaniem pracy przymusowej na rynku unijnym zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej 12 grudnia 2024 r. i wejdzie w życie 14 grudnia 2027 r. (z wyjątkiem kilku wskazanych w nim artykułów, które weszły w życie 13 grudnia 2024 r.). Autor stawia hipotezę, że rozporządzenie wpisuje się w globalny trend zwalczania powszechnego wykorzystywania pracy przymusowej na świecie. Inne akty prawne przyjęte w tym zakresie to m.in.: ustawa o walce z pracą przymusową i pracą dzieci w łańcuchach dostaw (Kanada), ustawa o zapobieganiu pracy przymusowej Ujgurów (Stany Zjednoczone), ustawa o współczesnym niewolnictwie z 2015 r. (Wielka Brytania) oraz ustawa o współczesnym niewolnictwie (Australia). Celem niniejszego artykułu jest analiza i krytyczna ocena procedur administracyjnych przyjętych w rozporządzeniu UE, przy założeniu, że szczególna uwaga zostanie poświęcona kwestiom „dochodzeń", „decyzji" i „egzekwowania". Autor testuje hipotezę, według której rozporządzenie wpisuje się w procedury administracyjne trzeciej generacji.

Słowa kluczowe: postępowanie administracyjne, praca przymusowa, produkty wytwarzane z wykorzystaniem pracy przymusowej, rozporządzenie UE w sprawie zakazu produktów wytwarzanych z wykorzystaniem pracy przymusowej na rynku unijnym, wiodący właściwy organ

Introduction

The aim of this article is to analyse and assess the administrative procedures adopted in the Regulation (EU) 2024/3015 of the European Parliament and of the Council of 27 November 2024 on prohibiting products made with forced labour on the Union market and amending Directive (EU) 2019/1937[1] (hereinafter referred to as "the EU regulation" or "the regulation")[2]. As stated in the EU regulation itself, the global number of people in forced labour is estimated at 27.6 million. It is further highlighted that women and children, persons with disabilities, ethnic minorities, lower casters, indigenous and tribal people, as well as migrants, in particular undocumented ones, who have a precarious status and operate in the informal economy are the most vulnerable groups to experience forced labour. Effective actions are necessary to prevent the persistence of forced labour,[3] the freedom of which is considered a human right,[4] and the EU regulation is a response to this need.

[1] Regulation (EU) 2024/3015 of the European Parliament and of the Council of 27 November 2024 on prohibiting products made with forced labour on the Union market and amending Directive (EU) 2019/1937 (Text with EEA relevance), OJ L, 2024/3015, https://eur-lex.europa.eu/eli/reg/2024/3015/oj/eng#ntr2-L_202403015EN.000101-E0002 [date of access: 12.12.2024].

[2] For earlier research, see: A. Fruscione, *The European Commission Proposes a Regulation to Ban Products Made With Forced Labour*, "Global Trade and Customs Journal" 2023, vol. 18, issue 3, pp.120-124; F. Caygın Aydın, *Strengthening the EU's Stand Against Forced Labour: the Regulation on Prohibiting Products Made with Forced Labour*, The Danish Institute for Human Rights 2025, https://www.humanrights.dk/files/media/document/Forced%20Labour%20Regulation%20report_070125.pdf; Grado V., *Trade Prohibitions on Forced-Labour Products: A First Assessment of the Forthcoming EU's Forced Labour Regulation,* [in:] eds. J. Bäumler et al., "European Yearbook of International Economic Law", vol. 15, Cham 2024, pp 149–190; C. Methven O'Brien, A. Weatherburn, *Commission Proposal for a Regulation on prohibiting products made with forced labour on the Union market: The issue of remedies*, European Parliament, 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702583/EXPO_BRI(2023)702583_EN.pdf; C. Martínez San Millán, *European Union's governance through trade. Considerations on the Proposal for a Regulation on prohibiting products made with forced labour on the Union market*, "Spanish Yearbook of International Law" 2023, no. 27, pp. 163-189; A. Altmayer, S. Spinaci, *Proposal for a ban on goods made using forced labour, Briefing EU Legislation in Progress*, PE 739.356, November 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739356/EPRS_BRI(2023)73 9356_EN.pdf; N. Burnichon, A. Bourgin, *Les futures obligations en matière de lutte contre le travail forcé pour les opérateurs européens: une approche comparée au regard du droit américain*, "Revue Lamy Droit des affaires" 2023, no. 197, pp. 16-22; O. Claude, C. Ghilardi, *Les réglementations émergentes sur l'interdiction des produits issus du travail forcé; Note sous Commission Européenne, doc. COM(2022) 453 final, 14 septembre 2022, proposition de règlement relatif à l'interdiction des produits issus du travail forcé sur le marché de l'Union*, "Revue internationale de la compliance et de l'éthique des affaires" 2022, no. 6, pp. 36-37.

[3] A lot of research has been done on forced labour. For example, see: International Labour Conference, *A global alliance against forced labour. Global Report under the Follow-up to the ILO Declaration on Fundamental Principles and Rights at Work 2005*, International Labour Office, Geneva 2005, https://webapps.ilo.org/public/english/standards/relm/ilc/ilc93/pdf/rep-i-b.pdf; D. R. Maul, *The International Labour Organization and the Struggle against Forced Labour from 1919 to the Present*, "Labor History" 2007, vol. 48, issue 4, pp. 477–500; N. Phillips, F. Mieres, *The Governance of Forced Labour in the Global Economy,* "Globalizations" 2014, vol. 12, issue 2, pp. 244-260; L. Palumbo, *Slavery, Forced Labour, and Trafficking,* [in:] *Taking Vulnerabilities to Labour Exploitation Seriously. A Critical Analysis of Legal and Policy Approaches and Instruments in Europe*, ed. L. Palumbo, IMISCOE Research Series, Cham 2024, pp. 1-30.

[4] International Labour Organization*, ILO Declaration on Fundamental Principles and Rights at Work*, International Labour Conference, 86th Session, Geneva 1998.

In respect of the research methods and techniques used in this article, the author conducts a critical analysis of primary and secondary sources. The former embrace, in particular, legal acts discussed in this work, and the latter include the subject literature. Thus, the method of analysis and criticism of literature, as well as the dogmatic-legal method (or analytical method) allowing for the analysis and interpretation of legal acts are employed. Auxiliarily, comparative legal methodology is used with regard to the need to analyse foreign (non-EU) law. Finally, the hypothetico-deductive methodology is applied in this article. This means that "a causal hypothesis is initially formulated, some observational consequences are predicted on the base of this hypothesis and they are finally confronted with the data."[5]. In other words, the author will start with two "probable hypotheses and find further support for them through positive confirmations."[6].

In order to give a clear picture of the different possible approaches in the world to the topic discussed, namely prohibiting products made with forced labour, the author puts forward a hypothesis that the EU regulation fits into the global trend to combat the use of widespread forced labour. He will analyse the EU regulation in the context of a similar legislation that was previously adopted in the United States: the Uyghur Forced Labor Prevention Act.[7] He will also note the existence of some other acts adopted in this context in Canada, in the United Kingdom and Australia.

Besides, in this article the author will test the hypothesis that the EU regulation fits into the use of so-called third generation administrative procedures. The EU regulation refers to the introduction of socially significant public policies with the use of appropriate administrative procedures (policy – and decision-making procedures). It establishes controls and the evaluation of the enforcement and the implementation of the regulation, which exert impact on its efficiency, thanks to which the implementation of administrative procedures can be perceived as an ongoing process.[8]

---

[5] S. Mateiescu S., *The Limits of Interventionism – Causality in the Social Sciences,* [in:] *Probabilities, Laws, and Structures*, eds. D. Dieks, W.J. González, S. Hartmann, M. Stöltzner and M. Weber, Dordrecht 2012, p. 152. More: Russo F., *Causality and causal modelling in the social sciences. Measuring variations.* Methodos Series. New York 2009, p. 70 et seq.

[6] W. C. Salmon W.C., *The Foundations of Scientific Inference. 50th Anniversary Edition*, University of Pittsburgh Press 2017, p. 115.

[7] H.R. 1155 – Uyghur Forced Labor Prevention Act, 117th Cong. (2021–2022), *Ensuring that goods made with forced labor in the Xinjiang Uyghur Autonomous Region of the People's Republic of China do not enter the United States market, and for other purposes*, https://www.congress.gov/bill/117th-congress/house-bill/1155/text [date of access?[date of access: 12.12.2024]

[8] J. Barnes, *Three generations of administrative procedures,* [in:] *Comparative Administrative Law*, eds. S. Rose-Ackerman, P.L. Lindseth, B. Emerson, Cheltenham 2017, pp. 302-318; J. Barnes, *Towards a third generation of administrative procedure.* First draft – Conference on Comparative Administrative Law, April 29-30, 2016, https://law.yale.edu/sites/default/files/area/conference/compadmin/compadmin16_barnes_towards.pdf; J. Barnes, *El procedimiento administrativo. Análisis histórico y comparado,* [in:] *Curso de Derecho Administrativo*

Before discussing the procedures adopted in the EU regulation, it should be stressed that for the purposes of the EU regulation under discussion, forced labour "means forced or compulsory labour as defined in Article 2 of ILO Convention No 29, including forced child labour"; and forced labour imposed by state authorities "means the use of forced labour as described in Article 1 of ILO Convention No 105". Importantly, a very broad definition of "a product made with forced labour" has been adopted for the purposes of the regulation. It means "a product for which forced labour has been used in whole or in part at any stage of its extraction, harvest, production or manufacture, including in the working or processing related to a product at any stage of its supply chain".

The article proceeds in five parts. After the introduction, part 1 explores the Uyghur Forced Labor Prevention Act, which is in force in the United States, part 2 "investigations", part 3 "decisions", and part 4 "enforcement of decisions" issues. Part 5 includes discussion and conclusion.

1. United States: The Uyghur Forced Labor Prevention Act

The Uyghur Forced Labor Prevention was enacted on December 23, 2021, and took effect on June 21, 2022. This act differs from the EU regulation because it has not adopted a risk-based approach but has established a rebuttable presumption that all goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part in the Xinjiang Uyghur Autonomous Region of China, or by persons working with the Xinjiang Uyghur Autonomous Region government for purposes of the "poverty alleviation" programme or the "pairing-assistance" programme which subsidises the establishment of manufacturing facilities in the Xinjiang Uyghur Autonomous Region, shall be deemed to be goods, wares, articles, and merchandise described in section 307 of the Tariff Act of 1930 (19 U.S.C. 1307)[9] and shall not be entitled to entry at any of the ports of the United States (section 4 entitled "Prohibition on importation of goods made in the Xinjiang Uyghur Autonomous Region").[10] Moreover, the Uyghur Forced Labor Prevention

Iberoamericano, eds. J. Rodríguez-Arana, L. Rodríguez Rodríguez, M. Rodríguez Martín-Retortillo, Granada 2015, pp. 203-294.

[9] Section 307 of the Tariff Act of 1930 (19 U.S.C. 1307) states that it is illegal to import into the United States "goods, wares, articles, and merchandise mined, produced, or manufactured wholly or in part" by forced labor. Such merchandise is subject to exclusion or seizure and may lead to criminal investigation of the importer.

[10] This presumption applies unless the Commissioner of US Customs and Border Protection determines, by clear and convincing evidence, that any specific goods, wares, articles, or merchandise were not produced wholly or in part by convict labour, forced labour, or indentured labour under penal sanctions; and submits to the appropriate congressional committees and makes available to the public a report that contains such determination.

Act has another important characteristic related to the enforcement strategy to effectively address forced labour in the Xinjiang Uyghur Autonomous Region of China or products made by Uyghurs, Kazakhs, Kyrgyz, Tibetans, or members of other persecuted groups through forced labour in any other part of China. The strategy includes issuing specific "Withhold Release Orders" to support enforcement of section 4, with regard to each listed facility or entity.[11] At the time of writing this article (June 2025), the last Withhold Release Order was issued by the US Customs and Border Protection on May 28, 2025. It was issued against Zhen Fa 7, a Chinese-flagged fishing vessel. It means that the US Customs and Border Protection officers at all US ports of entry detain seafood harvested by Zhen Fa 7 "based on reasonable suspicion that the vessel uses forced labor to harvest such seafood."[12] This approach is completely different from the one designed by the EU, which will be discussed below.

It should be noted that such acts/regulations concerning the fight against forced labour are part of a broader current trend. The scope of this study does not allow for a comprehensive discussion of all legal acts, but it is worth paying particular attention to, e.g.: the Fighting Against Forced Labour and Child Labour in Supply Chains Act adopted in Canada,[13] the Modern Slavery Act 2015 adopted in the UK[14] and the Modern Slavery Act 2018 adopted in Australia.[15]

Investigations

Article 3, namely "Prohibition of products made with forced labour" is the essence of the EU regulation. According to this provision, "economic operators shall not

[11] On the Uyghur Forced Labor Prevention Act see also: M.M. Fang, *A Never-Ending U.S.-China Solar Trade War? The Uyghur Forced Labor Prevention Act and International Trade Law*, "Minnesota Journal of International Law" 2024, vol. 33, issue 1, pp. 189-225, https://scholarship.law.umn.edu/minn-jrnl-intl-law/vol33/iss1/4; Y. Ru, *The US Uyghur Forced Labor Protection Act: the GATT 1994 Perspective*, "Journal of World Trade" 2024, vol. 58, issue 5, pp. 761-779, https://kluwerlawonline.com/journalarticle/Journal+of+World+Trade/58.1/TRAD2024038; S. Kang, *WTO-Consistency of the Uyghur Forced Labor Prevention Act (UFLPA): The Re-Emergence of the Process Production Methods (PPM) Regulations*, "Asian Journal of WTO & International Health Law and Policy" 2024, vol. 19, no. 2, pp. 281-314.

[12] Customs and Border Protection, CBP issues Withhold Release Order on Zhen Fa 7, May 28, 2025, https://www.cbp.gov/newsroom/national-media-release/cbp-issues-withhold-release-order-zhen-fa-7 [date of access: 12.12.2024]

[13] Fighting Against Forced Labour and Child Labour in Supply Chains Act, S.C. 2023, c. 9, Assented to 11 May 2023, consolidated to 2 December 2025, https://laws.justice.gc.ca/eng/acts/F-10.6/page-1.html [date of access: 12.12.2024].

[14] **Modern Slavery Act 2015**, *c.* 30, enacted 26 March 2015, United Kingdom of Great Britain and Northern Ireland, https://www.legislation.gov.uk/ukpga/2015/30/contents/enacted [date of access: 12.12.2024].

[15] **Modern Slavery Act 2018 (Cth)**, *Act No. 153 of 2018*, enacted 10 December 2018, in force 1 January 2019, Commonwealth of Australia, https://www.legislation.gov.au/C2018A00153/latest/text [date of access: 12.12.2024]. jeśli podajemy stronę internetową, to [date of access], jeśli źródło, to wydaje mi się, że analogicznie do str. 2 podpunkt f z wytycznych: Federal Register of Legislation of 2018, item

place or make available on the Union market products that are made with forced labour, nor shall they export such products".[16] It should be however mentioned that the EU regulation does not apply to the withdrawal of products which have reached so-called "end users" in the EU market.

Unlike in the United States where a rebuttable presumption has been established, the EU has decided to adopt a risk-based approach when evaluating the "likelihood" of a breach of the prohibition included in Article 3.

Before going into details on the risk-based approach and the investigations, it is important for us to note which bodies are responsible. Thus, when it comes to the "allocation of investigations", on the one hand, the Commission will act as the lead competent authority in cases where the suspected forced labour is taking place outside the territory of the Union. On the other hand, in a situation where the suspected forced labour is taking place in the territory of a Member State, a competent authority of that Member State (and not the Commission) will act as the lead competent authority. In the original project of the EU regulation, a much greater burden and obligations rested on Member States, so this change and the final shape of the regulation should be assessed positively.

Importantly, a risk-based approach is used not only when evaluating the "likelihood" of a breach of a prohibition included in Article 3, but also "when initiating and conducting the preliminary phase of the investigations and when identifying the products and economic operators concerned". However, as set out in the EU regulation, when assessing the "likelihood" of a breach Article 3, both the Commission and the competent authorities should take into consideration "all relevant, factual, and verifiable information" available to them, and use certain criteria "in order to prioritise products suspected to have been made with forced labour". These criteria are as follows:

- "the scale and severity of the suspected forced labour, including whether forced labour imposed by state authorities could be a concern"
- "the quantity or volume of products placed or made available on the Union market"
- "the share of the part of the product suspected to have been made with forced labour in the final product".

At this point, the question of what the risk-based approach is (in the context of initiating a preliminary investigation) should be answered. Consequently, when initiating a preliminary investigation, the lead competent authority should (to

[16] Regulation (EU) 2024/3015 of the European Parliament and of the Council of 27 November 2024 on prohibiting products made with forced labour on the Union market, op. cit., Art. 3.

the extent possible) concentrate "on the economic operators and, where relevant, product suppliers involved in the steps of the supply chain as close as possible to where the forced labour is likely occurring, and with the highest leverage to prevent, mitigate and bring to an end the use of forced labour." Moreover, the lead competent authority should focus on "the size and economic resources of the economic operators" in question, "in particular whether the economic operator is an SME, and the complexity of the supply chain."

From the point of view of the efficient conduct of the procedure, the principle of coordination of investigations and mutual assistance is crucial. In the light of the EU regulation, the Commission and competent authorities should "cooperate closely with each other and provide each other with mutual assistance" so that they are able to implement the EU regulation "in a consistent and efficient" way. The EU regulation under discussion clarifies that on each occasion (in other words – at all stages of the process) the lead competent authority should respect the right of the economic operator to be heard. There is also an additional duty on the lead competent authority, namely, to communicate via the information and communication system (referred to in Article 34 of the EU Regulation 2019/1020[17]) if it finds out new information about suspected forced labour taking place in a territory for which it is not competent.

At the same time, the lead competent authority can get appropriate help from other relevant competent authorities upon request. Such help may involve, for example, "requesting support in order to contact economic operators whose place of establishment is within the territory of that Member State or whose language of operation is that of a Member State."

Article 17 of the EU regulation concerns preliminary phase of investigations. This provision stipulates that prior to launching an investigation, the lead competent authority should "request information from the economic operators" in respect of which the assessment is made and, "where relevant, other product suppliers, on the relevant actions they have taken in order to identify, prevent, mitigate, bring to an end or remediate risks of forced labour in their operations and supply chains with respect to the products under assessment". Economic operators are given 30 working days for reply and are allowed to submit any other information they consider useful. Next, the lead competent authority concludes the preliminary phase of its investigation and makes a decision whether there is a substantiated concern that economic operators have placed or made available on

[17] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance), OJ L 169, 25.6.2019, p. 1–44.

the Union market products made with forced labour, or they have exported such products. The existence of such a concern regarding violation of Article 3 is one of the most important elements of the procedure because it leads to the opening of an investigation. Particular attention should be paid to the matters to be communicated to economic operators subject to the investigation within 3 working days of the date of the decision to trigger such investigation. These are as follows:

- the commencement of the investigation,
- the possible consequences of the investigation,
- the products subject to the investigation,
- the reasons for the commencement of the investigation, unless it would jeopardise its outcome,
- the right of the economic operators to submit documents or information to the lead competent authority, and the date by which such information should be submitted.

There are numerous information obligations on the part of economic operators under investigation. If the lead competent authority so requests, they must provide (within 60 working days, but rightly with the possibility of an extension) any information that is necessary and relevant for the investigation. This includes "information identifying the products under investigation and, where appropriate, identifying the part of the product to which the investigation should be limited, as well as the manufacturer, producer, product supplier, the importer or the exporter of those products or parts thereof." Following the risk-based approach, the lead competent authority (when requesting such information) prioritises the economic operators involved in the steps of the supply chain as close as possible to where the forced labour is likely occurring. Besides, the lead competent authority considers the economic operators' size and resources, including whether it is a small or medium-sized enterprise, the quantity of products in question, the complexity of the supply chain, and the scale of suspected forced labour.

Under exceptional circumstances and only if necessary, organising field inspections would be possible, but it is the duty of the lead competent authority to take account of the place where the risk of forced labour is situated. On the one hand, the lead competent authority carries out its inspection under national and the EU laws where the risk of forced labour is situated in the Member State's territory. On the other hand, where the risk of forced labour is situated outside the EU's territory, the lead competent authority, namely the Commission as explained above, is bound to conduct all necessary checks and inspections subject to prior consent from the economic operators in question, as well as subject to notification

to the government of the third country in which the inspections are to take place and provided there is no objection from that government.

Decisions

It is incumbent upon the lead competent authority to assess all information and evidence and decide whether or not Article 3 of the EU regulation has been violated. Importantly, it should endeavour to adopt its decision or close the investigation within 9 months of the date it initiated the investigation. The EU regulation imposes an obligation on the lead competent authority to close the investigation and inform the economic operators about this fact[18] if it cannot establish a violation of Article 3. Closing the investigation does not preclude the initiation of a new investigation in relation to the same product and economic operator in the case of new relevant information.

This article is aimed at analysing all important elements of the decision issued by the lead competent body in the event that it discovers a breach of Article 3. Thus, such a decision shall contain:

- a prohibition on the placing or making available of the products in question on the EU market and on exporting them,
- an order requiring the economic operators that have been subject to the investigation to withdraw the products that have already been placed or made available on the EU market or to remove content from an online interface referring to the products or listings of the products concerned,
- an order requiring the economic operators that have been subject to the investigation to dispose of the products concerned or, if parts of the product which are found to be in violation of Article 3 are replaceable, an order requiring those economic operators to dispose of those parts of that product. Significantly, decisions taken by a lead competent authority of one Member State should be recognised and enforced by competent authorities in the other Member States, "insofar as they relate to products with the same identification information and as originating from the same supply chain which has been found to be using forced labour."

The economic operators affected by a decision may request a review of that decision at any time.[19] However, such a request should be accompanied by all information demonstrating that the products are placed or made available on the market or are to be exported in compliance with Article 3. "That information shall contain new substantial information that was not brought to the attention of the lead competent authority during the investigation".

[18] As well as all other competent authorities through the information and communication system.

[19] The lead competent authority takes a decision within 30 working days of the receipt of that request.

Last but not least, Article 22 of the EU regulation regulates the content of decisions regarding the violation of Article 3. Thus, a decision should embrace all of the following:

- the findings of the investigation ,
- the information, as well as the evidence underpinning the findings,
- reasonable time limits for the economic operators to comply with the orders, which shall not be less than (generally) 30 working days; when setting the time limits, the lead competent authority should take into consideration the size and economic resources of the economic operator, including whether the operator is a small or medium-sized enterprise, the share of the part of the product and whether it is replaceable; the time limits shall be proportionate to the time needed to comply with the different orders and no longer than necessary,
- all relevant information, in particular the details allowing the identification of the product to which the decision applies, including details about the manufacturer, producer, product suppliers, the importer, the exporter and, where appropriate, the production site,
- where available and applicable, information required under customs legislation as defined in Article 5, point 2, of the EU Regulation No 952/2013,[20]
- information on the taking of a judicial review against a decision.

It is worth stressing that the Commission should adopt implementing acts further specifying the details of the information to be included in the decision.

Enforcement of decisions

It may always happen that an economic operator fails to comply with the above-discussed decision. In such a situation, the competent authorities are responsible for the enforcement of that decision. Thus, they shall ensure all of the following:

- the prohibition on the placing or making available of the products in question on the EU market and on the export of them,
- the withdrawal from the EU market by relevant authorities of products that have already been placed or made available on the market, in accordance with the EU and national laws,
- the disposal of withdrawn products and products remaining with the economic operator, at the expense of that economic operator,

[20] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (recast), OJ L 269, 10.10.2013, p. 1–101.

– the restriction of access to the products concerned and to listings referring to those products by requesting the relevant third party to implement such restriction.

Additionally, penalties will be imposed on the economic operator which has failed to comply with the decision. Penalties will be inflicted by the competent authority either directly, in cooperation with other authorities, or by way of an application to the competent judicial authorities.

It is interesting to note that an order to withdraw and dispose of products placed or made available on the EU market should be communicated, through the information and communication system, to the market surveillance authorities referred to in Article 10 of Regulation (EU) 2019/1020 and any other relevant authorities for the products in question. The enforcement of the withdrawal and disposal of the above-mentioned products should be the responsibility of the competent authority, in coordination with any other relevant authorities for the products in question.

When it comes to the method of disposal of products made with forced labour, economic operators and the Member States competent authorities responsible for the disposal of products should dispose of those products by recycling them or, when that is not possible, by rendering those products inoperable. Perishable products should be donated for charitable or public interest purposes or, when that is not possible, be rendered inoperable. The method of disposal of products made with forced labour should be in compliance with the waste hierarchy regulated in Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives.[21]

Discussion and conclusion

A special issue of "Public Administration and Security Studies" is devoted to "analysing Europe's response to contemporary crises and their wider implications".[22] The aim of the issue is to "examine the multifaceted challenges confronting Europe, including the European Union and its member states […]". In fact, Europe has been flooded with products derived from forced labour for a long time. The crisis of human rights violations has even increased in the past few years. For example, it has been recently revealed that "a substantial volume of apparel tainted by

[21] OJ L 312, 22.11.2008, p. 3-30.

[22] Y. Uluyol et al., *Tailoring Responsibility: Tracing Apparel Supply Chains from the Uyghur Region to Europe*, Sheffield Hallam University Helena Kennedy Centre for International Justice 2023, https://www.researchgate.net/publication/376410063_Tailoring_Responsibility_Tracing_Apparel_Supply_Chains_from_the_Uyghur_Region_to_Europe [date of access: date of access: 12.12.2024].

Uyghur forced labour is moving into the EU without restriction."[23] The new EU Regulation 2024/3015 on prohibiting products made with forced labour on the Union market is a response to that crisis.

Research has been carried out in a broader context to test two hypotheses, namely that there is a global trend towards combating forced labour and that the EU regulation fits into the use of third generation administrative procedures. This study reinforced both of them. As regards the first of the hypotheses mentioned, it has been shown that the EU regulation is not the only one aimed at solving the crisis of forced labour. Appropriate legislative solutions have also been adopted in other countries, e.g. the US, the UK, Canada or Australia (although the approaches they follow may differ significantly).

Regarding the second hypothesis, according to J. Barnes, the third-generation procedures are carried out within the framework of the networked policy-making, involving "a greater variety of actors and voices".[24] They are "based on procedural collaboration between administrations" and aim at enabling "participation in different stages". The third-generation procedures "allow for more diversity and decentralization, foster deliberative arenas, mutual learning and information gathering, and permit more flexibility, monitoring and revisability". The "ongoing information exchange between agencies at national, supranational, and global levels", "assessing public policy options", "monitoring and reviewing decisions, programs, plans, or standards" are another feature of these procedures. Moreover, the promotion of public values to be taken into consideration by private parties is inscribed in the third-generation procedures. Nevertheless, "their most characteristic feature is that they are based on collaborative governance. Collaboration focuses on bringing together and engaging critical stakeholders and administrations at a national and transnational level."[25] We should now ask: how does all this translate into the assessment of the EU regulation? As stated above, the EU regulation fits into the use of third generation administrative procedures. Apart from the obvious fact of promoting public values, for the sake of illustration only, a few of its provisions should be mentioned: first, the Commission and competent authorities should "cooperate closely with each other and provide each other with mutual assistance". Second, "if economic operators demonstrate that they have eliminated forced labour from the supply chain with regard to the product concerned, without changing that product and by bringing to an end the forced labour identified in the decision, the lead competent authority shall review its decision."

[23] Ibidem.
[24] J. Barnes, *Three generations...*, op. cit., pp. 308-309.
[25] Ibidem.

Third, by December 14, 2029, and every 5 years thereafter, the Commission shall carry out an evaluation of the enforcement and the implementation of the EU regulation. Fourth, the Commission shall create a database of forced labour risks in order to support the work of competent authorities in evaluating potential infringements of Article 3 of the EU regulation and help economic operators detect possible forced labour risks in their supply chains. Such a database should be made publicly available through the "Forced Labour Single Portal".

In conclusion, this article contributes to the literature by offering insights on the new EU Regulation 2024/3015 on prohibiting products made with forced labour on the Union market in the context of its administrative procedures. The aim of this work was to explore the administrative procedures adopted in the EU regulation, including "investigations", "decisions", and "enforcement of decisions" issues. Undoubtedly, they have the potential to actively combat forced labour, although it remains to be seen how they will be applied in practice. Further research could embrace the analysis of their effectiveness and could also answer the question whether a risk-based approach (EU) or a rebuttable presumption (US) is more effective in practice.

Bibliography

1. Altmayer A., Spinaci S., *Proposal for a ban on goods made using forced labour, Briefing EU Legislation in Progress*, PE 739.356, November 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739356/EPRS_BRI(2023)739356_EN.pdf.
2. Barnes J., *El procedimiento administrativo. Análisis histórico y comparado,* [in:] *Curso de Derecho Administrativo Iberoamericano*, eds. J. Rodríguez-Arana, L. Rodríguez Rodríguez, M. Rodríguez Martín-Retortillo, Granada 2015, pp. 203-294.
3. Barnes J., *Three generations of administrative procedures,* [in:] *Comparative Administrative Law*, eds. S. Rose-Ackerman, P.L. Lindseth, B. Emerson, Cheltenham 2017, pp. 302-318.
4. Barnes J., *Towards a third generation of administrative procedure.* First draft – Conference on Comparative Administrative Law, April 29-30, 2016, https://law.yale.edu/sites/default/files/area/conference/compadmin/compadmin16_barnes_towards.pdf.
5. Burnichon N., Bourgin A., *Les futures obligations en matière de lutte contre le travail forcé pour les opérateurs européens: une approche comparée au regard du droit américain*, "Revue Lamy Droit des affaires" 2023, no. 197, pp. 16-22.
6. Caygın Aydın F., *Strengthening the EU's Stand Against Forced Labour: the Regulation on Prohibiting Products Made with Forced Labour*, The Danish Institute for Human Rights 2025, https://www.humanrights.dk/files/media/document/Forced%20Labour%20Regulation%20report_070125.pdf.
7. Claude O., Ghilardi C, *Les réglementations émergentes sur l'interdiction des produits issus du travail forcé; Note sous Commission Européenne, doc. COM(2022) 453 final, 14 septembre 2022, proposition de règlement relatif à l'interdiction des produits issus du travail forcé sur le marché de l'Union*, "Revue internationale de la compliance et de l'éthique des affaires" 2022, no. 6, pp. 36-37.

8. Customs and Border Protection, *CBP issues Withhold Release Order on Zhen Fa 7*, May 28, 2025, https://www.cbp.gov/newsroom/national-media-release/cbp-issues-withhold-release-order-zhen-fa-7.
9. Fang M.M., *A Never-Ending U.S.-China Solar Trade War? The Uyghur Forced Labor Prevention Act and International Trade Law*, "Minnesota Journal of International Law" 2024, vol. 33, issue 1, pp. 189-225, https://scholarship.law.umn.edu/minn-jrnl-intl-law/vol33/iss1/4.
10. Fruscione A., *The European Commission Proposes a Regulation to Ban Products Made With Forced Labour*, "Global Trade and Customs Journal" 2023, vol. 18, issue 3, pp. 120-124.
11. Grado V., *Trade Prohibitions on Forced-Labour Products: A First Assessment of the Forthcoming EU's Forced Labour Regulation,* [in:] eds. J. Bäumler et al., "European Yearbook of International Economic Law", vol. 15, Cham 2024, pp. 149–190.
12. International Labour Conference*, A global alliance against forced labour. Global Report under the Follow-up to the ILO Declaration on Fundamental Principles and Rights at Work 2005*, International Labour Office, Geneva 2005, https://webapps.ilo.org/public/english/standards/relm/ilc/ilc93/pdf/rep-i-b.pdf.
13. Kang S., *WTO-Consistency of the Uyghur Forced Labor Prevention Act (UFLPA): The Re-Emergence of the Process Production Methods (PPM) Regulations*, "Asian Journal of WTO & International Health Law and Policy" 2024, vol. 19, no. 2, pp. 281-314.
14. Martínez San Millán C., *European Union's governance through trade. Considerations on the Proposal for a Regulation on prohibiting products made with forced labour on the Union market*, "Spanish Yearbook of International Law" 2023, no. 27, pp. 163-189.
15. Mateiescu S., *The Limits of Interventionism – Causality in the Social Sciences* [in:] *Probabilities, Laws, and Structures*, eds. D. Dieks, W.J. González, S. Hartmann, M. Stöltzner and M. Weber, Dordrecht 2012.
16. Maul, D. R., *The International Labour Organization and the Struggle against Forced Labour from 1919 to the Present*, "Labor History" 2007, vol. 48, issue 4, pp. 477–500.
17. Methven O'Brien C., Weatherburn A., *Commission Proposal for a Regulation on prohibiting products made with forced labour on the Union market: The issue of remedies*, European Parliament, 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702583/EXPO_BRI(2023)702583_EN.pdf.
18. Palumbo L., *Slavery, Forced Labour, and Trafficking,* [in:] *Taking Vulnerabilities to Labour Exploitation Seriously. A Critical Analysis of Legal and Policy Approaches and Instruments in Europe*, ed. L. Palumbo, IMISCOE Research Series, Cham 2024, pp. 1-30.
19. Phillips N., Mieres F., *The Governance of Forced Labour in the Global Economy,* "Globalizations" 2014, vol. 12, issue 2, pp. 244-260.
20. Ru Y., *The US Uyghur Forced Labor Protection Act: the GATT 1994 Perspective*, "Journal of World Trade" 2024, vol. 58, issue 5, pp. 761-779, https://kluwerlawonline.com/journalarticle/Journal+of+World+Trade/58.1/TRAD2024038.
21. Russo F., *Causality and causal modelling in the social sciences. Measuring variations*. Methodos Series. New York: Springer 2009.
22. Salmon W.C., *The Foundations of Scientific Inference. 50th Anniversary Edition*, University of Pittsburgh Press 2017.
23. Uluyol Y. et al., *Tailoring Responsibility: Tracing Apparel Supply Chains from the Uyghur Region to Europe*, Sheffield Hallam University Helena Kennedy Centre for International Justice 2023, https://www.researchgate.net/publication/376410063_Tailoring_Responsibility_Tracing_Apparel_Supply_Chains_from_the_Uyghur_Region_to_Europe.

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 287–302

ISSN 2543-6961
e-ISSN 2720-3093

Zbigniew Czachór
ORCID:0000-0001-9397-6261
Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim

The Rule of Law Crisis and the Conditionality Mechanism for Protecting the EU Budget: Research Assumptions Derived from the Provisions of Regulation (EU, Euratom) 2020/2092 of the European Parliament and the Council

Kryzys praworządności a system warunkowości służący ochronie budżetu Unii Europejskiej. Założenia badawcze wywiedzione z przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2020/209

Abstract
The research objective of the scientific considerations presented in this article is a multifactor analysis of the legal and political crisis within the European Union in connection with the adoption process of the EU Multiannual Financial Framework for 2021–2027 and financial instruments under the Next Generation EU initiative. The key reference point for this article is Regulation (EU, Euratom) 2020/2092 of the European Parliament and the Council of December 16, 2020, on a general conditionality mechanism for the protection of the EU budget. Based on the formal and substantive assumptions outlined in this regulation, five research assumptions have been formulated for the purposes of this study.

Keywords: crisis, EU Multiannual Financial Framework, *Next Generation EU*, regulation, conditionality system, protection of the EU budget

Abstrakt
Celem badawczym zawartych w artykule rozważań naukowych jest wieloczynnikowa analiza kryzysowej sytuacji prawnej i politycznej w Unii Europejskiej, w związku z procesem przyjmowania Wieloletnich Ram Finansowych UE na lata 2021-2027 oraz instrumentów finansowych w ramach Next Generation EU. Kluczowe znaczenie dla przygotowanego artykułu ma treść Rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2020/209 z dnia 16 grudnia 2020 r. w sprawie ogólnego systemu warunkowości służącego ochronie budżetu Unii. Z odwołaniem do zawartych w nim założeń formalnych i merytorycznych na użytek artykułu sformułowano 5 założeń badawczych uzupełnionych o uwarunkowania prawne i scenariusze na przyszłość, zawarte w podsumowaniu.

Słowa kluczowe: kryzys, wieloletnie ramy finansowe UE, Next Generation EU, rozporządzenie, system warunkowości, ochrona budżetu Unii

Introduction

The primary objective of this study is to conduct a thorough and multifactor analysis of the legal and political crisis within the European Union in the context of the adoption process of the EU Multiannual Financial Framework for 2021–2027 and financial instruments under the Next Generation EU initiative. These funds are primarily intended for the recovery of the EU following the COVID-19 pandemic and the implementation of the European Green Deal.[1]

In this scientific study, certain elements of the systemic method and institutional analysis within the framework of historical institutionalism have proven useful, as they are based on a comprehensive approach to the EU decision-making process. This analytical perspective has enabled the exposition of specific proposals as well as political and legal solutions.

From a methodological perspective, the author relied on a detailed extraction and exposition of all key statements and formulations found in the analyzed material. The study also employed methods of citation and comparison, as well as commentary and confrontation of various elements of documents (including legal acts) and statements. The entire work is divided into several sections, highlighting five research assumptions along with legal conditions and future scenarios presented in the conclusion.

The analysis is contextually embedded in the post-crisis period following the COVID-19 pandemic and other internal and external disruptions within the EU after 2020. The threat posed by the coronavirus shook Europe and the world, testing the resilience of healthcare and social systems, societies, economies, and the ways of living and working across Europe and beyond. In response to these challenges, the European Commission proposed a comprehensive recovery plan for the European Union, aiming for a sustainable, equitable, solidarity-driven, and fair implementation across all member states. The new instrument proposed by the Commission and adopted by the European Council, known as Next Generation EU, was incorporated into an effective, modern, and long-term program for systemic change.[2]

The key reference point for this article is Regulation (EU, Euratom) 2020/2092 of the European Parliament and the Council of December 16, 2020, on a general conditionality mechanism for the protection of the EU budget.[3] With reference

[1] See: Z. Czachór, *Sytuacja prawna i polityczna Polski w Unii Europejskiej w obliczu nowego podziału budżetu, w oparciu o stan praworządności w państwach członkowskich, Analiza przygotowana na zlecenie Biura Senatora Marcina Bosackiego*, Poznań 20.11.2020.

[2] *Council Regulation (EU) 2020/2094 of 14 December 2020 establishing a European Union Recovery Instrument to support the recovery in the aftermath of the COVID-19 crisis,* OJ EU L 433I, 22.12.2020.

[3] *Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget*, OJ EU, L.2020.433I.1, 22.12.2020.

to its formal and substantive assumptions, the following statements have been formulated for the purposes of this article, derived from official documents and the practice of the European Commission:[4]

- When a candidate country becomes a member state, it joins a legal
- framework based on the fundamental assumption that EU members and their institutional representatives share a set of common values on which the Union is founded, particularly those specified in Article 2 of the Treaty on European Union (TEU).[5]
- Commitment to the rule of law is inextricably linked to the respect
- for democracy and fundamental rights.
- Proper management of EU finances can only be ensured by
- member states when their public authorities act in accordance with the law and when cases of financial misconduct, including tax fraud, tax evasion, corruption, conflicts of interest, and other legal violations, are effectively prosecuted by investigative and prosecutorial authorities. Additionally, arbitrary or unlawful decisions made by public bodies, including law enforcement agencies, must be subject to effective judicial review by independent courts and the Court of Justice of the European Union.
- The independence and impartiality of the judiciary must always
- be guaranteed, and investigative and prosecutorial authorities should be able to properly fulfill their duties. Final court rulings must be effectively enforced.
- Article 19 TEU, which concretizes the rule of law value set out in
- Article 2 TEU, requires member states to ensure effective judicial protection in areas covered by EU law, including those related to the implementation of the EU budget.

Violations of the rule of law principles, particularly those affecting the proper functioning of public authorities and the effectiveness of judicial oversight, can seriously harm the financial interests of the European Union. For the purposes of this study, the author adopts the view that the concept of the "rule of law" includes: the principle of legality, meaning a transparent, accountable, democratic, and pluralistic law-making process; the principle of legal certainty; the prohibition of arbitrariness in the actions of the executive authorities; the principle of effective judicial protection, including access to justice provided by independent and

[4] *Communication from the Commission Guidelines on the application of the Regulation (EU, EURATOM) 2020/2092 on a general regime of conditionality for the protection of the Union budget 2022/C123/02*, C(2022) 1382, OJ EU C 123, final Brussels, 2.3.2022.

[5] *Consolidated version of the Treaty on European Union*, OJ C 326/13, 26.10.2012.

impartial courts, also in relation to fundamental rights; the principle of separation of powers; non-discrimination and equality before the law.[6]

In accordance with applicable EU law, the following should be considered violations of the aforementioned principles and rules: threats to judicial independence; failure to prevent, correct, or sanction arbitrary or unlawful decisions by public authorities, including law enforcement agencies; failure to allocate sufficient financial and human resources to ensure their proper functioning; or failure to prevent conflicts of interest; restricting the availability and effectiveness of legal remedies, including through overly restrictive procedural rules, failure to enforce court rulings, or limiting the effective conduct of investigations into legal violations, the prosecution of such violations, or the imposition of penalties related to them.[7]

1. First Research Assumption: The rule of law is the foundation of the European Union's system of values, as derived from the Treaty on European Union (TEU), and must be strictly upheld by all member states

The preamble to the Treaty on European Union (TEU) states: "Drawing inspiration from the cultural, religious and humanist inheritance of Europe, from which have developed the universal values of the inviolable and inalienable rights of the human person, freedom, democracy, equality and the rule of law."[8]

Another provision explicitly states that the founding states of the EU reaffirm "their attachment to the principles of liberty, democracy and respect for human rights and fundamental freedoms and of the rule of law."[9]

Article 2 of the Treaty on European Union (TEU) states: "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail."[10]

Through the Accession Treaty, which entered into force on May 1, 2004, Poland became legally bound by this international legal commitment. In the Polish translation of the Treaty on European Union (TEU), the term "praworządność" (rule of law) does not appear literally. Instead, the phrase "państwo prawne" is

[6] See: R. Potorski, M. Witkowska*, Can You Count on Luck Without Buying a Lottery Ticket? Predictions on Obtaining Funds from the National Recovery Plan in Light of the Debate on the Rule of Law in Poland*, "Studia Europejskie – Studies in European Affairs" 2024, no. 4, pp. ?.

[7] Ibidem.

[8] *Consolidated version of the Treaty on European Union*..., op. cit.

[9] Ibidem.

[10] Ibidem.

used. To refer to other language versions of the TEU, the English version uses "the rule of law", whilethe German version uses "Rechtsstaatlichkeit".

For Poland, a formal understanding of the rule of law within the EU was significantly shaped by the accession criteria established by the European Council at the Copenhagen Summit in 1993 and further reinforced at the Madrid Summit in 1995.[11]

2. Second Research Assumption: The principle of the rule of law also derives from the general principles of EU law, which complement the treaty-based regulatory system

The general principles of EU law are inseparably linked to any developed legal system. They can also be derived from the legal systems of the Member States and are common to them. Some of these principles arise from the very nature of the European Union and its objectives.

Additionally, they include fundamental rights of individuals, provided these rights hold community-wide significance. A significant portion of these principles is also embedded in the precedent-setting interpretations of EU law, as outlined in the judgments of the Court of Justice of the European Union (CJEU).

In recent years, the European Commission has developed the European Rule of Law Mechanism, based on the principles of EU law. This mechanism consists of an annual dialogue on the rule of law involving the Commission, the Council, and the European Parliament, as well as Member States, national parliaments, civil society, and other stakeholders.

The core element of this new procedure is the Rule of Law Report, which serves as a basis for discussions within the EU and aims to prevent the emergence or escalation of rule of law issues. The main objective of the mechanism is to stimulate inter-institutional cooperation and encourage all EU institutions to contribute in line with their institutional roles.[12]

The rapid identification of problems, with mutual support from the Commission, other Member States, and relevant stakeholders, including the Council of Europe and the Venice Commission, can help Member States find solutions to ensure and safeguard the rule of law.

---

[11] *Communication from the Commission to the European Parliament and the Council. A new EU Framework to strengthen the Rule of Law*, Brussels, 11.3.2014, COM(2014) 158 final; *Communication from the Commission to the European Parliament, the European Council and the Council. Further strengthening the Rule of Law within the Union. State of play and possible next steps*, Brussels, 3.4.2019, COM/2019/163 final.

[12] *Annual Rule of Law Cycle*, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/annual-rule-law-cycle_en [date of access: 31.12.2024].

3. The third research assumption: The Treaty on the European Union, to which Poland is a party, provides for the possibility of crisis sanctions for violations of EU principles (including the rule of law) in a member state, which may even result in the suspension of that state's membership rights

The text of Article 7 of the Treaty on European Union reads as follows: "On a reasoned proposal by one third of the Member States, by the European Parliament or by the European Commission, the Council, acting by a majority of four fifths of its members after obtaining the consent of the European Parliament, may determine that there is a clear risk of a serious breach by a Member State of the values referred to in Article 2. Before making such a determination, the Council shall hear the Member State in question and may address recommendations to it, acting in accordance with the same procedure. The Council shall regularly verify that the grounds on which such a determination was made continue to apply. The European Council, acting by unanimity on a proposal by one third of the Member States or by the Commission and after obtaining the consent of the European Parliament, may determine the existence of a serious and persistent breach by a Member State of the values referred to in Article 2, after inviting the Member State in question to submit its observations. Where a determination under paragraph 2 has been made, the Council, acting by a qualified majority, may decide to suspend certain of the rights deriving from the application of the Treaties to the Member State in question, including the voting rights of the representative of the government of that Member State in the Council. In doing so, the Council shall take into account the possible consequences of such a suspension on the rights and obligations of natural and legal persons. The obligations of the Member State in question under the Treaties shall in any case continue to be binding on that State. The Council, acting by a qualified majority, may decide subsequently to vary or revoke measures taken under paragraph 3 in response to changes in the situation which led to their being imposed. The voting arrangements applying to the European Parliament, the European Council and the Council for the purposes of this Article are laid down in Article 354 of the Treaty on the Functioning of the European Union."[13]

So far, the procedure under Article 7 has been initiated against Poland by the European Commission and against Hungary by the European Parliament. In both cases, no formal vote was held in the EU Council. A qualified majority needed to

[13] *Consolidated version of the Treaty on European Union*, op. cit.

support both motions was not reached. The governments of Poland and Hungary managed to (informally) establish a blocking minority.

It is worth emphasizing that on May 29, 2024, the European Commission decided to conclude the procedure under Article 7 of the Treaty on the EU against Poland. The Commission determined that there was no longer a clear violation of the rule of law in Poland, with particular reference to the judiciary. The basis for this decision was the strategy (the so-called Action Plan) proposed by Minister of Justice A. Bodnar. Poland's Action Plan for restoring the rule of law includes, among other things, reforms of the National Council of the Judiciary, the Supreme Court, and the Constitutional Tribunal, as well as the separation of the roles of Minister of Justice and Prosecutor General.[14]

4. The fourth research assumption: The Multiannual Financial Framework 2021-2027 and the Next Generation EU recovery instrument have been equipped with systemic and crisis-response mechanisms to prevent and sanction violations of the rule of law

The Multiannual Financial Framework of the EU (MFF), covering the seven-year period between 2021 and 2027 and distributed across seven annual budgets, was designed to enable Member States to respond to current and future challenges and implement modernization priorities.[15] The same arguments applied to the Next Generation EU instrument, which became a key tool for implementing the aid package in response to the socio-economic impacts of the COVID-19 pandemic.

Since 2016, EU institutions have been warning selected Member States (mainly Hungary and Poland) about violations of EU values. In Poland's case, both the European Commission and the Court of Justice of the EU have repeatedly confirmed that the judicial law undermines judicial independence and is incompatible with the principle of the primacy of EU law. This law prevents Polish courts from directly applying certain EU legal provisions protecting judicial independence and from referring such matters to the Court of Justice of the European Union for a preliminary ruling.

The confrontation between Hungary and Poland and the EU and its institutions over respect for EU values, particularly the rule of law, did not lead to a compromise. As a result, the European Commission proposed an early warning mechanism that enables dialogue between the Commission and a Member State

[14] *Zakończenie procedury z art. 7 Traktatu o UE wobec Polski*, https://www.gov.pl/web/sprawiedliwosc/zakonczenie-procedury-z-art-7-traktatu-o-ue-wobec-polski [date of access: 1.01.2025].

[15] *Council Regulation (EU, Euratom) 2020/2093 of 17 December 2020 laying down the multiannual financial framework for the years 2021 to 2027*, OJ EU L 433I, 22.12.2020, pp. 11–22.

on budgetary matters, preventing the emergence of a systemic threat to the rule of law. This dialogue served as an alternative to the procedure under Article 7 of the TEU and is referred to as an additional pre-preventive procedure.[16]

On October 12, 2017, the EU Council adopted a regulation implementing enhanced cooperation in establishing the European Public Prosecutor's Office (EPPO), which became the authority responsible for investigating, prosecuting, and bringing to trial cases related to crimes affecting the financial interests of the EU.[17] Less than a year later, on May 5, 2018, the European Commission presented a proposal for a regulation of the European Parliament and the Council on the protection of the EU budget (COM(2018) 324 final) in cases of generalized deficiencies in the rule of law in Member States. The content of this regulation introduced the rule of law conditionality mechanism, aimed at protecting the budget (Multiannual Financial Framework) and EU funds from the *Next Generation EU* instrument.[18] The European Commission was supported in this matter by the European Parliament, which adopted an extraordinary legislative resolution on April 4, 2019.[19]

In July 2020, during a meeting, the European Council agreed to introduce a conditionality mechanism to protect the budget and the *Next Generation EU* instrument, referring to the EU values enshrined in Article 2 of the TEU. Poland supported this solution.

The text of the European Council Conclusions from July 17-21, 2020, which were supported by all EU Member States, reads as follows: "The financial interests of the Union shall be protected in accordance with the general principles enshrined in the Union Treaties, in particular in line with the values set out in Article 2 TEU. The European Council emphasizes the importance of protecting the financial interests of the Union. The European Council stresses the importance of respecting the rule of law. On this basis, a conditionality mechanism will be introduced to protect the budget and the Next Generation EU instrument. In this context, the Commission will

[16] *Mechanizmy na rzecz przestrzegania praworządności w Unii Europejskiej*, https://oide.sejm.gov.pl/oide/en/images/files/pigulki/Rule_of_law.pdf [date of access: 2.01.2025].

[17] *Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'),* OJ EU L 283, 31.10.2017. pp. 1-71.

[18] *Proposal for a Regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States*, COM/2018/324 final – 2018/0136 (COD).

[19] *Protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States. European Parliament legislative resolution of 4 April 2019 on the proposal for a regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States (COM(2018)0324 – C8-0178/2018 – 2018/0136(COD)) P8_TC1-COD(2018)0136 Position of the European Parliament adopted at first reading on 4 April 2019 with a view to the adoption of Regulation (EU) of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States*, OJ EU C 116, 31.3.2021, pp. 150-161.

propose measures in cases of violations, to be adopted by the Council by qualified majority. The European Council will swiftly return to this matter."[20]

The European Council, with its decision, weakened the European Commission's 2018 proposal, as it determined that the qualified majority procedure in the EU Council would apply when adopting the Commission's proposal on rule of law violations. This effectively ruled out the "reverse qualified majority voting" procedure in the EU Council, which would have required a qualified majority to reject the Commission's proposal regarding a Member State's potential rule of law violations and the subsequent freezing or withdrawal of its financial resources.

According to the European Council Conclusions from July 2020, which Poland also agreed to**,** the European Commission, the EU Council, and the European Parliament were authorized to establish a legal procedure for applying the conditionality principle in relation to the EU funds disbursement system for Member States.[21] These institutions effectively took action in this regard, leading to the adoption of a new EU regulation that sanctions the rule of law violations by Member States.

The 2020 regulation introduced a new conditionality mechanism, allowing the European Commission to suspend or withdraw EU funds from Member States where generalized deficiencies in the rule of law are detected. The regulation explicitly states that its provisions aim to protect the EU's financial interests. Generalized deficiencies in the rule of law in a Member State affect or may affect (pose a serious risk to) EU funds, particularly when they undermine: the proper functioning of national authorities responsible for executing the EU budget, especially in the context of public procurement, monitoring, and control; the effective operation of investigative and law enforcement authorities in prosecuting financial fraud, corruption, or other violations of EU law related to budget execution; judicial oversight of actions or omissions affecting EU funds; rules preventing and penalizing financial fraud, corruption, and other breaches of EU law, including ensuring effective and dissuasive sanctions imposed by national courts and administrative bodies; the recovery system for unduly paid funds; the efficiency and timeliness of cooperation – based on relevant legal acts and the principle of sincere cooperation – with the European Anti-Fraud Office (OLAF) and the European Public Prosecutor's Office (EPPO) in the course of their investigations, preliminary proceedings, or prosecutions.[22]

---

[20] *Special meeting of the European Council (17, 18, 19, 20 and 21 July 2020). Conclusions*, General Secretariat of the Council, EUCO 10/20, European Council, Brussels, 21 July 2020.

[21] In the framework of the co-decision procedure based on qualified majority voting (QMV) in the Council of the EU.

[22] *Regulation (EU, Euratom) 2020/2092...,* op. cit., pp. 1-10.

5. Fifth research assumption: EU institutions, led by the European Commission, the European Parliament, and the Court of Justice of the EU, have developed a new crisis-response system for monitoring and sanctioning rule of law violations in Member States

Respect for the rule of law is one of the fundamental conditions for EU membership, but it must also align with the principle of sound financial management, as stipulated in Article 317 of the Treaty on the Functioning of the European Union (TFEU).[23]

Financial management can only be ensured by Member States when public authorities act in accordance with the law and when cases of financial misconduct – including tax fraud, tax evasion, corruption, conflicts of interest, and other legal violations – are effectively prosecuted by investigative and prosecutorial authorities. Additionally, arbitrary or unlawful decisions made by public authorities, including law enforcement agencies, must be subject to effective judicial oversight by independent courts and the Court of Justice of the European Union.[24]

The new system for monitoring and sanctioning rule of law violations in Member States, as outlined in the analyzed regulation, establishes that judicial independence and impartiality must always be guaranteed, and that investigative and prosecutorial authorities must be able to properly fulfill their duties. The judiciary, investigative services, and prosecution authorities must have sufficient financial and human resources as well as adequate procedures to operate effectively while ensuring full respect for the right to an impartial trial, including the right to defense. Additionally, final court rulings must be effectively enforced. These conditions serve as minimum safeguards against unlawful and arbitrary decisions by public authorities that could harm the EU's financial interests.[25]

"Judicial independence requires, in particular, that a given judicial body is able to perform its functions fully autonomously – both under the applicable legal provisions and in practice without being subject to a hierarchical structure, without subordination to any entity, and free from instructions or directives from any source. In this way, it remains protected from external interference or pressure that could jeopardize the independence of its members' judgment and influence their decisions.

Guarantees of independence and impartiality require the existence of rules – especially concerning the composition of the judicial body, the appointment of its

[23] *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 Tables of equivalences*, OJ EU C 202, 7.6.2016, pp. 1-388.

[24] *Regulation (EU, Euratom) 2020/2092...,* op. cit., p. 2.

[25] Ibidem.

members, the duration of their terms of office, and the grounds for their exclusion or removal. These rules must eliminate, in the eyes of the parties to proceedings, any reasonable doubt about the judicial body's independence from external factors and its neutrality concerning the competing interests before it."[26]

Determining violations of the rule of law requires the Commission to conduct a thorough qualitative assessment. This assessment must be objective, impartial, and fair, taking into account relevant information from available sources and recognized institutions. These sources include judgments of the Court of Justice of the European Union**,** reports from the European Court of Auditors**,** the Commission's annual rule of law reports, and the EU Justice Scoreboard. Additionally, the assessment should consider reports from the European Anti-Fraud Office (OLAF), and where applicable, the European Public Prosecutor's Office (EPPO), as well as findings and recommendations from relevant international organizations and networks. This includes Council of Europe bodies, such as the Group of States against Corruption (GRECO) and the Venice Commission, particularly its Rule of Law Checklist. The European Network of Supreme Courts and the European Network of Councils for the Judiciary should also be consulted. If necessary, the Commission could seek further consultation with the EU Agency for Fundamental Rights and the Venice Commission to ensure a comprehensive qualitative assessment.[27]

The measures provided in this regulation are necessary, particularly in cases where other procedures established in Union law would not provide more effective protection of the EU budget. EU financial legislation, along with applicable sectoral and financial rules, includes various mechanisms to protect the budget, such as suspension, withholding, or financial corrections in response to irregularities or serious deficiencies in management and control systems. It is essential to define both the measures to be taken in cases of violations of the rule of law and the procedure for adopting such measures. These measures should include:s-Suspension of payments and commitments; – sSuspension of disbursement of installments or early repayment of loans; – rReduction of funding under existing commitments, and prohibition on incurring new obligations for beneficiaries or entering into new loan agreements or other instruments guaranteed by the EU budget.

When determining the measures to be adopted, the principle of proportionality should apply. This means taking into account: the severity of the crisis situation ; the time elapsed since the initiation of the relevant action; the duration

[26] **Court of Justice of the European Union.** Judgment of 27 February 2018, *Associação Sindical dos Juízes Portugueses v Tribunal de Contas* (Case C-64/16). ECLI:EU:C:2018:117, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0064 [date of access: 31.12.2024].

[27] *Regulation (EU, Euratom) 2020/2092...,* op. cit., p. 2.

and recurrence of the violation; the intent and level of cooperation of the Member State in addressing the breaches of the rule of law; the impact of these violations on the proper management of EU budget finances or on the EU's financial interests.[28]

This provides empirical evidence of the effectiveness of the new rule-of-law control and sanctioning system introduced by Regulation (EU, Euratom) 2020/2092. One key example is the European Commission's continued refusal to lift the blockade on payments to Hungary, imposed in 2022 under the conditionality mechanism analyzed in this article.

The €6 billion payout to Hungary remains frozen due to violations of the regulation in areas such as: public procurement; prosecutorial actions; conflicts of interest; anti-corruption efforts. Additionally, concerns were raised over the so-called trusts, which manage EU funds but are not subject to EU public procurement law.[29]

Secondly, both Hungary and Poland filed a complaint with the Court of Justice of the European Union (CJEU), seeking the annulment of Regulation (EU, Euratom) 2020/2092. In their complaints, they argued that: the EU Treaties do not provide a proper legal basis for adopting the regulation; the EU exceeded its competences in establishing the rule-of-law conditionality mechanism; the regulation violates the principle of legal certainty.[30]

The Court of Justice of the European Union (CJEU) ruled that sound financial management of the EU budget and the financial interests of the Union could be seriously threatened by violations of the rule of law in a member state. As a result, the "horizontal conditionality mechanism", established by the regulation which ties access to EU funds to compliance with rule-of-law principles, falls within the EU's competence to establish "financial rules" for the implementation of the budget. The CJEU also confirmed that this procedure does not circumvent the process established under Article 7 TEU and does not exceed the competences conferred upon the EU. Therefore, the Court dismissed the complaints filed by Hungary and Poland in their entirety.[31]

In response to the crisis situation in Hungary and Poland, the European Parliament adopted an extraordinary resolution in 2022. The resolution referenced

[28] Ibidem.

[29] *Komisja Europejska zadecydowała. Blokada pieniędzy dla Węgier*, 16.12.2024, https://www.money.pl/pieniadze/blokada-pieniedzy-dla-wegier-jest-decyzja-komisji-europejskiej-7103976839564032a.pdf.

[30] *Measures for the protection of the Union budget: the Court of Justice, sitting as a full Court, dismisses the actions brought by Hungary and Poland against the conditionality mechanism which makes the receipt of financing from the Union budget subject to the respect by the Member States for the principles of the rule of law,* Court of Justice of the European Union, Press Release, No 28/22, Luxembourg, 16 February 2022.

[31] See: *AG Campos Sánchez-Bordona: the actions brought by Hungary and Poland against the regime of conditionality for the protection of the Union budget in the event of breaches of the principles of the rule of law should be dismissed. Advocate General's Opinion in Case C-156/21 and Case C-157/21 Hungary v Parliament and Council; Poland v Parliament and Council*, Court of Justice of the European Union, Press Release No 217/21, Luxembourg, 2 December 2021.

Article 2 TEU, the Charter of Fundamental Rights, the content of the conditionality regulation, and case law from both the CJEU and the European Court of Human Rights (ECHR). The Parliament cited numerous cases indicating a clear risk of serious breaches by these member states of the values on which the EU is founded. The resolution specifically pointed to: the judicial disciplinary system in Poland; attacks on media freedom and journalists; violations of migrants' rights; restrictions on women's rights; discrimination against LGBTIQ persons; threats to freedom of association and assembly. This move by the European Parliament reinforced the legal and political pressure on Hungary and Poland, emphasizing the broad scope of rule-of-law concerns in these countries.[32]

And fourthly, due to violations of the rule of law, the European Commission and the Member States determined that by the end of 2023, three conditions for the disbursement of funds to Poland from the Recovery and Resilience Facility (RRF) (under the Polish National Recovery Plan – KPO) had not been met. Hungary also did not receive these funds.[33]

Conclusions

The Regulation of the European Parliament and the Council (EU, Euratom) 2020/2092 on the general conditionality regime for the protection of the Union budget, subjected to scientific explanation in this article,[34] was, in the author's opinion, an appropriate response to crisis-related violations of the rule of law in member states and, consequently, to violations of the EU's financial interests. This concerned the protection of the EU budget in relation to cohesion policy, the common agricultural policy, and the Recovery and Resilience Facility, which is the main component of the recovery instrument – Next Generation EU. It enabled the European Commission, as well as the European Parliament and the Council of the EU, to monitor the crisis situation in all EU member states, collect relevant data on violations, and take immediate sanctioning and corrective actions.

The research assumptions presented in the article, derived from the provisions of the Regulation of the European Parliament and the Council (EU, Euratom) 2020/2092, lead to several scientific conclusions.

First, the principle of the rule of law has been linked to the principle of conditionality to serve the protection of the European Union's budget and financial

[32] *European Parliament resolution of 10 March 2022 on the rule of law and the consequences of the ECJ ruling (2022/2535(RSP)),* OJ EU C 347, 9.9.2022, pp. 168-171.

[33] Ibidem.

[34] The process of explaining attitudes, behaviors, phenomena, and relationships among variables that are observed and measured during research.

interests. Second, the rule of law, as a fundamental value of the European Union derived from the Treaty on European Union, must be unconditionally respected by all member states. Third, the rule of law, derived from the general principles of EU law, complements the treaty-based regulatory system. Fourth, the Treaty on European Union, to which Poland is a party, provides for the possibility of sanctioning violations of EU principles (including the rule of law) in a member state, which may even result in the suspension of that state's membership rights. Fifth, the Multiannual Financial Framework 2021-2027 and the Next Generation EU recovery instrument have been equipped with effective systemic mechanisms to prevent and sanction violations of the rule of law. And sixth, EU institutions, led by the European Commission, the European Parliament, and the Court of Justice, have developed a new system for monitoring and enforcing the rule of law in member states. The analyzed Regulation of the European Parliament and the Council (EU, Euratom) 2020/2092 is one of the most important elements of this system.

The system linking the rule of law with the principle of conditionality, adopted in the European Union as of January 1, 2021 (the date when the provisions of the Regulation entered into force), could not function effectively and deterrently without the set of sanctions proposed within it. The catalog of these sanctions includes: suspension of payments or the execution of a legal obligation, or termination of its validity; prohibition on incurring new legal obligations; suspension of the disbursement of installments, in whole or in part, or early repayment of loans guaranteed by the EU budget; suspension or reduction of economic benefits under an instrument guaranteed by the EU budget; prohibition on concluding new loan agreements or other instruments guaranteed by the EU budget; suspension of the approval of a program or programs or modification of such suspension; suspension of commitments; limitation of commitments, including through financial corrections or reallocation of funds to other expenditure programs; reduction of advance payments; suspension of payment deadlines; suspension of payments.

The content of the article clearly demonstrates that the European Commission and its President play a key role in the legal and political order of the European Union today. Many tend to forget that this institution can be referred to as the government of the European Union. Its influence and impact cannot be compared to any other international organization or structure. According to Article 17 of the Treaty on the European Union, the European Commission promotes the general interest of the Union and takes appropriate initiatives to this end, including those related to sanctioning violations of the rule of law.

As the "guardian of the treaties," the European Commission ensures the application of the treaties and all regulations and decisions adopted by EU institutions based on them. Importantly, it oversees the implementation of EU law under the constant supervision of the Court of Justice of the European Union, while also holding supervisory and sanctioning powers in this regard (e.g., through complaints submitted to the Commission). It executes the budget and manages the EU's financial programs. The Commission performs coordinating, executive, and managerial functions within the entire integration system, in relation to member states and other EU institutions and bodies. It represents the Union both externally and internally, although it does not hold a monopoly in this area. Most EU legislative acts are adopted solely on the Commission's initiative. Crucially, the European Commission is entirely independent in carrying out its duties. Its members neither seek nor accept instructions from any government, institution, body, or organizational entity.

Bibliography

1. *AG Campos Sánchez-Bordona: the actions brought by Hungary and Poland against the regime of conditionality for the protection of the Union budget in the event of breaches of the principles of the rule of law should be dismissed. Advocate General's Opinion in Case C-156/21 and Case C-157/21 Hungary v Parliament and Council; Poland v Parliament and Council*, Court of Justice of the European Union, Press Release No 217/21, Luxembourg, 2 December 2021.
2. *Annual Rule of Law Cycle*, https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/annual-rule-law-cycle_en..
3. *Budżet UE: Komisji publikuje wytyczne dotyczące mechanizmu warunkowości*. Komunikat prasowy, Bruksela 2 marca 2022.
4. *Communication from the Commission Guidelines on the application of the Regulation (EU, EURATOM) 2020/2092 on a general regime of conditionality for the protection of the Union budget 2022/C123/02*, C(2022) 1382, OJ EU C 123, final Brussels, 2.3.2022.
5. *Communication from the Commission to the European Parliament and the Council. A new EU Framework to strengthen the Rule of Law*, Brussels, 11.3.2014, COM(2014) 158 final.
6. *Communication from the Commission to the European Parliament, the European Council and the Council. Further strengthening the Rule of Law within the Union. State of play and possible next steps*, Brussels, 3.4.2019, COM/2019/163 final.
7. *Consolidated version of the Treaty on European Union*, OJ C 326/13, 26.10.2012.
8. *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 Tables of equivalences*, OJ EU C 202, 7.6.2016.
9. *Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')*, OJ EU L 283, 31.10.2017.
10. *Council Regulation (EU, Euratom) 2020/2093 of 17 December 2020 laying down the multiannual financial framework for the years 2021 to 2027*, OJ EU L 433I, 22.12.2020.

11. *Council Regulation (EU) 2020/2094 of 14 December 2020 establishing a European Union Recovery Instrument to support the recovery in the aftermath of the COVID-19 crisis,* OJ EU L 433I, 22.12.2020.
12. Court of Justice of the European Union. *Judgment of 27 February 2018, Associação Sindical dos Juízes Portugueses v Tribunal de Contas (Case C-64/16). ECLI:EU:C:2018:117. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0064.*
13. Czachór Z., *Sytuacja prawna i polityczna Polski w Unii Europejskiej w obliczu nowego podziału budżetu, w oparciu o stan praworządności w państwach członkowskich,* Analiza przygotowana na zlecenie Biura Senatora Marcina Bosackiego, Poznań 20.11.2020.
14. *European Parliament resolution of 10 March 2022 on the rule of law and the consequences of the ECJ ruling (2022/2535(RSP))*, OJ EU C 347, 9.9.2022.
15. *Komisja Europejska zadecydowała. Blokada pieniędzy dla Węgier*, 16.12.2024, https://www.money.pl/pieniadze/blokada-pieniedzy-dla-wegier-jest-decyzja-komisji-europejskiej-7103976839564032a.pdf.
16. *Measures for the protection of the Union budget: the Court of Justice, sitting as a full Court, dismisses the actions brought by Hungary and Poland against the conditionality mechanism which makes the receipt of financing from the Union budget subject to the respect by the Member States for the principles of the rule of law,* Court of Justice of the European Union, Press Release, No 28/22, Luxembourg, 16 February 2022.
17. *Mechanizmy na rzecz przestrzegania praworządności w Unii Europejskiej*, https://oide.sejm.gov.pl/oide/en/images/files/pigulki/Rule_of_law.pdf.
18. Potorski R., Witkowska M., *Can You Count on Luck Without Buying a Lottery Ticket? Predictions on Obtaining Funds from the National Recovery Plan in Light of the Debate on the Rule of Law in Poland*, "Studia Europejskie – Studies in European Affairs" 2024, no. 4, pages?.
19. *Proposal for a Regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States*, COM/2018/324 final – 2018/0136 (COD).
20. *Protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States. European Parliament legislative resolution of 4 April 2019 on the proposal for a regulation of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States (COM(2018)0324 – C8-0178/2018 – 2018/0136(COD)) P8_TC1-COD(2018)0136 Position of the European Parliament adopted at first reading on 4 April 2019 with a view to the adoption of Regulation (EU) of the European Parliament and of the Council on the protection of the Union's budget in case of generalised deficiencies as regards the rule of law in the Member States*, OJ EU C 116, 31.3.2021.
21. *Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget*, OJ EU, L.2020.433I.1, 22.12.2020.
22. *Special meeting of the European Council (17, 18, 19, 20 and 21 July 2020). Conclusions*, General Secretariat of the Council, EUCO 10/20, European Council, Brussels, 21 July 2020.
23. *Zakończenie procedury z art. 7 Traktatu o UE wobec Polski*, https://www.gov.pl/web/sprawiedliwosc/zakonczenie-procedury-z-art-7-traktatu-o-ue-wobec-polski.

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 303–317

ISSN 2543-6961
e-ISSN 2720-3093

Mira Malczyńska-Biały
ORCID: 0000-0003-3083-800X
University of Rzeszów

Information as an element of consumer safety in the European Union[1]

Informacja jako element bezpieczeństwa konsumentów w Unii Europejskiej

Abstract
The article seeks to present information as a key aspect of consumer safety within the European Union. It examines consumer information safety as an ongoing objective in the consumer policy programmes of both the European Economic Community and the European Union. The concept of protecting consumer information in the European Union was realised through a range of legal and organisational measures, including consumer legislation along with informational and educational initiatives by consumer protection bodies. The necessity to guarantee consumer information safety arose from the significant power imbalance between professionals and consumers. It was essential for buyers to have sufficient knowledge of contract terms, product safety, unfair market practices, and complaint procedures to fully participate in the market.

Keywords: consumer safety, information, consumer, consumer policy, European Union

Abstrakt
Artykuł ma na celu przedstawienie informacji jako elementu bezpieczeństwa konsumentów w Unii Europejskiej. Przeanalizowano w nim bezpieczeństwo konsumentów w zakresie informacji jako celu powtarzanego w programach polityki konsumenckiej w Europejskiej Wspólnocie Gospodarczej oraz Unii Europejskiej. Idea ochrony konsumentów w zakresie informacji w Unii Europejskiej realizowana była poprzez szereg działań prawno-organizacyjnych, tj. tworzone prawodawstwo konsumenckie, jak również, działania informacyjne i edukacyjne podmiotów ochrony konsumentów. Potrzeba zapewnienia konsumentom bezpieczeństwa w zakresie informacji wynikała z dysproporcji, jaka występowała pomiędzy profesjonalistą a konsumentem. Odpowiednia wiedza nabywców w zakresie warunków zawierana umów, bezpieczeństwa produktów, nieuczciwych praktyk rynkowych czy sposobów dochodzenia roszczeń konieczna była do pełnego uczestnictwa w procesie rynkowym

Słowa kluczowe: bezpieczeństwo konsumentów, informacja, konsument, polityka konsumencka, Unia Europejska

[1] The text has been produced with funding from the project "Migrants from Ukraine in the Podkarpackie Voivodeship. Socio-Economic Implications" and funded by the Ministry of Science under the Regional Excellence Initiative programme 2024-2027, No. RID/SP/0011/2024/1.

Introduction

This article aims to present information as an element of consumer safety in European Union consumer policy strategies. The article poses the following research questions: first, is ensuring consumer safety and protection in terms of information the primary objective of EU consumer policy? Second, is consumer information one of the elements necessary to ensure consumer safety?

Security means not only guaranteeing the inviolable survival of a given entity but also its freedom of development.[2] In the context of the consumer purchasing process, security assumes a special significance. Effective consumer policy guarantees the safe use of the benefits of the free market. Consumer policy can be defined as a set of legal and organizational activities undertaken by institutions and non-governmental organizations under consumer policy programs for a given period. These activities aim to protect consumer rights in the areas of health, economic interests, redress, information, education, and organizing.[3]

The need to protect consumer information arose from the gap between professionals and consumers. For consumers to fully participate in the market, it was vital to have a comprehensive understanding of contract terms, product safety, unfair market practices, and ways to claim their rights. While companies generally had extensive knowledge in these areas, consumers often only had limited and scattered information, which constitutes a key aspect of consumer policy. The aim was to increase consumer awareness, prevent irrational and mistaken purchases, and defend consumer rights. Well-informed buyers who knew their rights and could assert them—either on their own or with the help of specialised institutions—became partners to producers and sellers, which encouraged compliance with good commercial practices and ethical business principles.[4]

In addressing the problem, we drew on research methods and techniques significant in the field of social sciences. Primarily dogmatic analysis was used to analyse legal acts regulating the discussed issues. The article also utilises a comparative method to compare specific information security measures across successive consumer policy programmes of the European Economic Community and the European Union.

[2] P. Majer, *W poszukiwaniu uniwersalne definicji bezpieczeństwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, no. 7, p. 11.

[3] M. Malczyńska-Biały, *Consumer protection in the chosen system of human rights*, „Polityka i Społeczeństwo" 2018, no. 4, pp. 104-114.

[4] M. Malczyńska-Biały, *Education and information in consumer policy in the Republic of Poland*, „Środkowoeuropejskie Studia Polityczne" 2019, no. 2, pp. 47- 63.

1. Information security in consumer policy programmes of the European Economic Community

The need to guarantee consumers information security was present in the consumer policy of the European Economic Community.

The concept of consumer information security was developed in legal acts in the form of consumer policy programs and implemented through a range of legal and organisational activities, including consumer legislation, as well as informational and educational activities of consumer protection entities.

The 1975 Consumer Protection and Information Policy Annex[5] outlined consumers' right to information. Article 34 of the Annex stipulated that consumers were to be provided with adequate access to information on goods and services, the necessary knowledge to understand their basic characteristics (the type, quality, quantity, and price[6]). It enabled making rational choices between competing goods and services. The secondary intention of the regulation was to facilitate safe and satisfactory use of selected goods and services. Therefore, the legislation at the time, for instance the Directive on the harmonization of the laws of the Member States relating to labelling, presentation, and advertising of foodstuffs intended for sale to an individual consumer,[7] regulated several detailed, very strictly observed obligations for businesses related to labelling products with appropriate information. Educated consumers with comprehensive knowledge would be confident of their rights and thus would seek compensation for any harm or damage resulting from the use of goods or services.[8]

The Second Consumer Policy Program of 1981[9] reiterated consumer rights to information in point 2 of the annex. Point 3 added a specific consumer right to the catalogue, i.e. protection in goods and services. This right was related, among other things, to the provision of comprehensive information, particularly those placed on labels.[10] It primarily concentrated on the prices of goods and services, information about the quality and the names of specific goods,[11] as well

[5] Council Resolution of 14 April 1975 on a preliminary program of the European Economic Community for a consumer protection and information policy, O.J. C 92, 25/04/1975.

[6] In Community legislation these issues are regulated by: Council Directive 79/581/EEC of 19 June 1979 on consumer protection in the indication of the process of foodstuffs, O.J. EC L 16/19, 26/06/1979.

[7] Council Directive 79/112/EEC of 18 December 1978 on the approximation of the laws of the Member States relating to the labeling, presentation, and advertising of foodstuffs for sale to the ultimate consumer, O.J. EC L 33/1, 08/02/1979.

[8] K. G. Grunert, *The consumer Information Deficit: Assessment and Policy Implications*, "Journal of Consumer Policy" 1984, no.3, pp. 362-364.

[9] Council Resolution of 19 May 1981 on a second program of the European Economic Community for a consumer protection and information policy, O.J. C 133, 3/06/1981.

[10] "Bulletin of the European Communities" 1981, no. 5, p. 25.

[11] "Bulletin of the European Communities " 1983, no. 10, p. 37.

as misleading information about products. An important element of the right to information was the protection from unfair advertising, which aimed to prevent consumers from making decisions that were unfavourable to them and based on false premises. Misleading advertising constituted an act of unfair competition.[12] Counteracting misleading or false information in advertising was reflected in Directive 84/450/EEC.[13] When determining whether an advertisement was misleading, a few factors were considered, i.e. the information concerning the characteristics of the goods or services contained therein, such as, the price, type, properties, and rights of the advertiser.[14]

A summary of activities related to the implementation of existing consumer protection programs was included in the Communication from the European Commission to the Council of the European Communities on a new impetus for consumer protection policy of 27 June 1985.[15] According to point 18 of the Communication, the Community should focus on achieving three fundamental objectives. The second of these concerned the right to benefit from the free market, to be achieved, among other things, by standardizing knowledge on goods and their prices in all EU Member States.[16] The notification was given through advertising on satellite television. The development of new technology used to provide data to consumers in the form of computer databases was also mentioned.

The Commission continued to work on improving the quality of information consumers receive about price differences that could occur in the case of identical goods. For this reason, several studies were conducted, either in cross-border regions or in individual Member States.[17]

The three-year action plan on consumer policy of the European Economic Community of 3 May 1990[18] focused in its "B" part, among other things, on the right to information. According to point 2, the right to consumer information concerned increasing their confidence in the benefits of a single market through making appropriate information about products and services more available. The idea had many aspects. It encompassed information services, understandable

[12] B. Lipińska, *Dyrektywa Rady Wspólnot Europejskiej nr 84/150/EEC, w sprawie zbliżania ustaw, rozporządzeń i przepisów administracyjnych państw członkowskich w zakresie reklamy wprowadzającej w błąd*, „Biuletyn Urzędu Antymonopolowego" 1994, no. 3, pp. 5-6.

[13] Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising, O.J. L 250, 19/09/1984.

[14] Ibidem, article 3.

[15] A New Impetus for Consumer Protection Policy. Communication from the Commission to the Council, COM (85) 314, 27/06/1985.

[16] Council Directive 88/314/EEC of 7 June 1988 on consumer protection in the indication of the process of non-food products, OJ EC L. 142/19, 09/06/1988.

[17] Bulletin of the European Communities 1986, no. 9, p. 62.

[18] Three years action plan of consumer policy in the EEC (1990-1992). COM (90) 98 final, 3/05/1990.

information and comparative testing, and information contained in advertising.[19] The services were to ensure appropriate data flows that would meet consumer needs. It depended on developing information standards among economic and social entities, including entrepreneurs, and both consumer and professional advisory organizations. Information about sales promotions was not a sufficient basis for making purchasing decisions. Consumers needed access to information and advice throughout the entire transaction process. Council Directive 90/496 of the European Economic Community of 24 September 1990[20] aimed at introducing uniform rules for including nutritional information on foodstuffs in all Member States, allowing for the elimination of technical barriers to trade.

Transparency in consumer information rights was linked to the need to strive for the highest possible level of clarity of information. This was particularly important for the maximum directness regarding the presentation and delivery of goods and services. Many of the regulations in force, at the time, governing market transactions did not provide clear information for consumers. Therefore, it was deemed necessary to establish uniform requirements across all market sectors, with particular emphasis on food products. It should also be recognized that transparency requirements were changing and evolving. Therefore, there was an urgency for reviewing existing standards in terms of rationalising them and ensuring that new regulations addressed the issue. The program provided a detailed analysis of the development of product labelling legislation. The goal was to eliminate misunderstandings and meet anticipated consumer demands. The necessity to develop appropriate symbols regarding production quality was also highlighted.[21] Information transparency also concerned the adoption of legislative measures to facilitate consumer choice when making cross-border payments and financial transfers.[22] It was essential to consequently implement and adapt Directive 79/112 on food labelling to consumer needs.[23] This was to be achieved by increasing the amount of relevant consumer information by providing comparative tests, that would influence consumer choices, by facilitating price and quality comparison on the internal market, including, the credibility of advertised products.[24]

[19] V. Kendall, *EC Consumer Law,* , London-New York-Chichester 1994, pp. 163-178.
[20] Council Directive 90/496 EEC of 24 September 1990 on nutrition labeling for foodstuffs, O.J. EC L 276/40, 06/10/1990.
[21] Ibidem, point 2b.
[22] *25th General Report on the Activities of the European Communities 1991,* Brussels-Luxembourg 1992, p. 214.
[23] Council Directive 79/112/EEC of 18 December 1978 on the approximation of the laws of the Member States relating to the labeling, presentation, and advertising of foodstuffs for sale to the ultimate consumer, OJ EC L 33, 8/02/1979.
[24] Council Directive 84/450/EEC… op. cit.

2. Information security in the European Union's consumer policy programmes

The idea of information security was further developed in the Council Resolution of 13 July 1992 on future priorities for the development of consumer protection policy.[25] The Resolution emphasized that the information in the single market should serve to safeguard the interests and rights of consumers by providing better education on services, which was to be granted by establishing cross-border centres and improving the pricing of consumer goods and services. What was also accented was the need to expand consumer knowledge on product recycling programs, the rational use of natural mineral resources, and of ecological packaging.

The second three-year consumer policy program[26] implemented the concept aiming at improving consumer protection and raising awareness of their rights. This prioritized developing and strengthening consumer information. On October 26, 1992, the report "The Internal Market after 1992: Meeting the Challenge" was presented to the Commission.[27] It contained a list of recommendations intended to address consumer ignorance. The report emphasized the need to develop an information strategy and highlight the issue of access to justice. In general, freedom of choice could not be effective if market conditions were unclear and if available information was not disseminated.[28]

Consumer information security ensured the inclusion of truthful information in contracts concluded with consumers.[29] The Commission also took steps to ensure that reliable information is given on labels. The program attempted to achieve consensus on the required labels and ensure the widest possible range of solutions. It was also essential to strengthen information enabling consumers to choose products in an informed manner regarding their potential environmental impact. The Commission supported price reviews, which constituted an invaluable source of information. Comparative tests also demonstrated their beneficial impact on consumer responsibility. At the Community level the instructions were developed and disseminated by the Commission to consumer organizations and institutions, information centres, and the media.[30]

[25] Council Resolution of 13 July 1992 on future priorities for the development of consumer protection Policy, Journal of Laws O.J. EC C186, 23/07/1992.
[26] Second Commission three-year consumer policy action plan 1993-1995, KOM (93) 378, 28/07/1993.
[27] The text of the report is available on the University of Pittsburgh website, http://aei.pitt.edu/1025/ , [date of access: 21.05.2024].
[28] Council Resolution 93/C 110/01, O.J.C 110/1, 20/04/1993.
[29] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contractsL 95, 21/04/1993.
[30] 27th General Report on the Activities of the European Communities 1993, Brussels and Luxembourg 1994, p. 135.

The next consumer policy program for 1996-1998[31] concentrated on the idea of information security. Improving and developing consumer information was linked to counteracting the spread of inappropriate information about goods and misleading information about their prices.[32] When presented with accurate information, consumers would make rational choices, without being misguided and thus protected appropriately. The practical development of information services would facilitate the elimination of consumer problems. It was found that erroneous information on products challenged the process of selecting the right product from among the goods and services available.[33]

The demand to develop information security continued in the Consumer Policy Action Plan for 1999-2001.[34] It was achieved, among other things, by ensuring adequate and reliable consumer information. A key element of this action was focusing on a single priority topic, greater involvement of consumer organizations in information issues, and the creation of national information offices.[35]

Under Article 12 of Directive 2001/95/EC[36], a Community Rapid Alert System, regarding measures and actions taken in relation to products posing a serious risk to consumer health and safety, was developed for the swift exchange of data between Member States and the Commission. The RAPEX system helped prevent introduction of products posing a serious risk to consumer health and safety into the European market. It facilitated monitoring of the effectiveness and consistency of market surveillance, and the enforcement activities in Member States. It also provided a basis for identifying the urge for action at Community level, helping, at the same time, to ensure steady application of EU product safety requirements and a smooth functioning of the internal market. The detailed scope of the system is included in Annex II to the directive under review.[37]

Providing information to consumers in the European Union related to establishing legal regulations promoting consumer protection in the field of information. This concerned the right to information, with the intention of providing consumers with free, independent choices and guarantees of safety. We can essentially

[31] Communication from the Commission – priorities for consumer policy 1996-1998, COM (95)519, 31/10/1991.

[32] Directive 98/6/EC of the European Parliament and of the Council of 7 June 1998 on consumer protection in the indication of the prices of products offered to consumers, O.J. EC *L 080, 18/03/1998.*

[33] Pt. 1 Communication from the Commission – priorities for consumer policy 1996-1998... op. cit.

[34] Communication from the Commission. Consumer Policy Action Plan 1999-2001, COM (98), 14/01/1998.

[35] Pt 3.4 Communication from the Commission. Consumer Policy Action Plan 1999-2001… op. cit.

[36] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, O.J. L 11, 15.1.2002.

[37] Annex II Procedures for the application of the RAPEX system and guidelines for notifications to Directive 2001/95/EC…., op. cit.

distinguish two types of information that consumers could expect: product information and information about the terms and conditions of consumer contracts. Product information can be defined as the principle that every product intended for consumers should be accompanied with information regarding its characteristics, intended use, and a manual. Consequently, EU legislation developed a series of detailed, very strictly observed labelling obligations, including both requirements for properly provided information, and prohibitions concerning specific content.[38]

The obligation to provide information on the terms and conditions of the concluded contract, its subject and the subject of the service, as well as its effects in a true, factual and complete manner, while maintaining a specific form, for example in writing, was considered a general feature of contract law and resulted from the obligation of loyal contracting.[39]

The successful implementation of the rules concerning consumer information security involved performing information activities on product safety, which focused on eliminating unfair practices used against consumers. Application of these objectives was further specified in the provisions of Directive 2005/29/EC.[40] The issue of misguiding information was regulated by Article 6 of the act, stipulating that a commercial practice was considered misleading if it contained false information and was therefore untrue, or in any way misled or was likely to mislead the average consumer. A practice was also unfair if the information was factually incorrect in one or more respects, and caused or was likely to cause the consumer to make a transactional decision they would not have made otherwise. The practices were associated with factors such as the sole existence or type of the product, the main characteristics of the product, the scope of the trader's responsibilities, the price, necessary services, type, characteristics and rights of the trader or their representative, and consumer rights. A commercial practice was considered misleading if, in a specific case, considering all its features and circumstances, it caused or was likely to cause the average consumer to take a transactional decision that they would not have made otherwise. This included, among other things, misleading information in the form of comparative advertising that created confusion between the products, the trademarks, the trade names, or other distinguishing marks of the trader and its competitor.

[38] A. Streżyńska, *Ochrona konsumentów w Unii Europejskiej i Polsce,* Warszawa 2000, p. 98.

[39] S. Grzybowski, *System prawa cywilnego*, *vol. I, Część ogólna*, Wrocław 1974, p. 550.

[40] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, O.J. L 149, 11.6.2005.

Under Article 7, a commercial practice was also considered misguiding if, in a specific case, considering all its features and circumstances and the limitations of the communication medium, it omitted material information necessary for the average consumer. Thus, it caused or was likely to cause the average consumer to take a transactional decision that they would not have made if it had not been for the practice. An omission when a trader concealed or provided material product information in an unclear, incomprehensible, ambiguous, or untimely manner, was also treated as a misleading practice. Additionally, the list included situations when the trader failed to disclose the commercial purpose of the practice if it was not clear from the context.[41]

In 2006, the issue of unfair information in the form of misleading and comparative advertising was regulated in accordance with the concept.[42] According to Article 2 of the Directive of 12 December 2006,[43] misleading advertising was any advertising that, in any way, including its form, misled or was likely to mislead the persons to whom it was addressed, and one that, because of its deceptive nature, was likely to influence their economic conduct, or for these reasons, harmed or was likely to harm a competitor. Comparative advertising, on the other hand, meant any advertising that explicitly or by implication identified a competitor or goods or services offered by a competitor.[44]

Proper regulation of labelling of certain product categories was intended to eliminate unfair information practices.[45] The directions in this regard were outlined, among others, in the Council Resolution of 1 March 2002.[46]

Between 2002 and 2006, providing consumer information concentrated on creating and implementing legal regulations aimed at protecting consumers by ensuring that the prices of offered products are indicated properly.[47] All Member States adopted national legislation transposing Directive 98/6/EC on consumer protection in the indication of prices of products offered to consumers. The main

[41] Article 7 Directive 2005/29/EC... op. cit.

[42] "Bulletin of the European Union" 2006, no. 5, p. 75.

[43] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising, O.J. L 376, 27/12/2006.

[44] "Bulletin of the European Union" 2006, no. 10, pp. 87-88; "Bulletin of the European Union" 2006, no. 11, pp. 82-83.

[45] "Bulletin of the European Union" 2002, no. 1/2, pp.105-106, "Bulletin of the European Union" 2005, no. 5, pp. 40-41.

[46] Council Resolution of 1 March 2002 on the protection of consumers, in particular young people, through the labeling of certain video games and computer games according to age groups, C 65/2, 14.3.2002.

[47] Communication from the Commission to the Council and the European Parliament on the implementation of Directive 1998/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of prices of products offered to consumers, COM (2006) 325, 21/06/2006, "Bulletin of the European Union" 2006, no. 6, pp. 102-103.

objective of this directive was to guarantee that the economic operators display the selling price and the price per unit of measurement (unit price) for all products offered to consumers to fully inform consumers and make price comparisons easier. The selling price had to be unambiguous, easily visible, and legible.[48]

Introducing data on the packaging of specific product categories was yet another element of providing consumer safety.[49] According to Article 11, for the safe use of toys, appropriate warnings were required to indicate restrictions on their use. Specific warnings were not to be displayed on toys if they were inconsistent with the intended use based on their function, size, and characteristics. Manufacturers were to display warnings in a clearly visible, easily legible, understandable, and accurate manner.[50]

From 2007 to 2013, consumer information security was driven by the development of the RAPEX rapid alert system for non-food products. In October 2012, „Global Recalls" portal was launched,[51] extending the reach of the RAPEX system beyond the European Union. It allowed global exchange of information on dangerous products withdrawn from the market. The project was developed jointly by the member states of the European Union and the Organisation for Economic Co-operation and Development, including Australia, Canada, and the United States.[52] During the reviewed period, the principles, requirements, and responsibilities for food information, and in particular food labelling, were regulated by the Regulation of the European Parliament and of the Council of 25 October 2011.[53]

In accordance with the Consumer Policy strategy[54] the marking and labelling of selected product categories were regulated between 2007 and 2013. The Regulation of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance played a particular role in this regard. Article 7 imposed information reporting obligations on each

[48] Directive 98/6/EC of the European Union Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers, O.J. L 80, 18/03/1998.

[49] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys, O.J. L 170, 30/06/2009.

[50] "Bulletin of the European Union" 2008, no. 9, p. 93.

[51] https://globalrecalls.oecd.org [date of access: 1.06.2025].

[52] *General report on the activities of the European Union 2012,* Brussels-Luxembourg 2013, p. 120.

[53] Regulation (EU) No 1169/2011 of the European Parliament and of the Council of 25 October 2011 on the provision of food information to consumers, amending Regulations (EC) No 1924/2006 and (EC) No 1925/2006 of the European Parliament and of the Council, and repealing Commission Directive 87/250/EEC, Council Directive 90/496/EEC, Commission Directive 1999/10/EC, Directive 2000/13/EC of the European Parliament and of the Council , Commission Directives 2002/67/EC and 2008/5/EC and Commission Regulation (EC) No 608/2004, O.J. L 304, 22/11/2011.

[54] Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee - EU Consumer Policy strategy 2007-2013 - Empowering consumers, enhancing their welfare, effectively protecting breath, COM(2007) 99, 13.3.2007.

national accreditation body, which informed other national accreditation bodies about the conformity assessment activities performed in the accreditation process and about any changes in this regard[55].

In 2014-2020[56] providing information to consumers focused on creating and improving the availability of a universal information base on consumer product safety. The transparency of markets and consumer information was also increased. The RAPEX system served as an information base for dangerous non-food products. Year after year, the system recorded an increase in published product information.[57] Market transparency and consumer information were enhanced and reinforced by developing consumer legislation. In early January 2019, Directive 2019/2161 on the better enforcement and modernization of EU consumer protection rules reached the statute book.[58] The new ruling enabled changes to consumer regulations, particularly those related to increased transparency in online marketing and sales activities.[59]

The adoption of selected laws aimed at improving information, as defined in the directive on better enforcement and modernization of EU consumer protection rules, contributed to increasing market transparency and consumer information.[60] The directive connected consumer rights to new technologies by introducing important requirements related to online transactions and digital services, and prohibited, for example, hidden advertising in browser search results and "fake" consumer reviews. It also introduced a requirement concerning consumers being informed about the identity of digital platform partners (whether individuals or professional retailers), the parameters determining result rankings, and the personalization of prices through automated decision-making.[61]

The current trends in consumer information security are outlined in the Consumer Program for 2020-2025.[62] Due to the epidemiological situation,

[55] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, O.J. L 218, 13/08/2008.

[56] Regulation (EU) No 254/2014 of the European Parliament and of the Council of 26 February 2014 on a multiannual consumer program for the years 2014-20 and repealing Decision No. 1926/2006/EC, O.J. L 84, 20/03/2014.

[57] *General report on the activities of the European Union in 2016,* Brussels-Luxembourg 2017, p. 67.

[58] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules, O.J. L 328, 18.12.2019.

[59] *General report on the activities of the European Union in 2018,* Brussels-Luxembourg 2019, p. 102.

[60] Directive (EU) 2019/2161... op. cit.

[61] *General report on the activities of the European Union in 2018...,* op. cit., p. 95.

[62] Communication from the Commission to the European Parliament and the Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery, COM(2020)696, 13/11/2020.

the program aims to counteract the impact of COVID-19 on consumer rights. This includes fraud, travel-related issues, exploiting financial instability, misleading information about products and services, and unfair commercial practices (in particular, online influence techniques and personalization).[63]

The Commission plans to finance the project creating "EU e-Lab", a platform that could be used by authorities to conduct online investigations and monitor dangerous products purchased online. Facilitating individual redress will remain a priority. There is also a plan to continue EU funding and modernization of European Consumer Centres, alternative dispute resolution (ADR), and online dispute resolution tools.[64]

Conclusion

The idea of developing consumer information was already present in the consumer policy of the European Economic Community. In 1993, with the Treaty on European Union becoming effective, consumer policy gained a new dimension, growing into one of the Community's strategic objectives.

The need to guarantee consumer information security was present in the consumer policy of the European Economic Community and continued in the European Union. Essentially, it protected consumers against their ignorance and inexperience. Its primary purpose was to welcome diverse consumer attitudes into informed decision-making and the selection of goods and services. It also involved creating an appropriate legal environment. It involved the creation of legal regulations containing guidelines for consumer information provided by sellers and entrepreneurs (on packaging, labels, and in advertising).

Based on the analyses conducted in the article, the research questions were answered. It was confirmed that ensuring consumer safety and protection in terms of information is an overriding objective in subsequent European Union consumer policy strategies and programmes. It is implemented through a series of measures during specific periods of consumer strategy validity. Consumer information is also one of the elements necessary to ensure consumer safety.

[63] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules, O.J. L 328, 18.12.2019.

[64] Regulation (EU) 2021/240 of the European Parliament and of the Council of 10 February 2021 establishing a Technical Support Instrument, O.J. L 57, 18/02/2021.

Bibliography

1. A New Impetus for Consumer Protection Policy. Communication from the Commission to the Council, COM (85) 314, 27.06. 1985.
2. „Bulletin of the European Communities" 1981, no. 5, p. 25.
3. „Bulletin of the European Communities" 1983, no. 10, p. 37.
4. „Bulletin of the European Union" 2006, no. 5, p. 75.
5. „Bulletin of the European Union" 2006, no. 10, pp. 87-88.
6. „Bulletin of the European Union" 2006, no. 11, pp. 82-83.
7. „Bulletin of the European Union" 2002, no. 1/2, pp. 105-106.
8. „Bulletin of the European Union" 2005 no. 5, p. 40-41.
9. Communication from the Commission – priorities for consumer Policy 1996-1998, COM (95)519, 31.10.1991.
10. Communication from the Commission. Consumer Policy Action Plan 1999-2001, COM (98), 14.01.1998.
11. Communication from the Commission to the Council and the European Parliament on the implementation of Directive 1998/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of prices of products offered to consumers, COM (2006) 325, 21.6.2006. „Bulletin of the European Union" 2006 no. 6, p. 102-103.
12. Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee - EU Consumer Policy strategy 2007-2013 - Empowering consumers, enhancing their welfare, effectively protecting them, COM(2007) 99, 13.3.2007.
13. Communication from the Commission to the European Parliament and the Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery, COM(2020)696, 13.11.2020.
14. Council Resolution of 14 April 1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy, O.J. C 92, 25.4.1975.
15. Council Directive 79/581/EEC of 19 June 1979 on consumer protection in the indication of the process of foodstuffs, O. J. EC L 16/19, 26.06.1979.
16. Council Directive 79/112/EEC of 18 December 1978 on the approximation of the laws of the Member States relating to the labeling, presentation and advertising of foodstuffs for sale to the ultimate consumer, O.J. EC L 33/1, 08.02.1979.
17. Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising, O.J. L 250, 19.9.1984.
18. Council Directive 88/314/EEC of 7 June 1988 on consumer protection in the indication of the process of non-food products, O.J. EC L. 142/19, 09.06.1988.
19. Council Directive 90/496 EEC of 24 September 1990 on nutrition labeling for foodstuffs, O.J. EC L 276/40, 06.10.1990.
20. Council Directive 79/112/EEC of 18 December 1978 on the approximation of the laws of the Member States relating to the labeling, presentation and advertising of foodstuffs for sale to the ultimate consumer, O. J. EC L 33, 8.02.1979.
21. Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts
22. O.J. L 95, 21.4.1993.
23. Council Resolution 93/C 110/01, O.J. C. 110/1, 20.04.1993.

24. Council Resolution of 1 March 2002 on the protection of consumers, in particular young people, through the labelling of certain video games and computer games according to age groups, C 65/2, 14.3.2002.
25. Directive 98/6/EC of the European Parliament and of the Council of 7 June 1998 on consumer protection in the indication of the prices of products offered to consumers, O.J. EC L 080, 18.03.1998.001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, O.J. L 11, 15.1.2002.
26. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, O.J. L 149, 11.6.2005.
27. Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising, O.J. L 376, 27.12.2006.
28. Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers, O.J. L 80, 18.3.1998.
29. Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, O.J. L 328, 18.12.2019.
30. Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, O.J. L 328, 18.12.2019.
31. *General report on the activities of the European Union 2012*, Brussels-Luxembourg 2013, p. 120.
32. *General report on the activities of the European Union in 2016*, Brussels-Luxembourg, 2017, p. 67.
33. *General report on the activities of the European Union in 2018*, Brussels-Luxembourg 2019, p. 102.
34. Grunert K. G., *The consumer Information Deficit: Assessment and Policy Implications*, „Journal of Consumer Policy" 1984, no. 3, p. 362-364.
35. Grzybowski S., *System prawa cywilnego*, *t. I, Część ogólna*, Wrocław 1974.
36. http://aei.pitt.edu/1025/
37. https://globalrecalls.oecd.org
38. Kendall V., *EC Consumer Law*, London-New York-Chichester 1994.
39. Majer P., *W poszukiwaniu uniwersalne definicji bezpieczeństwa,* „Przegląd Bezpieczeństwa Wewnętrznego" 2012, no.7, p. 11.
40. Malczyńska-Biały M., *Consumer protection in chosen system of human rights*, „Polityka i Społeczeństwo" 2018, no. 4, pp.104-114.
41. Malczyńska-Biały M., *Education and information in consumer policy in the Republic of Poland*, „Środkowoeuropejskie Studia Polityczne" 2019, no. 2, pp. 47-63.

42. Regulation (EU) No 1169/2011 of the European Parliament and of the Council of 25 October 2011 on the provision of food information to consumers, amending Regulations (EC) No 1924/2006 and (EC) No 1925/2006 of the European Parliament and of the Council, and repealing Commission Directive 87/250/EEC, Council Directive 90/496/EEC, Commission Directive 1999/10/EC, Directive 2000/13/EC of the European Parliament and of the Council, Commission Directives 2002/67/EC and 2008/5/EC and Commission Regulation (EC) No 608/2004, O.J. L 304, 22.11.2011.
43. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, O.J. L 218, 13.8.2008.
44. Regulation (EU) No 254/2014 of the European Parliament and of the Council of 26 February 2014 on a multiannual consumer programme for the years 2014-20 and repealing Decision No 1926/2006/EC, O.J. L 84, 20.3.2014.
45. Regulation (EU) 2021/240 of the European Parliament and of the Council of 10 February 2021 establishing a Technical Support Instrument, O.J. L 57, 18.2.2021.
46. Second Commission three-year consumer policy action plan 1993-1995, KOM (93) 378, 28.07.1993.
47. Strężyńska A., *Ochrona konsumentów w Unii Europejskiej i Polsce,* Warszawa 2000.
48. Three-year action plan of consumer policy in the EEC (1990-1992). COM (90) 98 final, 3.05.1990.
49. *XXVth General Report on the Activities of the European Communities 1991,* Brussels-Luxembourg 1992, p. 214.
50. *XXVIIth General Report on the Activities of the European Communities 1993*, Brussels-Luxembourg 1994, p. 135.

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 319–329

ISSN 2543-6961
e-ISSN 2720-3093

Martyna Kaczmarczyk
ORCID: 0000-0001-6169-9466
Uniwersytet Warmińsko-Mazurski w Olsztynie

Selected security, ethical and moral issues related to the use of artificial intelligence – in the perspective of new European legal regulations

Wybrane zagadnienia bezpieczeństwa, etyki i moralności związane z wykorzystaniem sztucznej inteligencji – w perspektywie nowych europejskich regulacji prawnych

Abstract
The article analyzes new European regulations on artificial intelligence in the context of values such as safety, ethics, and morality, assessing whether these frameworks adequately protect them. It examines Regulation (EU) 2024/1689 establishing harmonised AI rules and the 2024 Council of Europe Framework Convention on AI, human rights, democracy, and the rule of law. These instruments are presented as a milestone in defining legal boundaries, principles, and liability for the use of AI systems. The article discusses key features of AI systems, regulatory challenges, and potential legal consequences related to the protected values. It highlights selected issues relevant in a period of rapid technological advancement and frames them as a basis for further scientific and social debate.

Keywords: artificial intelligence, European Union law, security, human rights, ethics, morality

Abstrakt
Artykuł analizuje nowe europejskie regulacje dotyczące sztucznej inteligencji w kontekście bezpieczeństwa, etyki i moralności, oceniając, czy zapewniają one odpowiednią ochronę tych wartości. Omówiono Rozporządzenie (UE) 2024/1689 ustanawiające zharmonizowane przepisy dla systemów SI oraz Konwencję Ramową Rady Europy z 2024 r. dotyczącą SI, praw człowieka, demokracji i praworządności. Wskazano, że regulacje te są kluczowe dla wyznaczenia granic prawnych i zasad odpowiedzialności związanej ze stosowaniem SI. Przedstawiono charakterystykę systemów SI, wyzwania dla ustawodawcy oraz potencjalne konsekwencje prawne w odniesieniu do wskazanych wartości. Artykuł podkreśla wybrane zagadnienia istotne w warunkach szybkiego rozwoju technologii oraz stanowi punkt wyjścia do dalszej dyskusji naukowej i społecznej.

Słowa kluczowe: sztuczna inteligencja, prawo Unii Europejskiej, bezpieczeństwo, prawa człowieka, etyka, moralność

Introduction

Artificial intelligence is a phenomenon that has already become a part of our reality. It is nothing new, as it has been operating in various areas of human life for many years. The term has been around since the 1950s, and has flourished since the 1980s. However, the most intensive development of artificial intelligence is currently underway. At present, it cannot be stated that new technologies do not exhibit the characteristics of intelligence. They are at such a high level of advancement that they often exceed human capabilities in their analysis, calculation, and prediction skills. That is why they are used wherever error-free operation and work under time pressure are necessary. The main ideas of AI are reasoning, knowledge, planning, learning, natural language processing (e.g. reasoning, speaking), perception and the ability to move. There are three types of artificial intelligence. First, there is narrow AI, whose abilities are limited to performing specific tasks, for example it can be used in wide technology to create voice assistants. Second, we have general AI, which is capable of performing any tasks that a human could take, for example it is able to learn, solve problems and also plan. The last, third type, is superintelligence, which is intellectually superior to any human being.[1]

Most studies show artificial intelligence as the research of agents. Software and machines have a set of options to choose from and fulfil specific goals. A closely related concept is machine learning, which is related to abilities for software to reason on previous experience. This should enable answering questions about previously collected data and also about its new information. Machine learning helps to classify and regress, so it firstly recognizes classes from a lot of data and then predict one outcome from another.[2] Machine learning is the basis of artificial intelligence. Deep learning, on the other hand, is a category of machine learning. This phenomenon involves creating an algorithm inspired by the human mind, learning from a large amount of data, which is then used to create, for example, paintings or music. Constructed neural networks allow learning without human supervision.[3]

Scientific research on artificial intelligence can be divided into two types, mainly due to the motivation that accompanies it. The first is the psychological-philosophical motivation, which aims to build machines that operate on the model of the human mind. This may be due to various reasons, e.g. to improve, legitimize human work, support certain processes, such as AI in medicine. The

[1] A. Konieczna, *Problematyka sztucznej inteligencji w świetle prawa autorskiego*, "Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2019, no. 4, pp. 104-105.

[2] M. Maternowska, *Nowe technologie i ich wpływ na łańcuchy dostaw. Sztuczna inteligencja,* "Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2019, no. 388, p. 62.

[3] A. Konieczna, op. cit., s. 62-63.

second type of motivation is engineering, which aims to create autonomous systems that would replace humans in demanding tasks and, what's more, would work better than humans.[4]

Due to its great complexity, artificial intelligence needs a thorough and adapted legal framework to protect values such as human rights, security, morality, and ethics. Year 2024 brought expected regulations that had been developing for many years in the European system. Artificial intelligence is developing very quickly on a global scale and has a strong impact on societies, markets, and economies. Europe, in the global context, is a highly advanced region in artificial intelligence research, not only technologically, but also in the legislative aspect of creating legal norms.[5] The analysis of these regulations was carried out in terms of the above-mentioned values. This will be presented in the following sections in the article.

1. Legislation

In terms of the international approach to ensuring legal protection of human rights and freedoms, transparency of procedures and principles for implementing artificial intelligence systems, taking responsibility for negative effects that may occur in connection with activities of AI, work was undertaken almost simultaneously in the European Union and the Council of Europe to establish expert committees, bodies and comprehensive legal studies in the field of artificial intelligence.[6]

In May 2024, the European Commission completed procedure for adopting new EU regulations, culminating in the signing of Regulation 2024/1689 of 13 June 2024 on the establishment of harmonised rules on artificial intelligence (so-called AI Act).[7] The document entered into force on 1 August 2024, but will be fully applicable in 2 years. The new EU regulation on AI systems is based on risk analysis divided into unacceptable risk, high risk and low or minimal risk.

Obligations imposed on AI providers and users depend on the risk assessment. Regulation precisely specifies which practices within the scope of AI systems are prohibited practices due to their conflict with fundamental principles

[4] P. Wawrzyński, *Podstawy sztucznej inteligencji*, Warszawa 2019, p. 10.

[5] A. M. Świątkowski, *Warunki rozwoju i wpływ sztucznej inteligencji na pracę, zatrudnienie, i inne niektóre prawnie nieuregulowane w Unii Europejskiej zagadnienia społeczne, technologiczne i gospodarcze,* "Roczniki Administracji i Prawa" 2021, vol. XXI, p. 114 et seq.

[6] J. Mazur, *Unia Europejska wobec rozwoju sztucznej inteligencji: proponowane strategie regulacyjnea budowanie jednolitego rynku cyfrowego*, "Europejski Przegląd Sądowy" 2020, no. 4, p. 13 et seq.

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

and rights of the Union. They include, among others, AI-based activities related to propaganda, exploiting the weakness of natural persons, analyzing the emotions of an individual, introducing the categorization of data, including biometric data. In addition, a statutory dictionary has been established, which contains legal definitions of as many as 68 concepts, including artificial intelligence, risk, provider, individual types of data and systems relevant from the point of view of AI technology. Regulation introduces guiding principles for AI systems. First of them is the rule of human supervision over high-risk AI systems. This means that a human being always supervises such systems, thereby preventing or minimising risks to health, safety and fundamental rights.

In addition, the issue of designing a high-risk system is important in this case, as it requires the use of appropriate human-machine interface tools. Another guiding principle of AI systems is the rule of transparency and making information available to entities using them. The third, equally important principle expresses the obligation of accuracy, robustness and cybersecurity in the design and development of artificial intelligence systems. In addition, obligations of suppliers of artificial intelligence systems have also been defined, consisting in monitoring and reporting events. The entire AI cycle must be monitored from the moment it is introduced to the market. The supplier is also obliged to report any incidents and irregularities in operation. The EU legislator has imposed on the Member States the obligation to designate national notifying authorities and market surveillance authorities.[8]

Second international legal regime for AI systems will be the Council of Europe Convention on artificial intelligence, which has not yet been adopted. On 5 September 2024, the European Commission, on behalf of the EU, signed a binding international treaty on artificial intelligence, the Framework Convention on artificial intelligence and human rights, democracy and the rule of law.[9] The Council of Europe Convention is based on the values expressed by the European Convention on Human Rights, i.e. most fundamental freedoms and human rights. Generally speaking, proposed provisions concern regulation of fundamental values for artificial intelligence systems, i.e. the basic principles and rules of law. The Convention introduces a legal definition of AI systems and other related terms, but to a limited extent. The main legal rule of the document is the application of provisions of the Convention at every stage of the life cycle of an artificial intelligence system, emphasizing respect for fundamental human rights and the values

[8] M. Kaczmarczyk, *O systemach sztucznej inteligencji w kontekście praw człowieka w orzecznictwie Europejskiego Trybunału Praw Człowieka*, "Studia Prawa Publicznego" 2025, no. 2, p. 11 et seq.

[9] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Vilnius, 5.IX.2024, Council of Europe Treaty Series – No. 225.

of democracy and the rule of law. The CoE Framework Convention, although consistent with provisions of the EU regulation, is relatively concise, not very detailed, and does not address many issues as thoroughly as the EU regulation. An example of a generalized provision is Article 9, which rather enigmatically states that states are obliged to take the necessary measures to protect individual freedom, human dignity and autonomy. However, it is not known what measures are meant. The regulation is imprecise, which allows for a very broad interpretation of what actions on the part of the state are meant.

Similarly, principles relating to the design, development and use of artificial intelligence systems have been presented in a very general manner – counteracting discrimination, equality, safety, are not values dedicated to AI. They have their reference to numerous legal regulations, so again we are dealing with a generalization and a lack of precision. An important issue-difference between the framework convention and the EU regulation, apart from the numerous differences in the level of detail of individual legal issues, is the shaping of the system of liability for violations of human rights and freedoms. This has been regulated completely differently in both documents. Within the framework of the EU regulation, specific obligations related to liability for AI activities have been imposed on natural and legal persons in the role of suppliers. In the framework convention, on the other hand, liability and the obligation to pay compensation rest with the state.[10]

2. Definition

It is necessary to present a definition of artificial intelligence for the sake of order. AI is a dynamically developing field of computer science, but – due to the accumulation of contexts from various scientific disciplines – it is difficult to provide one binding definition. Starting with the name, artificial intelligence aims to reproduce the operation of human intelligence, and in particular the ability to learn. Following John McCarthy, we can say that intelligence itself is defined as "computational ability to achieve goals in the world."[11] Generally, definitions of artificial intelligence focus on the concept of creating computer programs that are capable of performing behaviors that would be considered intelligent if these behaviors were performed by humans.[12] References to human intelligence are necessary, because it has not yet been decided what specific types of computational procedures can be considered intelligence (in isolation from human intelligence).

[10] M. Kaczmarczyk, op. cit., p. 12 et seq.

[11] K. Binkowski, *Sztuczna inteligencja a wykładnia prawa – propozycja zastosowania systemów AI do ustalania założenia o racjonalnym prawodawcy*, "Zeszyt Prawniczy UAM" 2023, no. 13, pp. 7-18.

[12] J. Kaplan, *Sztuczna inteligencja. Co każdy powinien wiedzieć*, Warszawa 2019, pp. 15-16.

According to a doctrinal definition of AI, it is a system that allows for the performance of tasks that require a learning process and taking into account new circumstances in the course of solving a given problem and that can, to a varying degree – depending on the configuration – act autonomously and interact with the environment.[13] Artificial intelligence is the study of machines that perform tasks that require intelligence while being performed by humans (M. Minsky). It is an activity of computer science that concerns methods and techniques of symbolic reasoning by a computer, as well as symbolic representation of knowledge during reasoning (E. Feigenbaum). It concerns problem-solving that is based on actions and cognitive processes that are natural to humans using computer simulation (R. J. Schalkoff)[14]. Neural networks have a special place among models used in machine learning. These networks are inspired by the structure of the human nervous system and are created in its shape. These models are numerous and adapted to the specifics of the types of data processed, applications and types of processed data.[15]

Artificial intelligence is a field related to many sciences. It correlates of course with computer science, teleinformatics, mathematics, but also with psychology, economics, sociology and law, and its many branches. It was undoubtedly very difficult that for many years artificial intelligence systems did not have their legal definition. In fact, each of these fields has developed its own definition over the years. Each definition uses a conceptual scope appropriate to its area. Unfortunately, this does not change the fact that such definitions are the result of scientific needs, but do not have their impact on legal regulations. That is why it was so important to create a legal definition. Breakthrough came in 2024 when the AI act regulation came into force. Although theis regulation contains a very rich dictionary of legal definitions and the very definition of an AI system is consistent with previous scientific definitions, there remains a certain dissatisfaction. It is about including the definition of AI systems in the discussed regulation.

As stated in Article 3, point 1, the artificial intelligence system is: "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical

[13] T. Zalewski, *Rozdział I. Definicja sztucznej inteligencji*, [in:] *Prawo sztucznej inteligencji*, eds. L. Lai, M. Świerczyński, Warszawa 2020, pp. .

[14] L. Rutkowski, *Metody i techniki sztucznej inteligencji,* Warszawa 2012, s. 19.

[15] J. Arabas, J. Chudziak, *Sztuczna inteligencja w odbiorze społecznym. Metafory a rzeczywistość,* [in:] *Informatyka a filozofia. Zaufanie do systemów sztucznej inteligencji,* eds. M. Jakubiak, P. Stacewicz, Warszawa 2023, p. 18.

or virtual environments."[16] Unfortunately, the AI system is being pointed out here, not the AI itself. We can say that we still do not legally know what the AI itself is. Definition of risk, provider, deployer, importer, distributor, importer, behind which each time stands a physical or legal person. Hence, the entire regulatory system is based on the principle of risk and human responsibility for the negative effects of AI activity. However, delving very deep into artificial intelligence, we have not legally defined what it is in itself. This is a big shortcoming and simplification.

The same applies to the definition of artificial intelligence in the framework convention. In Article 2 it is stated that "artificial intelligence system means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment."[17]

First of all, this results from the need to reach the very foundations of the issue of artificial intelligence, and then it is about clarifying many other legal issues that the European legislator did not include in the regulation. Above all, the role of humans may be limited to merely formally approving the results of the program's operation. AI often operates in an unclear and complicated manner, and often there is a lack of knowledge and skills to verify the correctness of its results, which is the reason why people tend to approve AI actions without controlling them. The second issue is the dignity of artificial intelligence, whether we can talk about it at all or in what aspect. Will it correspond to human dignity or should it be appropriately modified. These aspects are of great importance in fundamental issues such as morality, ethical conduct and safety.

3. Safety problems

To operate safely, artificial intelligence systems need to be based on good quality data. The input and acquisition of such data depend on humans and their responsibility for operational and analytical data. In addition, these data are created and acquired from humans.[18] Current requirements and guidelines that new regulations contain are very relevant. They are primarily about human efficiency and oversight, technical soundness and security, privacy and data management, transparency, diversity and non-discrimination, fairness, social and environmental well-being.

[16] Article 3 of Regulation 2024/1689.
[17] Article 2 of Framework Convention.
[18] M. Nowakowski, *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych,* Warszawa 2023, p. 48.

In relation to security, both European regulations refer differently. Firstly, the Framework Convention does not refer at all to the value of security and its types. It is different in the case of the EU Regulation 2024/1689. Security appears in the normative act very often and in different contexts. Many references to different security values can be found in the extended preamble of the act. Most often, the legislator refers to security and the protection of fundamental human rights. There are also references to the security of justice system, food, and personal security. Some regulations refer to national security. If AI systems are placed on the market, put into service or used, with or without modification, for military, defence or national security purposes, they should be excluded from the scope of this Regulation, regardless of the entity carrying out those activities – for example, whether it is a public or private entity. In the case of national security purposes, this exclusion is justified both by the fact that national security is the exclusive responsibility of the Member States by the fact that national security activities are of a specific nature, entail specific operational needs and are subject to specific national rules. However, where an AI system is developed, placed on the market, put into service or used for military, defence or national security purposes is used temporarily or permanently for other purposes, for example civilian or humanitarian purposes, law enforcement or public security, such a system will fall within the scope of this Regulation.[19]

Artificial intelligence can significantly impact broadly understood security, automating threat detection, monitoring human activities and even predicting potential threats. At the same time a lot of caution is needed, because AI itself creates new threats, often very advanced ones. This mainly concerns cyberattacks, data manipulation, and theft. This is due to the fact that AI systems have access to very sensitive data – personal data, they interfere with the right to privacy, and have contact with biometric data obtained from people. AI can be used to generate convincing fake news, photos, videos, which can lead to disinformation and numerous manipulations. This in turn can have significant social consequences. More and more network users are sharing highly confidential information, which poses a risk to privacy and data security. In this context, it is important to note that AI can also make mistakes, especially if it is working with poor quality data or which is limited or biased. This in turn can lead to poor decision-making or discrimination. In this regard, appropriate education and campaigns are also necessary to make people aware that AI is a blessing of our times, but it is also a great threat if it gets out of control.

[19] Preamble, article 1 and article 2 of Regulation 2024/1689.

4. AI and ethics

Intelligent robots may in the future cast a shadow over the foundations of philosophy and religion. Ethical and moral doubts are raised by the fact whether something that is not natural, has no biological origin, can be treated within the framework of the same for all living beings, so people and animals. This applies to issues concerning the mind and thinking, emotions and their feeling and expression, as well as the aforementioned dignity.[20]

And at this point, the important distinction between weak and strong AI is pointed out. The weak one means a kind of technology that simulates, imitates, and uses simple commands. A much bigger problem is strong artificial intelligence, characterised by such enormous technological advancement that it works in a way similar to the human mind, often surpassing its capabilities.[21]

J. Kaplan asks very pertinent questions in his work "*Artificial Intelligence. What everyone needs to know*", such as: "can a computer think?", "does a computer have free will?", "can a computer be conscious?", "can a computer feel?"[22] At first glance, these seem to be rhetorical questions, too ideological, or maybe even nonsensical – taken from science fiction movies. Nothing could be further from the truth. Artificial intelligence is becoming our reality. Although it seems that visions of the world around us with robots are unrealistic or very distant, this is a much closer future. Therefore, legislation should now aim to introduce a complete, legal framework that will protect the most important values from potential violations by AI. This applies to both the European legislator and other systems of international law, e.g. the United Nations, the Council of Europe, but also to each national legislator.

From an ethical perspective, the key issue within AI systems is trust, which is based and verified on credibility. The decision to trust leans primarily on the analysis and assessment of credibility. In turn, credibility, which is very important from the AI perspective, can be distinguished between substantive and ethical-moral. First depends on factors such as knowledge, competence or experience. Second is the result of acting on the basis of ethical norms and principles. At current stage of development of artificial intelligence, substantive credibility is important, because for now these systems do not fully make their own ethical choices. Of course, it is possible that at a higher level of technological development such actions will be possible. Currently, people program AI, so morality is related to their decisions and choices. However, the potential of machine learning is so great that in some time robots may show human characteristics, such as being guided by the rules of ethics and morality or not.[23]

[20] J. Kaplan, op. cit., s. 90-91.
[21] J. Kaplan, op. cit., s. 92.
[22] J. Kaplan, op. cit., s. 93-113.
[23] P. Stacewicz, *Wyjaśnianie, zaufanie i test Turinga*, [in:] *Informatyka a filozofia…,* op. cit., p. 27.

Understanding the concept of trust in the context of AI must be based on the distinction between ethics and thin and thick concepts. The thin concept is focused on action while lacking moral responsibility. This results from the lack of self-awareness of AI – at least at the current stage of technological development, because this may change in the near future. This type of approach is appropriate for technical sciences and their methodologies. Trust here is based on the developed technology and, above all, on reliability. The thick concept of trust differs because it is about deep valuation, axiology through the pursuit of moral perfection.[24]

In the perspective of the current development of new technologies, artificial intelligence systems are assessed as trusted or not through the prism of industry. Therefore, the fulfilment of certain criteria, such as practical, operational and technological requirements, is examined.[25] AI systems should be created in such a way that they provide benefits to the society. Introducing AI only for the purpose of improving technology or making it more interesting is not good. Similarly, the creation and use of systems should not take place only for the profit or benefit of its creators, if this would have a negative balance for the whole.[26]

Conclusions

In conclusion to the analysis of European regulations in the matter of artificial intelligence, it should be stated with full certainty that this regulation constitutes an innovative and groundbreaking approach to the legal systematization of AI. While the creation of basic principles of functioning of artificial intelligence, the issue of liability for damages, and the introduction of division of AI systems due to risk should be referred to with great approval, there are certainly some shortcomings. Fundamental issues were missed by the legislator.

What is particularly problematic in both regulations is the lack of a fundamental explanation of the concept of artificial intelligence itself, which affects the foundations of the entire AI system. It is possible that at the current stage of development of new technologies the applicable assumptions will be sufficient, but in the longer term they may unfortunately prove to be insufficient, too general and too shallow. Certainly, this system should be expanded to establish and define the concepts underlying it, i.e. artificial intelligence itself, and not just artificial intelligence systems. In connection with this, the issues of dignity and rights that belong to artificial intelligence should also be expanded. Basing AI on the

[24] P. Polak, R. Krzanowski, *Ku zaufanej sztucznej inteligencji. Perspektywa fronetyczna,* [in:] *Informatyka a filozofia…,* op. cit., p. 38.
[25] P. Polak, R. Krzanowski, op. cit., p. 37.
[26] P. Polak, R. Krzanowski, op. cit., p. 40.

principle of the human factor and its participation and control at every stage of life of artificial intelligence is a good solution for now, but in the future it may not be enough. We can already see that we are dealing with autonomous systems. An autonomous system is a system capable of acting and making decisions without constant human intervention, with the ability to self-regulate and maintain its state in a changing environment. An example of such a system would be a vehicle controlled autonomously by artificial intelligence. It should be borne in mind that we will increasingly be dealing with such systems, including robots, in our space.

Bibliography

1. Arabas J., Chudziak J., *Sztuczna inteligencja w odbiorze społecznym. Metafory a rzeczywistość,* [in:] *Informatyka a filozofia. Zaufanie do systemów sztucznej inteligencji*, eds. M. Jakubiak, P. Stacewicz, Warszawa 2023, pp. 9-22.
2. Binkowski K., *Sztuczna inteligencja a wykładnia prawa – propozycja zastosowania systemów AI do ustalania założenia o racjonalnym prawodawcy*, "Zeszyt Prawniczy UAM" 2023, no. 13, pp. 7-18.
3. Kaczmarczyk M., *O systemach sztucznej inteligencji w kontekście praw człowieka w orzecznictwie Europejskiego Trybunału Praw Człowieka*, "Studia Prawa Publicznego" 2025, no. 2, pp. 9-30.
4. Kaplan J., *Sztuczna inteligencja. Co każdy powinien wiedzieć*, Warszawa 2019.
5. Konieczna A., *Problematyka sztucznej inteligencji w świetle prawa autorskiego*, "Zeszyty Naukowe Uniwersytetu Jagiellońskiego" 2019, no. 4, pp. 104-115.
6. Maternowska M., *Nowe technologie i ich wpływ na łańcuchy dostaw. Sztuczna inteligencja*, "Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2019, no. 388, pp. 59-73.
7. Mazur J., *Unia Europejska wobec rozwoju sztucznej inteligencji: proponowane strategie regulacyjne a budowanie jednolitego rynku cyfrowego*, "Europejski Przegląd Sądowy" 2020, no. 4, pp. 13-18.
8. Nowakowski M., *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2023.
9. Polak P., Krzanowski R., *Ku zaufanej sztucznej inteligencji. Perspektywa fronetyczna*, [in:] *Informatyka a filozofia. Zaufanie do systemów sztucznej inteligencji*, eds. M. Jakubiak, P. Stacewicz, Warszawa 2023, pp. 35-45.
10. Rutkowski L., *Metody i techniki sztucznej inteligencji*, Warszawa 2012.
11. Stacewicz P., *Wyjaśnianie, zaufanie i test Turinga,* [in:] *Informatyka a filozofia. Zaufanie do systemów sztucznej inteligencji*, eds. M. Jakubiak, P. Stacewicz, Warszawa 2023, pp. 23-34.
12. Świątkowski A. M., *Warunki rozwojui wpływ sztucznej inteligencji na pracę, zatrudnienie, i inne niektóre prawnie nieuregulowane w Unii Europejskiej zagadnienia społeczne, technologiczne i gospodarcze,* "Roczniki Administracji i Prawa" 2021, vol. XXI, pp. 113-127.
13. Wawrzyński P., *Podstawy sztucznej inteligencji*, Warszawa 2019.
14. Zalewski T., *Definicja sztucznej inteligencji*, [in:] *Prawo sztucznej inteligencji*, eds. L. Lai, M. Świerczyński, Warszawa 2020.

Part IV:

The Social Dimension of Security in Times of Crisis

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 333–344

ISSN 2543-6961
e-ISSN 2720-3093

Tomasz Marcinkowski
ORCID: 0000-0002-3568-5068
Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim

Health Security in the EU During the Implementation of the Vaccination Strategy in the Covid-19 Pandemic

Bezpieczeństwo zdrowotne w UE w trakcie realizacji strategii szczepień w czasie pandemii Covid-19

Abstract
The Covid-19 pandemic constituted an unprecedented challenge to public health, politics, and society in the European Union. This article examines the Union's actions aimed at strengthening health security through the implementation of mass vaccination. Key measures included the provision of high-quality, effective, and safe vaccines; support for research and production; the adjustment of legal frameworks and regulatory procedures; and transparent, proactive communication designed to counter disinformation. The European Medicines Agency played a central role through rolling reviews, conditional marketing authorizations, and post-market surveillance. The analysis conducted in this article indicates that the EU's vaccination strategy reinforced citizens' sense of health security, while simultaneously revealing the pre-existing limitations of supranational competences in this domain.

Keywords: EU health policy, Covid-19 pandemic, vaccination, health security, disinformation, public trust

Abstrakt
Pandemia Covid-19 stanowiła bezprecedensowe wyzwanie dla zdrowia publicznego, polityki i społeczeństwa w Unii Europejskiej. Artykuł analizuje działania UE w zakresie budowania bezpieczeństwa zdrowotnego poprzez masowe szczepienia. Kluczowe działania obejmowały zapewnienie wysokiej jakości, skutecznych i bezpiecznych szczepionek, wsparcie badań i produkcji, dostosowanie ram prawnych i stosowanych procedur oraz transparentną, aktywną komunikację w celu przeciwdziałania dezinformacji. Europejska Agencja Leków odegrała centralną rolę poprzez przeglądy ciągłe, warunkowe dopuszczenia do obrotu i nadzór po wprowadzeniu szczepionek na rynek. Przeprowadzona w artykule analiza wskazuje, że strategia szczepionkowa UE wzmocniła poczucie bezpieczeństwa zdrowotnego obywateli, ujawniając jednocześnie istniejące już wcześniej ograniczenia kompetencji ponadnarodowych w tym obszarze.

Słowa kluczowe: polityka zdrowotna w UE, pandemia Covid-19, szczepienia, bezpieczeństwo zdrowotne, dezinformacja**,** zaufanie publiczne

Introduction

The Covid-19 pandemic emerged as an unprecedented challenge for the entire world – one that was not confined to the health sector, but extended to economic, social, and political domains. A crucial dimension of this crisis concerned public trust in the institutions responsible for crisis management, both at the national and at the European level.[1] One of the most significant challenges in this regard was the need to build trust during the implementation of mass vaccination campaigns. This proved particularly difficult due to the traumatic experiences of Europeans during the first months of the pandemic, as well as the intensification of disinformation.[2]

The aim of this article is to examine the process of constructing a sense of security in the context of the unprecedented implementation of mass vaccination campaigns in EU member states. The author advances the hypothesis that safeguarding health security during the rollout of mass Covid-19 vaccination comprised two dimensions: first, the provision of high-quality and safe medical products (the medical dimension); and second, the pursuit of transparent communication policies designed to counteract disinformation (the societal dimension).

The analysis of the research problem is based on a purposive selection of EU documents as well as the relevant academic literature on health security and vaccination policy during the pandemic. The selection of documents is both selective and problem-oriented, allowing for the identification of key actions undertaken at the EU level in relation to mass vaccination. Methodologically, the article relies on qualitative research, encompassing: content analysis of strategic documents with reference to health security, vaccine quality, and public communication and literature studies that enable the situating of the issue within a broader context. The article adopts the form of a case study of the European Union's vaccination policy, with the objective not only of reconstructing the actions of EU institutions, but also of reflecting on how this process contributed to the strengthening (or weakening) of citizens' perceptions of health security.

The Pandemic as a Threat to Health Security in the EU

The issue of public health constitutes an important subject of inquiry not only within the field of health sciences, but also in political science, security studies, and international relations.[3] The Covid-19 pandemic placed health squarely at

[1] See Z. Czachór, P. Leszczyński, T. Marcinkowski, *Polska-Niemcy-Unia Europejska. Wartości i polityka wobec wybranych wyzwań współczesności*, Gorzów Wielkopolski 2025, pp.166-175.

[2] See Czachór Z., Marcinkowski T., Sikorski J., *Polityka zdrowotna Unii Europejskiej w obliczu działań klasyfikowanych jako walka informacyjna. Casus pandemii covid-19*, [in:] *Skutki i zagro¿enia cywilizacji informacyjnej*, eds. K.A. Nawrot, K. Prandecki, Warszawa 2023, pp. 159-179.

[3] See I. Wrześniewska-Wal, V. Korporowicz-Żmichowska, *Rezylientność i adaptacyjność polityki zdrowotnej w czasach zagrożeń egzystencjalnych: Studium na przykładzie kadry medycznej*, „Studia z Polityki

the center of politics, becoming a factor that reshaped dynamics at both the state level and within international organizations such as the European Union. The concept of health security is defined in various ways across the scholarly literature.[4] As M. Pietraś observes, "as a category of political practice, it has been gaining increasing acceptance, particularly under the conditions of the Covid-19 pandemic."[5] At present, health security is shaped by processes of globalization—especially social mobility—and conditioned by prevailing values as well as socio-economic determinants. Its significance becomes particularly salient in times of crisis.

The European Union possesses rather limited competences in the field of public health.[6] Responsibility for population health lies primarily with the member state authorities, while the Union plays a complementary role to national activity in this domain. Within the process of European integration, successive treaty revisions, rulings of the Court of Justice of the European Union, and initiatives of the European Commission have placed health policy under growing pressures of Europeanization.[7] Nevertheless, the solutions and legal frameworks developed prior to 2020 proved insufficient for an effective crisis response to the Covid-19 threat. The outbreak of the pandemic took the European Union—lacking appropriate supranational procedures and instruments—by considerable surprise. Member states, too, were initially caught unprepared, seeking to cope with the crisis through their own national strategies. Yet, the rapid spread of the pandemic, the magnitude of the problem, and its transboundary nature necessitated action at the EU level.[8]

An analysis of the Union's actions during the pandemic threat[9] indicates that vaccination and social distancing were, from the very outset, identified as key

Publicznej" 2024, vol. 11, no. 4, pp. 7-25, V. Korporowicz, *Polityka zdrowotna w systemie nauk o polityce publicznej*, „Studia z Polityki Publicznej" 2015, vol. 2, no.1(5), pp. 47-62, M.J. Kuczabski, *Kategoria bezpieczeństwa zdrowotnego w naukach o bezpieczeństwie*, „Studia Bezpieczeństwa Narodowego" 2021, issue 21 (2021), pp.11-32.

4 A. Augustynowicz, J. Opolski, M. Waszkiewicz, *Health Security: Definition Problems*, "International Journal of Environmental Research and Public Health" 2022, no. 19, pp. 1-7.

5 M. Pietraś, *Bezpieczeństwo zdrowotne jako wymiar bezpieczeństwa międzynarodowego*, „Atheneum. Polskie Studia Politologiczne" 2023, vol. 78(2), p. 263.

6 See M. Nabbe, H. Brand, *The European Health Union: European Union's Concern about Health for All. Concepts, Definition, and Scenarios*, "Healthcare" 2021, no. 9, pp. 1-13.

7 R. Riedel, *Europeizacja polityki zdrowotnej na przykładzie zdrowia w miejscu pracy*, [in:] *Wokół teoretycznych i praktycznych aspektów stosunków międzynarodowych*, eds. T. Kubin, J. Łapaj-Kucharska, T. Okraska, Kartowice 2020, p.261-276.

8 See. A. Alemanno, *The European Response to COVID-19: From Regulatory Emulation to Regulatory Coordination?*, "European Journal of Risk Regulation" 2020, vol. 11:2, pp. 307-316.

9 See S. Golinowska, M. Zabdyr-Jamroz, *Zarządzanie kryzysem zdrowotnym w pierwszym półroczu pandemii COVID-19. Analiza porównawcza na podstawie opinii ekspertów z wybranych krajów*, „Zdrowie Publiczne i Zarządzanie" 2020 18 (1), pp.1–31, T. Marcinkowski, *Polityka antykryzysowa Unii Europejskiej w obliczy pandemii SARS CoV-2 w obszarze zdrowia publicznego w 2020 roku. W poszukiwaniu rozwiązań funkcjonalnych*, „Rocznik Integracji Europejskiej" 2021, no. 15, pp. 181-194.

components of population-based management (PBM). Accordingly, the European Union undertook measures to support vaccine development.[10] This included financial support and guarantees that enabled scientific research and implementation efforts, as well as initiatives to expand production capacity. Regulatory adjustments were also introduced, aimed at accelerating the market authorization of vaccines in Europe as swiftly as possible, without compromising their quality and safety. Equally significant was the commitment to transparent strategic communication, serving as a response to the escalating scale of disinformation.[11]

The EU Vaccination Strategy and Vaccine Safety

On 17 June 2020, the European Commission presented the Union's vaccination strategy. It emphasized the urgent need for anti-pandemic measures and proposed a common approach to the challenge. The strategy identified three key objectives: ensuring the availability of effective, safe, and high-quality vaccines; securing rapid access to vaccines for residents of the member states; and guaranteeing, as swiftly as possible, equitable access to affordable vaccines worldwide. The Union's actions to achieve these objectives rested on two main pillars: first, securing sufficient vaccine production within the EU and adequate supply for member states; and second, adapting the legal framework to the crisis situation while making use of existing regulatory flexibility.[12]

In the analyzed strategic document, the Commission emphasized the necessity of adopting a special approach in light of the exceptional circumstances. It highlighted the need to significantly shorten the typically lengthy periods of vaccine development, diversify the financial risks associated with research and development, expand production capacity and access to raw materials, and facilitate the market entry of finalized vaccines within the Union. The importance of collective action was underscored, as it would prevent competition among member states.

[10] See K. Goniewicz, A. Khorram-Manesh, A.J. Hertelendy, M. Goniewicz, K. Naylor, F.M. Burkle Jr., *Current Response and Management Decisions of the European Union to the COVID-19 Outbreak: A Review*, „Sustainability" 2020, vol. 12, no. 9.

[11] See. T. Marcinkowski, J. Sikorski J., *The European Union's policy towards the COVID-19 crisis in 2020 and the Russian contribution to infodemic*, [in:] *Information, Security and Society in the COVID-19 Pandemic*, eds. N. Moch, W. Wereda, J. Stańczyk, Abingdon 2023, pp.147-172, J. Sikorski, *Social Implications of Infodemic Concurrent with COVID-19,* "Polish Political Science Yearbook" 2023 52(4), pp. 79-89, A. Demczuk, *Ruch antyszczepionkowy w Polsce i jego kabiny pogłosowe w alt-internet w latach 2020-2022*, "Rocznik Instytutu Europy Środkowo-Wschodniej" 2022, no. 3, pp. 9-35.

[12] EU Strategy for COVID-19 vaccines. Communication from the Commission to the European Parliament, the European Council, the Council and the European Investment Bank, Brussels, 17.6.2020, COM(2020) 245 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0245 [date of access:12.04.2024].

At the same time, it was stressed that vaccines must meet strict standards of quality, safety, and efficacy.

The Strategy also outlined criteria for decision-making regarding the financing of research and production of vaccines. Among these, a prominent role was assigned to the scientific soundness of the approach, which required reliance on all available scientific evidence concerning quality, safety, and efficacy. Additional criteria included: the speed of delivering large quantities of vaccines, the consideration of different technological approaches, cost factors, the capacity to ensure supply through the development of EU-based production capabilities, the clarification of risk and liability, early engagement with EU regulatory authorities, and the principle of global solidarity.[13] The document further emphasized the special role of the European Medicines Agency.

Attention to the problem of vaccine safety and efficacy was also drawn in Preparedness for COVID-19 vaccination strategies and vaccine deployment. The document emphasized that "the development and swift global deployment of safe and effective vaccines against COVID-19 remains an essential element in the management of and eventual solution to the public health crisis. Vaccination, once a safe and efficient vaccine is available, will play a central role in saving lives."[14] It was stressed that despite the time pressure connected with the pandemic crisis, the standards of quality, safety, and efficacy in the creation and production of vaccines would not be compromised. It was also underlined that until vaccinations in sufficient quantities were introduced in the member states, existing measures should be continued and intensified, both in response to the evolving epidemiological situation and in order to limit as far as possible the spread of the coronavirus.

The European Medicines Agency – Safety and Procedures

In the context of the pandemic crisis, there arose an expectation of maximum optimization of actions not only from pharmaceutical companies, but also from regulatory authorities within the EU and its member states. The aim in this regard was to strike a balance between accelerating the evaluation of submitted medicines and vaccines, and maintaining scientific standards as well as a high level of safety.[15]

[13] EU Strategy for COVID-19 vaccines. Communication from the Commission to the European Parliament, the European Council, the Council and the European Investment Bank, Brussels, 17.6.2020, COM(2020) 245 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0245 [date of access: 12.04.2024].

[14] Preparedness for COVID-19 vaccination strategies and vaccine deployment, Communication From The Commission To The European Parliament And The Council, COM(2020) 680 final, Brussels, 15.10.2020.

[15] See N. Wathion, EMA'S Response to The Covid-19 Pandemic. Putting People's Health First, European Medicines Agency, August 2023.

An important measure implemented by the European Medicines Agency was the rolling review, which made it possible to assess data on a given product as soon as they became available. Conditional marketing authorization was also applied. This enabled faster approval of vaccines once a positive benefit–risk balance had been established, even if the dataset was not yet complete. Such a solution, however, required a highly rigorous post-marketing control mechanism within the Union.[16] In addition, given the activities of anti-vaccination movements and the spread of disinformation, adequate and non-standard communication in this area proved essential.

As noted by the authors of *Shaping EU medicines regulation in the post COVID-19 era*, there also emerged demands for the introduction of an EU-wide temporary authorization for use in exceptional circumstances: "Around the time of approval of the first COVID-19 vaccine, mainstream media raised the need for a faster approval framework under temporary emergency use authorisation (EUA) at EU level. Such a mechanism to temporary supply unauthorised medicines in the context of a public health threat can be used by individual MSs at national level, but it does not exist EU-wide."[17]

In response to the unprecedented health crisis caused by the Covid-19 pandemic, the European Union—through the European Medicines Agency (EMA) and the national competent authorities (NCAs)—launched in November 2020 a harmonized, transnational mechanism for vaccine safety monitoring. These measures can be interpreted in light of neofunctionalist theory as an example of functional spillover, whereby integration in one domain (public health) generates deeper institutional and technocratic cooperation in other areas (pharmaceutical regulation). As described in the Report on pharmacovigilance tasks from EU Member States and the European Medicines Agency (EMA) 2019–2022, the safety monitoring plan established a comprehensive, centralized reporting system in which vaccine producers were required to submit Risk Management Plans (RMPs), Periodic Safety Update Reports (PSURs),[18] and monthly Summary Safety Reports (SSRs).[19] These mechanisms were intended to reinforce mutual trust and coordination among member states.

[16] M. Cavaleri, F. Sweeney, R. Gonzalez-Quevedo, M. Carr, *Shaping EU medicines regulation in the post COVID-19 era*, "The Lancet Regional Health – Europe" 2021, no. 9.

[17] M. Cavaleri, F. Sweeney, R. Gonzalez-Quevedo, M. Carr, *Shaping EU medicines regulation in the post COVID-19 era*, "The Lancet Regional Health – Europe" 2021, no. 9, p. 2.

[18] On the official guidelines regarding the preparation of periodic safety update reports (PSURs) for COVID-19 vaccines, See. Consideration on core requirements for PSURs of COVID-19 vaccines, corePSUR19 guidance, EMA/362988/2021, 8 July 2021.

[19] See: Consideration on core requirements for RMPs of COVID-19 vaccines, coreRMP19 guidance v3.1, EMA/PRAC/709308/2022, 01 September 2022.

At the operational level, a coordinated and intensified pharmacovigilance system was introduced, including near real-time monitoring of suspected adverse drug reactions (ADRs), particularly with regard to so-called Adverse Events of Special Interest (AESIs). The EU's EudraVigilance system, as a shared information infrastructure, played a key role in collecting 2.8 million individual reports in 2021–2022, representing an example of deepened technological and knowledge-centered integration. Analyses conducted during the pandemic using advanced statistical methods (e.g., observed vs. expected [O/E] analysis), along with the integration of tools such as standardized MedDRA queries and data visualization within the EudraVigilance system, confirm the processes of professionalization and epistemization of EU regulatory policy. The extraordinary mobilization of resources – such as ad hoc expert groups and accelerated MedDRA updates –simultaneously demonstrated the flexibility of Union structures under conditions of crisis.[20] These represent crucial institutional solutions and experiences that may be drawn upon in the future.

As a result of the measures undertaken within the EU, it was established that the vast majority of adverse reactions to Covid-19 vaccines were mild or moderate in nature, occurred shortly after vaccination, and were short-lived. However, rare or very rare adverse reactions were also observed—reactions that had not appeared during clinical development due to their infrequency. These, however, were quickly detected, assessed, and addressed.

For example, in cooperation with the U.S. Food and Drug Administration, an issue was identified concerning thrombosis with thrombocytopenia syndrome (TTS) in relation to adenovirus vector-based Covid-19 vaccines (Vaxzevria and Jcovden). The European Medicines Agency and the EU pharmacovigilance network responded proactively, taking action even before the broad rollout of the Janssen vaccine in the member states. It is worth emphasizing that data from the EudraVigilance system played a crucial role in the early detection and risk assessment of TTS. The actions of the Pharmacovigilance Risk Assessment Committee (PRAC) led to updates of the product information (PI), the Risk Management Plan (RMP), and the issuance of Direct Healthcare Professional Communications (DHPCs). The European Union was one of the first actors globally to identify and describe the link between TTS and the vaccines.

These measures demonstrated the Union's capacity for rapid response and effective supranational risk management. EudraVigilance thus proved its

[20] Report on pharmacovigilance tasks. From EU Member States and the European Medicines Agency (EMA) 2019-2022, EMA 142695/2023, European Medicines Agency 2023, see also S. B. Black, B. Law, R.T. Chen et al., *The critical role of background rates of possible adverse events in the assessment of COVID 19 vaccine safety*, "Vaccine" 2021, no. 39), pp. 1712-1718.

effectiveness as a tool for swift detection of safety signals and the implementation of appropriate regulatory actions, which was of central importance throughout the pandemic. This case confirmed the effectiveness of the EU's health security model, as well as the necessity of further strengthening European mechanisms of health coordination and shared monitoring infrastructure.[21]

Strategic Communication during the Covid-19 Pandemic and Trust in the Vaccination Process

As rightly noted by the authors of the *State of Vaccine Confidence in the EU+UK 2020* report: "Although public concerns over vaccines are as old as vaccines themselves, the rapid spread of infor[m]ation facilitated by hyper-connected online and offline populations has contributed to the spread and amplification of public concerns surrounding vaccination."[22] In Europe, anti-vaccination movements and disinformation have also been gaining increasing significance. This creates an environment that hampers the achievement of vaccination strategy objectives and undermines patients' trust in vaccines.[23]

According to surveys conducted in EU member states and the United Kingdom in 2020 on representative samples of adult residents, the vast majority considered vaccines to be important, safe, and effective. Researchers also demonstrated an increase in confidence in vaccines between 2018 and 2020. However, the level of confidence varied (though remained high overall) across the countries studied: it was highest in Portugal and Spain, and lowest in Hungary and Malta. At the same time, surveys among healthcare professionals revealed a higher level of confidence in vaccines compared to the general population. This is particularly significant, as physicians' opinions are an important factor shaping patients' attitudes and decisions. It is doctors and health system institutions—both at the national level and at the EU level (especially the European Medicines Agency)—that must serve as the source of reliable and effective communication during a crisis.

The European Medicines Agency, which played a decisive role in implementing the EU vaccination strategy, had to adopt special, non-standard measures in the field of communication. These measures included stakeholder meetings, strengthened

[21] See: 2021 Annual Report on EudraVigilance for the European Parliament, the Council and the Commission. Reporting period: 1 January to 31 December 2021, EMA/719826/2021 Noted, 17 March 2022, European Medicines Agency 2022.

[22] A. De Figueiredo, E. Karafillakis, H. J. Larson, *State of Vaccine Confidence in the EU+UK 2020*, Luxembourg: Publications Office of the European Union, 2020.

[23] See: A. Lusawa, J. Pinkas, W.S. Zgliczyński, M. Mazurek, W. Wierzba, *Nieprawdziwe informacje w zakresie szczepień ochronnych jako wyzwanie dla zdrowia publicznego*, „Zdrowie Publiczne i Zarządzanie" 2019, no. 17 (1), pp. 40–45.

cooperation with the media, and regular safety updates on pandemic-related products. To improve clarity, the Agency's communications made use of visual materials explaining regulatory issues and assessment outcomes (e.g., risk diagrams or approval process charts). Building a high level of trust also required measures of extraordinary transparency. Accordingly, the standard time for publishing assessment reports (e.g., European Public Assessment Reports – EPARs) was shortened, and permission was granted to publish data not usually disclosed for other medicines (e.g., lists of medicines receiving scientific advice from the ETF, full Risk Management Plans, etc.). At the same time, once Covid-19-related products were approved, the Agency published the report of the scientific assessment. During the process itself, representatives of patient, consumer, and healthcare professional organizations from across the EU were included in the ETF and participated in discussions.[24]

As highlighted in the document "Tackling COVID-19 disinformation – Getting the facts right", the Covid-19 pandemic was accompanied from the very beginning by an "infodemic".[25] Its effect was the creation of confusion, which could lead to a decline in trust in vaccination or medical measures in general, and ultimately hinder an effective anti-pandemic response. Among the examples of disinformation activities were fraudulent and misleading messages concerning healthcare, containing false claims (e.g., regarding the use of chemical substances as medical treatments), conspiracy theories (e.g., linking coronavirus to 5G),[26] incitement to hatred (e.g., blaming a specific national, ethnic, or religious group for the pandemic), as well as consumer fraud and other forms of cybercrime.

It was emphasized that the actions of the Union and the member states must remain consistent with democratic values while at the same time protecting

[24] The EMA COVID-19 Task Force (COVID-ETF) included: the Chair or Vice-Chair of the Committee for Medicinal Products for Human Use (CHMP), the Chair of the Paediatric Committee (PDCO) and of the Pharmacovigilance Risk Assessment Committee (PRAC), the Scientific Advice Working Party (SAWP), the Vaccine Working Party (VWP), and the Infectious Disease Working Party (IDWP). As needed, it also included representatives from the Biologics Working Party (BWP), the Quality Working Party (QWP), the Safety Working Party (SWP), the Blood Product Working Party (BPWP), and the Coordination Group for Mutual Recognition and Decentralised Procedures – Human (CMDh). Additionally, it comprised representatives from the Clinical Trial Facilitation Group (CTFG), the CHMP rapporteur or co-rapporteur for products intended to treat or prevent Covid-19, a representative of the Reference Member State (RMS) for products in the context of MRP/DCP intended to treat or prevent Covid-19, patient and healthcare professional representatives, and selected experts as required, Mandate, objectives and rules of procedure of the COVID-19 EMA pandemic Task Force (COVID-ETF), 20 June2021 EMA/166423/2020 Rev. 11, Biological Health Threats and Vaccines Strategy.

[25] See: Tackling COVID-19 disinformation – Getting the facts right. Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, High Representative of the Union for Foreign Affairs and Security Policy, JOIN(2020) 8 final, Brussels, 10.6.2020.

[26] See: T. Marcinkowski, J. Sikorski, L. Vomlela, *Conspiracy Narratives About the Covid-19 Pandemic and the Origins of the Sars-Cov-2 Virus: A Contribution to Polish-Czech Comparative Research*, "Politeja" 2025, no. 4(98), pp. 315-336.

citizens from the harmful influence of external and internal actors. Disinformation activities, as underlined, are intended, among other things, to undermine democracy and the credibility of Union institutions, and ultimately to weaken cohesion and disrupt the process of European integration. In view of the growing threat, proactive and positive communication on the part of crisis-response actors is essential. Efforts should also be made to build citizens' resilience (including raising awareness of disinformation threats and strengthening digital competences). Such efforts should involve not only EU institutions and bodies, but also the competent authorities of member states, non-governmental organizations, social media platforms, and other actors present in cyberspace.

In the analyzed document, the Commission announced the strengthening of strategic communication, the improvement of information exchange, and support for actions countering disinformation. Among the proposed measures was the creation of a special early warning section aimed at enhancing the flow of information related to COVID-19. At the same time, it announced stronger cooperation with online platforms, as well as support for organizations engaged in fact-checking and for researchers working in areas related to pandemic crisis management.

Reliable, rapid, and effective communication that builds trust constitutes an important part of vaccine safety. The effectiveness of COVID-19 vaccination campaigns depended not only on clinical trials and regulatory procedures, but also on public perception shaped by physicians, health institutions, policymakers, and the media. It is not enough for vaccines to be medically safe – what is crucial is whether potential patients share this conviction.

Conclusion

The pandemic, as an unprecedented challenge, revealed the limitations of crisis management at the EU level. At the same time, it exposed threats not only in the medical sphere (risks to health and life), but also in the social sphere (economic disruptions, disinformation, and societal problems). Containing the spread of the pandemic required social measures (e.g., distancing, disinfection, masks), better contact tracing, and the development and market introduction of vaccines. The effectiveness of vaccination strategies depended on the high quality, efficacy, safety, and availability of vaccines, as well as on shaping appropriate social attitudes. A critical condition for the implementation of the strategy was the achievement of a high level of public trust. A particular challenge in this area was the need to address the growing wave of disinformation during the pandemic. Vaccine safety is not only a matter of scientific evidence but also of social perception and strategic

communication. The European Union – including the European Commission and the European Medicines Agency – undertook specific measures both to ensure the high safety of medical products and to provide adequate, active strategic communication.

The COVID-19 pandemic, to some extent, accelerated functional integration in an area that had previously remained peripheral within the EU architecture. Strengthened coordination, the development of common surveillance mechanisms, and the mobilization of knowledge networks constitute a foundation for future health policies built on the principles of solidarity, mutual trust, and technocratic risk management. For health security, this represents both accumulated experience and a permanent strengthening of crisis response capacities.

References

1. 2021 Annual Report on EudraVigilance for the European Parliament, the Council and the Commission. Reporting period: 1 January to 31 December 2021, EMA/719826/2021 Noted, 17 March 2022, European Medicines Agency 2022.
2. Alemanno A., *The European Response to COVID-19: From Regulatory Emulation to Regulatory Coordination?*, "European Journal of Risk Regulation" 2020, vol. 11:2, pp. 307-316.
3. Augustynowicz A., Opolski J., Waszkiewicz M., *Health Security: Definition Problems*, "International Journal of Environmental Research and Public Health" 2022, no. 19., strony?
4. Black S. B., Law B., Chen R. T. et al., *The critical role of background rates of possible adverse events in the assessment of COVID 19 vaccine safety*, "Vaccine" 2021, no. 39, pp. 1712-1718.
5. Cavaleri M., Sweeney F., Gonzalez-Quevedo R., Carr M., *Shaping EU medicines regulation in the post COVID-19 era*, "The Lancet Regional Health – Europe" 2021, no. 9, strony?
6. Consideration on core requirements for PSURs of COVID-19 vaccines, corePSUR19 guidance, EMA/362988/2021, 8 July 2021.
7. Consideration on core requirements for RMPs of COVID-19 vaccines, coreRMP19 guidance v3.1, EMA/PRAC/709308/2022, 01 September 2022.
8. Czachór Z., Leszczyński P., Marcinkowski T., *Polska-Niemcy-Unia Europejska. Wartości i polityka wobec wybranych wyzwań współczesności*, Gorzów Wielkopolski 2025.
9. Czachór Z., Marcinkowski T., Sikorski J., *Polityka zdrowotna Unii Europejskiej w obliczu działań klasyfikowanych jako walka informacyjna. Casus pandemii covid-19*, [in:] *Skutki i zagrożenia cywilizacji informacyjnej*, eds. Nawrot K. A., Prandecki K., Warszawa 2023, strony?.
10. De Figueiredo A., Karafillakis E., Larson H. J., State of Vaccine Confidence in the EU+UK 2020, Luxembourg: Publications Office of the European Union, 2020.
11. Demczuk A., *Ruch antyszczepionkowy w Polsce i jego kabiny pogłosowe w alt-internet w latach 2020-2022*, "Rocznik Instytutu Europy Środkowo-Wschodniej" 2022, no. 3, strony?
12. EU Strategy for COVID-19 vaccines. Communication from the Commission to the European Parliament, the European Council, the Council and the European Investment Bank, Brussels, 17.6.2020, COM(2020) 245 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0245.
13. Golinowska S., Zabdyr-Jamroz M., *Zarządzanie kryzysem zdrowotnym w pierwszym półroczu pandemii COVID-19. Analiza porównawcza na podstawie opinii ekspertów z wybranych krajów*, „Zdrowie Publiczne i Zarządzanie" 2020, no. 18 (1), strony?

14. Goniewicz K., Khorram-Manesh A., Hertelendy A.J., Goniewicz M., Naylor K., Burkle F.M. Jr., *Current Response and Management Decisions of the European Union to the COVID-19 Outbreak: A Review*, „Sustainability" 2020, vol. 12, no. 9, strony?
15. Korporowicz V., *Polityka zdrowotna w systemie nauk o polityce publicznej*, „Studia z Polityki Publicznej" 2015, vol. 2, no.1(5), strony?
16. Kuczabski M. J., *Kategoria bezpieczeństwa zdrowotnego w naukach o bezpieczeństwie*, „Studia Bezpieczeństwa Narodowego" 2021, issue 21, strony?
17. Lusawa A., Pinkas J., Zgliczyński W.S., Mazurek M., Wierzba W., *Nieprawdziwe informacje w zakresie szczepień ochronnych jako wyzwanie dla zdrowia publicznego*, „Zdrowie Publiczne i Zarządzanie" 2019, no. 17 (1), pp. 40–45.
18. Mandate, objectives and rules of procedure of the COVID-19 EMA pandemic Task Force (COVID-ETF), 20 June2021 EMA/166423/2020 Rev. 11, Biological Health Threats and Vaccines Strategy.
19. Marcinkowski T., *Polityka antykryzysowa Unii Europejskiej w obliczy pandemii SARS CoV-2 w obszarze zdrowia publicznego w 2020 roku. W poszukiwaniu rozwiązań funkcjonalnych*, „Rocznik Integracji Europejskiej" 2021, no.15., strony?
20. Marcinkowski T., Sikorski J., *The European Union's policy towards the COVID-19 crisis in 2020 and the Russian contribution to infodemic*, [in:] *Information, Security and Society in the COVID-19 Pandemic* ,eds. N. Moch, W. Wereda, J. Stańczyk. Abingdon 2023, strony?.
21. Marcinkowski T., Sikorski J., Vomlela L., *Conspiracy Narratives About the Covid-19 Pandemic and the Origins of the Sars-Cov-2 Virus: A Contribution to Polish-Czech Comparative Research*, "Politeja" 2025, no. 4(98), strony?
22. Nabbe M., Brand H., *The European Health Union: European Union's Concern about Health for All. Concepts, Definition, and Scenarios*, "Healthcare" 2021, no. 9.
23. Pietraś M., *Bezpieczeństwo zdrowotne jako wymiar bezpieczeństwa międzynarodowego*, „Atheneum. Polskie Studia Politologiczne" 2023, vol. 78(2), strony?.
24. Preparedness for COVID-19 vaccination strategies and vaccine deployment, Communication from the Commission to the European Parliament and the Council, COM(2020) 680 final, Brussels, 15.10.2020.
25. Report on pharmacovigilance tasks. From EU Member States and the European Medicines Agency (EMA) 2019-2022, EMA 142695/2023, European Medicines Agency 2023.
26. Riedel R., *Europeizacja polityki zdrowotnej na przykładzie zdrowia w miejscu pracy*, [in:] *Wokół teoretycznych i praktycznych aspektów stosunków międzynarodowych*, eds. Kubin T., Łapaj-Kucharska J., Okraska T., Kartowice 2020, strony?.
27. Sikorski J., *Social Implications of Infodemic Concurrent with COVID-19*, "Polish Political Science Yearbook" 2023, no. 52(4), pp. 79-89.
28. Tackling COVID-19 disinformation – Getting the facts right. Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions, High Representative Of The Union For Foreign Affairs And Security Policy, JOIN(2020) 8 final, Brussels, 10.6.2020.
29. Wathion N., *EMA'S Response to The Covid-19 Pandemic. Putting People's Health First*, European Medicines Agency, August 2023.
30. Wrześniewska-Wal I., Korporowicz-Żmichowska V., *Rezylientność i adaptacyjność polityki zdrowotnej w czasach zagrożeń egzystencjalnych: Studium na przykładzie kadry medycznej*, „Studia z Polityki Publicznej" 2024, vol. 11, no. 4.

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 345–362

ISSN 2543-6961
e-ISSN 2720-3093

Oliwia Radkiewicz
ORCID: 0000-0002-7324-5821
Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim

Social Resilience and Social Security in the Face of Disasters: A Case Study of the 2024 Flood in Poland

Odporność społeczna a bezpieczeństwo społeczne w obliczu katastrof: studium przypadku powodzi w Polsce w 2024 roku

Abstract
The article examines the social and institutional impacts of the September 2024 flood in southwestern Poland, focusing on social resilience. Using qualitative data from four semi-structured interviews with affected residents and a crisis-management expert, the study identifies multidimensional consequences: material damage, psychological distress, and social tensions linked to insufficient coordination of institutional support. Procedural barriers to compensation disproportionately affected residents of smaller communities and people with lower educational attainment, weakening perceptions of safety and trust in public institutions. While community self-organization, mutual aid, and local solidarity helped mitigate losses, they were insufficient to offset the disaster's full effects. The article recommends improving early-warning systems, simplifying aid procedures, expanding professional psychological support, strengthening community-based initiatives, and modernizing flood-protection infrastructure. Findings are preliminary due to the small sample.

Keywords: social security, flood, natural disasters, climate change, citizen safety, social resilience

Abstrakt
Artykuł analizuje skutki społeczne i instytucjonalne powodzi, która dotknęła południowo-zachodnią Polskę we wrześniu 2024 roku, ze szczególnym uwzględnieniem odporności społecznej. Celem badania była ocena wpływu katastrofy na lokalne społeczności oraz roli solidarności i zdolności adaptacyjnych w łagodzeniu jej skutków. Badania jakościowe przeprowadzono w oparciu cztery półustrukturyzowane wywiady z osobami poszkodowanymi oraz ekspertem ds. zarządzania kryzysowego. Wyniki ujawniły wielowymiarowe konsekwencje – od strat materialnych, przez zaburzenia psychiczne, po napięcia społeczne wynikające z niewystarczającej koordynacji pomocy instytucjonalnej. Bariery proceduralne w dostępie do odszkodowań szczególnie dotykały mieszkańców mniejszych miejscowości i osoby z niższym wykształceniem, wpływając na poczucie bezpieczeństwa i zaufanie do instytucji publicznych. Badanie podkreśliło znaczenie odporności społecznej – samoorganizacji, wzajemnej pomocy i solidarności lokalnych wspólnot – choć nie wystarczała ona do całkowitego złagodzenia skutków katastrofy. Rekomendacje obejmują usprawnienie systemu wczesnego ostrzegania, uproszczenie procedur pomocowych, wprowadzenie profesjonalnego wsparcia psychologicznego oraz wzmacnianie inicjatyw społecznych, a także modernizację infrastruktury przeciwpowodziowej. Należy zaznaczyć, że ze względu na niewielką próbę badawczą (cztery osoby) wyniki mają charakter wstępny i ograniczony, co należy uwzględnić przy interpretacji wniosków.

Słowa kluczowe: bezpieczeństwo społeczne, powódź, katastrofy naturalne, zmiany klimatu, bezpieczeństwo obywateli, odporność społeczna

Introduction

Social security can be defined as the ability of the state and its institutions, supported by social mechanisms, to ensure the protection of citizens' lives, health, and fundamental living conditions. The literature emphasizes that while the state possesses the institutional capacity to carry out these tasks, society—through solidarity, social capital, the activity of non-governmental organizations, and civic pressure—has the potential to support and co-shape the security system. In this perspective, social security constitutes one of the key challenges faced by contemporary states. According to the author of this article (whose assumptions are based on an analysis of the scholarly literature), social security—and in particular one of its components—deserves special attention. In the face of the growing pace of climate change and the intensification of extreme phenomena, ensuring the continuity of the functioning of local communities and limiting the impacts of natural disasters takes on strategic importance.

In the context of Poland, the author assigns particular significance to floods. Due to the country's geographical and hydrological conditions, they constitute the most serious threat among natural disasters. Poland lies within the catchment areas of the Vistula and Oder rivers, as well as several smaller rivers, whose flood surges—typical of a temperate climate and caused by heavy rainfall, snowmelt, or torrential downpours—have repeatedly led to catastrophic consequences. This is best illustrated by the so-called "millennium flood" of 1997 and the flood of 2010, both of which resulted in extensive material losses,[1] mass evacuations, and long-lasting economic and social repercussions.

The flood that struck southwestern Poland in September 2024 became one of the most serious challenges for the social security system in recent years. This disaster highlighted both the scale of threats arising from climate change and the vulnerability of institutions and local communities to their impacts. In the face of sudden hydrological events, not only do material losses occur, but also a weakening of citizens' sense of security, the emergence of trauma, and tensions within local communities. An analysis of the experiences of those affected, along with the actions of public institutions, provides deeper insight into the mechanisms of crisis management and allows for the identification of weaknesses within the existing system of protection against natural disasters.

[1] The millennium flood of 1997 caused losses exceeding PLN 22 billion (almost 2.4% of GDP), and just a decade later the 2010 flood generated damages amounting to approximately PLN 13.6 billion, or about 1% of GDP. Source: *Susza i powódź jednocześnie? Oto Polska w czasach zmiany klimatu*, https://ziemianarozdrozu.pl/susza-i-powodz-jednoczesnie-oto-polska-w-czasach-zmiany-klimatu/? [date of access: 1.08.2025].

This article advances the research hypothesis that the 2024 flood in Poland revealed significant shortcomings in the civil protection and crisis management system, which adversely affected the sense of social security, while at the same time highlighting the importance of social resilience and the solidarity of local communities. Accordingly, the following research question was formulated: how did the experiences of individuals affected by the 2024 flood, along with the actions of public institutions, influence the sense of social security, and what mechanisms may enhance societal resilience to future natural disasters?

Theoretical Approach to Social Security

In the contemporary world, human beings face the necessity of constructing security across multiple domains and levels—ranging from the safety of individuals and local communities, through the national and international dimensions, to social, ecological, global, economic, public, and military security. The diversity of needs associated with the sense of security, as well as the scale of accompanying threats, make the engagement of all available actors and resources possessed by modern states and societies increasingly indispensable in the process of shaping it.

Until recently, the category of "social security" was not present in research on national security. However, in the 2014 *White Book of National Security of the Republic of Poland*, it was identified as one of the four fundamental domains of security, alongside defense, protective, and economic security. The issue of social security plays an important role in the state's strategic planning, which is reflected both in the *National Security Strategy of the Republic of Poland 2014* and in the 2020 Strategy. The 2014 document emphasized that the overarching objective of the state in this area is to ensure a rapid and tangible improvement in the quality of citizens' lives. This requires the implementation of an active social policy, encompassing poverty reduction, the mitigation of social exclusion, the increase of real incomes across all social groups, and the reduction of unemployment. The activities of state institutions are also aimed at counteracting excessive social stratification and reducing disparities in the development of individual regions.[2] At the same time, the fourth pillar of the 2020 Strategy underscores the crucial importance of environmental protection. It's very title—*Social and Economic Development. Environmental Protection*—indicates the centrality of this domain within national security. The fourth pillar stresses that issues related to environmental protection, including climate change and natural disasters, remain

[2] *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2014*, pp. 38-40, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf [date of access: 1.08.2025].

a priority and constitute an integral part of state security policy, closely linked to processes of social and economic development.[3]

Social security encompasses a broad range of legal and organizational measures undertaken by state entities, non-governmental organizations, and citizens themselves, aimed at ensuring an adequate standard of living for individuals, families, and social groups, as well as preventing their marginalization and social exclusion. In the scholarly literature, social security is also understood as the deliberate actions of the state designed to create existential conditions that guarantee at least the maintenance of citizens' existing standard of living. This includes support for individuals who are temporarily or permanently unable to engage in professional work and who find themselves in difficult life circumstances due to personal incapacity or events beyond their control, such as fires, floods, or other natural disasters.[4]

According to Marek Leszczyński, the expansion of the state's security scope to include a social dimension stem from the very nature of the modern democratic state, whose fundamental duty is to care for its citizens—regardless of their material status—and to ensure them genuine opportunities for participation in social life. Leszczyński emphasizes that the economic "disempowerment" of large segments of the population leads to the transformation of democracy into a façade system, in which democratic institutions become inaccessible to broad social groups.[5]

Supporting individuals in difficult life circumstances, regardless of the causes of their problems, constitutes a cornerstone of social security. However, the mere provision of support is insufficient—the system must also account for various social threats, commonly defined as situations within society in which negative phenomena and processes intensify, leading to the violation of fundamental existential values and significant interests of the nation and the state. Due to their broad scope, intensity, and long-lasting effects, these threats increasingly take on a global character, transcending national and continental boundaries, with consequences affecting all of humanity. Among the most pressing contemporary threats are those related to the natural environment, such as climate change, lack of access to potable water, deforestation of tropical forests, and excessive exploitation of natural resources. Individuals affected by such issues often find themselves in critical life situations, resulting in a weakened sense of security and existential stability.

[3] *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2020*, pp. 30-35, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [date of access: 01.08.2025]..

[4] M. Leszczyński, *Bezpieczeństwo socjalne jako obszar zainteresowania badawczego i składnik bezpieczeństwa państwa*, [in:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, ed. M. Lisiecki, Warszawa 2008, pp. 543–558.

[5] M. Leszczyński, *Kształtowanie bezpieczeństwa społecznego przez państwo,* "Prace naukowe uniwersytetu ekonomicznego we Wrocławiu" 2010, no. 102, p. 189.

In the context of social security, it is worth referring to two significant theoretical approaches: the theory of social resilience and crisis management. The former emphasizes the capacity of individuals, groups, and entire communities to adapt, overcome difficulties, and recover after experiencing crises such as natural disasters, conflicts, or sudden socio-economic changes. Resilience thus highlights the need to develop mechanisms that strengthen social self-sufficiency, solidarity, and the ability to rapidly regenerate.[6] However, as Janusz Ziarko notes in the journal *Bezpieczeństwo. Teoria i Praktyka*, communities are unable to precisely predict when a threat will occur, its course, or its consequences for people, infrastructure, or the natural environment. Under such conditions, building social resilience—the ability to adapt, respond, and recover in uncertain and dynamic situations—appears more appropriate.[7]Crisis management, on the other hand, focuses on the planning, organization, and coordination of state and social institution actions in the face of threats. It encompasses both the prevention of crises and responses to them, as well as post-crisis recovery. These two approaches are mutually complementary: social resilience enhances the capacity of individuals and communities to cope with the consequences of crises, while crisis management provides institutional and organizational frameworks for the effective protection of social security.

Social resilience enhances the capacity of individuals and communities to cope with the consequences of crises, while crisis management provides the institutional and organizational frameworks necessary for the effective protection of social security. An example of this correlation can be observed in flood situations within small communities: residents may independently organize temporary levees and safeguard their homes, demonstrating social resilience; however, they are unable to predict the scale or timing of the flood. It is precisely the crisis management system—through hydrological warnings, evacuation plans, and state support—that enables coordinated protective actions, minimizing the impacts of the disaster. Consequently, social resilience and crisis management form a synergistic mechanism: the former allows for rapid and flexible responses at the local level, while the latter ensures security on a systemic scale, providing planning, resources, and coordination where grassroots community initiatives may prove insufficient.

The literature emphasizes that social resilience is a multidimensional process encompassing the capacities of individuals and groups as well as

[6] J. Ziarko, *Uwarunkowania zarządczego podejścia do społecznej odporności na zagrożenia kryzysowe*, "Bezpieczeństwo. Teoria i Praktyka" 2024, no. 4, pp. 137-140.

[7] Ibidem, pp. 150-151.

broader mechanisms of community functioning.[8] Resilience is not understood as a static attribute but rather as a set of dynamic resources—social, economic, informational, and institutional — that enable communities to adapt to changing threat conditions.[9] Within this perspective, communities are resilient not because they avoid hazards, but because they are able to transform available resources into effective coping strategies.

Scholars also highlight the relationship between resilience, vulnerability, and adaptive capacity. As Norris and colleagues argue, resilience emerges from the interaction between reducing vulnerability and strengthening adaptive capacities: the more effectively local support networks function and the more transparent risk communication is, the stronger the resulting resilience mechanisms.[10] In the context of natural disasters, this means that the effectiveness of community responses depends both on their internal organization and on the extent to which public institutions are capable of supporting recovery processes. The authors further emphasize that resilience is embedded in social and institutional systems that enable the flow of information, coordination of actions, and mobilization of resources.[11] This implies that social resilience and crisis management operate in close interdependence: the former is rooted in bottom-up cooperation and solidarity, while the latter provides planning, anticipation, and organizational structures essential for protective actions.

Natural Disasters and Social Security

In the event of a natural disaster resulting in loss of human life and significant damage to infrastructure, a high degree of societal and resource vulnerability to such threats becomes evident. The escalation of losses generated by natural disasters—borne not only by local communities but also by the financial and insurance sectors as well as state structures—highlights the multidimensional nature of vulnerability. This encompasses not only economic and financial consequences but also social and political implications, underscoring the complexity and systemic scope of the impact of natural disasters. Natural disasters exert a destructive and long-lasting effect on the emotional well-being of communities. This impact is heterogeneous, meaning that certain social groups experience its consequences more intensely and over a longer duration compared to others. According to

[8] F.H. Norris, S.P. Stevens, B. Pfefferbaum, K.F. Wyche, R.L. Pfefferbaum, C*ommunity Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness*, "American Journal of Community Psychology" 2008, no. 41, p. 127.

[9] Ibidem, p. 131.

[10] Ibidem, p. 134.

[11] Ibidem, p. 139.

the author, a significant example is provided by hurricanes in the United States which, like floods in Poland, are characterized by a large scale of impact, causing severe damage to infrastructure, material losses, as well as profound social and psychological consequences. Their analysis makes it possible to understand how extreme phenomena affect both infrastructure and the social and psychological spheres, while at the same time revealing the differentiated emotional resilience of individual communities.

In the event of a natural disaster resulting in the loss of human life and significant damage to infrastructure, a high level of societal and resource vulnerability to such hazards becomes apparent. The escalation of losses caused by natural disasters—borne by local communities as well as the financial and insurance sectors and state institutions—reveals the multidimensional nature of vulnerability. This encompasses not only economic and financial consequences but also social and political implications, highlighting the complexity and systemic scope of the impact of natural disasters. Such events exert a destructive and long-term effect on the emotional well-being of affected communities. The impact is heterogeneous, meaning that certain social groups experience its consequences more intensely and over a longer duration compared to others.

Research by Bathina, ten Thij, and Bollen (2022)[12] indicates that hurricanes in the United States, such as Irma, Harvey, Florence, and Dorian, exerted a significant impact on the emotional well-being of affected communities. Analysis of geo-located content published on social media revealed a marked decline in positive sentiment both prior to and during the occurrence of these natural disasters, reflecting a deterioration in collective mood. Although, in most cases, recovery to pre-disaster levels occurred relatively quickly—typically within one to two weeks—substantial variability was observed across different communities. Some communities experienced a deeper and more prolonged decline in well-being, confirming the existence of heterogeneous levels of emotional resilience. The authors define emotional resilience as the capacity to restore emotional equilibrium following a negative shock, measured by the time required to return to the pre-disaster state (time to recovery). The findings underscore that hurricanes pose not only material and infrastructural threats but also exert significant social and psychological effects.[13]

[12] K. Bathina, M. ten Thij, M. J. Bollen, *Quantifying societal emotional resilience to natural disasters from geo-located social media content*, https://arxiv.org/pdf/2204.13210 [date of access: 15.08.2025].

[13] contentIbidem, pp. 6–10.

The experience of hurricanes can have serious consequences for the mental health of communities, leading to disorders such as post-traumatic stress disorder (PTSD), depression, and anxiety. Research conducted by the University of California among residents of Florida affected by Hurricanes Irma and Michael indicates that not only direct exposure to these disasters but also their media coverage can exacerbate health problems. This phenomenon is particularly pronounced among women, who, due to socio-economic factors, are more vulnerable to negative psychological effects. The increasing frequency of hurricanes associated with climate change may further amplify anxiety and uncertainty within society.[14]

Research conducted by the University Centre for Rural Health in Lismore indicates that the 2017 floods in the northern region of New South Wales had severe consequences for the mental health of affected communities. Individuals who were forced to leave their homes for more than six months were twice as likely to experience symptoms of depression, anxiety, and PTSD compared to those who were displaced for a shorter period. Furthermore, individuals whose homes, businesses, and communities were impacted by the flooding were six times more likely to report long-term PTSD. The findings suggest that reducing the duration of forced displacement and ensuring social support and community engagement are critical for safeguarding mental health.[15]

The flood in Benue State, Nigeria, which occurred in September 2017, had severe social consequences, affecting over 100,000 people across 21 of the 23 local government areas. Homes, agricultural fields, roads, and public infrastructure were inundated, resulting in mass displacement of the population. Many residents were forced to seek shelter with relatives or in refugee camps, where living conditions were difficult and access to basic services was limited. The destruction also impacted the agricultural sector, which constitutes the primary source of livelihood for many families in the region. The lack of effective response from central and local authorities exacerbated feelings of neglect and marginalization among the communities affected by the disaster.[16]

In summary, natural disasters exert a multidimensional and long-lasting impact on society, encompassing both material and psychosocial domains. Infrastructural

[14] A. England, *The Psychological Toll of Repeat Hurricane Exposure Should Not Be Overlooked. Strong winds wear down our resilience*, https://www.verywellmind.com/exposure-to-hurricanes-can-be-bad-for-mental-health-8727216?utm [date of access: 15.08.2025].

[15] *Floods expose social inequities, and potential mental health epidemic in its wake*, https://www.sydney.edu.au/news-opinion/news/2022/03/23/floods-expose-social-inequities--and-potential-mental-health-epi.html? [date of access: 16.08.2025].

[16] M. Ade, *The menace of floods in the Benue Trough and vulnerability analysis: 2017 Flood*, "Geophysical Research Abstracts" 2018, no. 4, pp. 8-13.

and economic losses are accompanied by negative mental health consequences, including the occurrence of PTSD, depression, and anxiety, with the severity of these effects varying according to the emotional resilience of individual communities. Those particularly vulnerable include individuals displaced for extended periods, women, and communities dependent on agriculture and local infrastructure. A lack of adequate social support and governmental response further exacerbates feelings of marginalization and uncertainty. The findings indicate that effective measures in preparedness, the reduction of displacement duration, and the promotion of social resilience are critical for mitigating the adverse effects of natural disasters on society.

The 2024 Flood in Poland – Background and Course of Events

The flood that affected the southwestern regions of Poland in September 2024 constituted an extreme hydrological event with meteorological, geomorphological,[17] and anthropogenic origins. The immediate cause of the event was a Genoese low-pressure system moving across Central Europe, which triggered intense and prolonged rainfall. Within three days, some areas of the Lower Silesian, Opole, and Silesian voivodeships recorded precipitation totals exceeding 400 mm, significantly surpassing the average monthly rainfall for the region. This flood was one of the most severe hydrological phenomena in the country's history. The event was transboundary in nature, also affecting other Central European countries such as Austria, the Czech Republic, Romania, Slovakia, Hungary, and Germany.

The flood was also caused by the specific topography of southern Poland, characterized by a dense river network and limited natural retention, which contributed to a rapid rise in water levels in both mountain and lowland rivers. Flood embankments and retention reservoirs, which in some locations were outdated or not adapted to extreme flows, were unable to effectively contain the runoff from the heavy rainfall.

The flood primarily affected the southwestern part of the country. The greatest losses were recorded in the Lower Silesian, Opole, and Silesian voivodeships, where intense and prolonged rainfall led to a rapid rise in water levels within the Oder River basin and its tributaries, resulting in numerous inundations and infrastructure damage. The scale of the phenomenon was, however, broader, as the flood also impacted the Lubusz voivodeship, where local breaches of flood embankments, disruptions to transportation, and the necessity of conducting evacuation operations were reported.

[17] Relating to geomorphology, that is, the study of landforms, their structures, the processes of their formation, and the changes occurring on the Earth's surface.

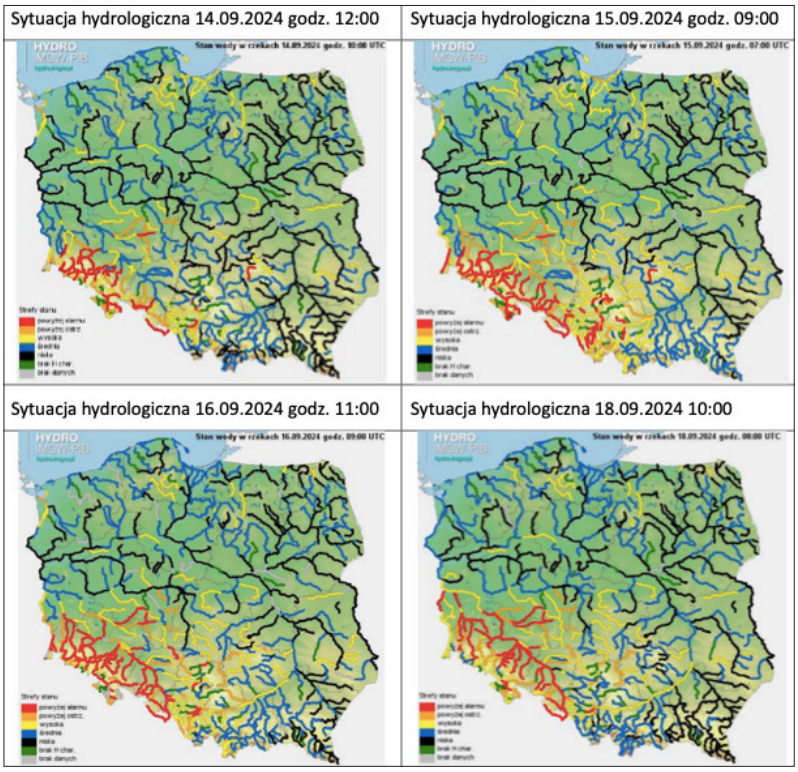

Figure 1. Map 1: Hydrological situation on September 14, 15, 16, and 18, 2024

Source: *Raport z przeglądu i aktualizacji wstępnej oceny ryzyka powodziowego w 3 cyklu planistycznym. Załącznik nr 7. Powódź we wrześniu 2024 [Report on the review and update of the preliminary flood risk assessment in the third planning cycle. Appendix No. 7. Flood in September 2024]*, p. 13.

In the first days of September 2024, intense rainfall associated with the Genoese low "Storm Boris" caused a rapid rise in smaller watercourses in south-western Poland, particularly in the Lower Silesian and Opole voivodeships. On September 12–13, local inundations occurred because of rivers Odra and Vistula exceeding alarm levels, and partially breached flood embankments necessitated the evacuation of residents. On September 14–15, the situation escalated, with water levels reaching catastrophic levels, resulting in widespread destruction of infrastructure, including roads, bridges, and power lines, as well as a significant number of people being forced to leave their homes. The intervention of emergency services, including the military and humanitarian organizations, was essential but at times delayed or constrained by logistical limitations, which heightened stress and the sense of threat among the affected population. Simultaneously, the Silesian voivodeship experienced damage to industrial and agricultural areas,

while the Lubusz voivodeship faced inundations on a smaller scale. In response to the crisis, on September 16, the Council of Ministers declared a state of natural disaster,[18] and rescue services—including the military and humanitarian organizations—initiated emergency and relief operations, which continued over the following weeks, alongside damage assessments and reconstruction planning.

The consequences of the 2024 flood in Poland affected four voivodeships: Lower Silesian, Opole, Silesian, and Lubusz. The disaster had a multidimensional impact—significant losses were recorded in economic activity, including the agricultural, industrial, and service sectors, as well as in transport and municipal infrastructure. At the same time, the flood had serious environmental consequences, leading to water pollution, soil erosion, and the destruction of green areas and local ecosystems. Most dramatically, however, the human population was affected—both in terms of physical health and daily life. Evacuations, the destruction of homes, and limited access to basic medical and sanitation services increased the risk of disease, injury, and post-traumatic stress. As a result of the flood, nine people lost their lives, highlighting the direct threat to the life and health of residents in the affected regions.

Table 1. Number of affected individuals and flooded buildings during the September 2024 flood in each voivodeship

Województwo	**śląskie**	**opolskie**	**lubuskie**	**dolnośląskie**
Liczba osób poszkodowanych	21 226	33 902	5 623	177 294
Liczba zalanych budynków mieszkalnych	156	192	430	9 744
Liczba zalanych budynków o znaczeniu społecznym	124	167	10	513

Source: *Raport z przeglądu i aktualizacji wstępnej oceny ryzyka powodziowego w 3 cyklu planistycznym. Załącznik nr 7. Powódź we wrześniu 2024 [Report on the review and update of the preliminary flood risk assessment in the third planning cycle. Appendix No. 7. Flood in September 2024]*, p. 30.

The table above presents the scale of human and material losses in the four voivodeships most affected by the September 2024 flood. The data reveal a clear disparity between regions—both in terms of the number of affected individuals and the extent of infrastructural damage. The highest number of victims was recorded in the Lower Silesian Voivodeship (177,294), confirming that it was the area most severely impacted by the disaster. It is followed by the Opole Voivodeship

[18] It remained in effect for 30 days, covering selected areas of the Lower Silesian, Opole, and Silesian voivodeships. As the situation developed further, the state of natural disaster was extended to additional counties and municipalities, with its scope updated on September 17 and 25, 2024. Ultimately, on October 15, 2024, the Council of Ministers decided to lift the state of natural disaster, citing the stabilization of weather conditions and the effective assistance provided to the affected population.

(33,902), the Silesian Voivodeship (21,226), and the Lubusz Voivodeship (5,623). A similar pattern is visible in the figures concerning residential buildings: in Lower Silesia, as many as 9,744 structures were flooded, significantly exceeding the numbers in the remaining regions. As for socially significant facilities (e.g., schools, healthcare centers, and care institutions), Lower Silesia also dominates (513).

The September 2024 flood disaster clearly revealed significant deficiencies in the existing flood protection systems, both in terms of hydraulic infrastructure and crisis management procedures. The scale and intensity of the event indicate that enhancing the country's resilience to future hydrological disasters requires strengthening both technical protection mechanisms, such as flood embankments, retention systems, and hydrological monitoring, and social adaptive mechanisms. Of particular importance is the cooperation between local communities and state institutions—through education, the development of evacuation plans, the preparation of crisis points, and the enhancement of early warning systems. The combination of technical and social efforts not only enables more effective mitigation of flood impacts but also increases adaptive capacity and social resilience in the face of dynamically changing hydrological threats.

Methodology of the Author's Research

The objective of the conducted research was to explore the experiences and perceptions of individuals affected by the September 2024 flood, as well as to understand the actions of institutions responsible for disaster response. The sample was purposively selected and consisted of two main groups of respondents: individuals directly impacted by the flood and experts with knowledge and experience in crisis management. Within the group of flood-affected individuals, three residents from smaller towns in southwestern Poland were included — one resident of Jelenia Góra (38 years old, cleaner), one resident of Szprotawa (28 years old, mechanic), and one resident of Kłodzko (43 years old, nurse). The expert group also comprised a former police officer from Jelenia Góra (57 years old) with experience in emergency response during natural disasters (flood in Poland in 2010). The selection criteria for specific participants were based on their direct experience with flooding or practical knowledge in crisis management, allowing insights from both the residents' perspective and experts in the field of social safety.

The research was conducted using semi-structured interviews, which allowed for the collection of detailed information regarding respondents' experiences, opinions, and perceptions while also enabling flexible follow-up questions

depending on the course of the conversation.[19] The semi-structured format facilitated the gathering of rich qualitative data encompassing material, psychological, and social impacts of the flood.

Data analysis was based on content analysis and thematic categorization. The interviews were transcribed and subjected to careful reading to identify recurring themes and patterns. The analysis resulted in the identification of key categories, including experiences related to property loss, the impact of the flood on daily life, the assessment of public institutions' effectiveness, and the effects of the disaster on respondents' health and sense of security. These categories enabled a systematic organization of observations and allowed for a comparison between residents' experiences and the expert perspective.

Data were collected using semi-structured interviews, which allowed for the elicitation of in-depth narratives regarding experiences related to the 2024 flood. Each interview lasted between 40 and 60 minutes and was conducted individually under conditions ensuring participants' safety and comfort. Following the interviews, detailed transcripts and research notes were prepared, forming the basis for further analysis. The empirical material was then systematically processed: the researcher produced precise transcriptions of the interviews based on the notes and subsequently coded them using an inductive approach, enabling the emergence of analytical categories without imposing pre-established frameworks. The coding process involved identifying recurring themes, categorizing them, and interpreting them in the context of material, psychological, and social experiences. This approach ensured transparency and methodological rigor while safeguarding participants' privacy and confidentiality.

It should be emphasized that the research sample was very small, consisting of two directly affected individuals and one expert. This selection allowed for an in-depth understanding of individual experiences but does not permit the formulation of generalized conclusions applicable to entire communities affected by the flood. The results should be treated as an exploratory case study highlighting key areas for further, broader research.

The selection of Jelenia Góra, Szprotawa, and Kłodzko was based on their location in regions particularly affected by the September 2024 flood. These towns represent diverse conditions—Jelenia Góra as a medium-sized city, Szprotawa as a smaller local town, and Kłodzko as a regional center—enabling the capture of various social and organizational perspectives in the face of the same disaster.

[19] M. Żelazo, *Kwestionariusz wywiadu jako narzędzie badawcze*, "Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2013, no. 2 (6), pp. 222-238.

Findings: Perspective of Flood-Affected Individuals

Analysis of the interviews conducted in Jelenia Góra, Szprotawa, and Kłodzko indicates that the experience of the 2024 flood had both material and deeply psychological and social dimensions. In the initial phase—just before the water arrived—residents reported feelings of uncertainty and disbelief. As one resident of Jelenia Góra noted: *"It rained all morning, but this is Lower Silesia—rain is normal. Only in the evening did the water start to seep into the basement, and the children were screaming as the furniture floated on the water."* A similar shock was described by a resident of Szprotawa: *"During the night, water entered our house, the car sank in mud, and my wife, children, and I had to flee on foot to friends in higher areas."* These accounts indicate that the peak of the event was associated with panic, a sense of helplessness, and intense stress—even among those with prior crisis management experience. A retired police officer from Jelenia Góra emphasized: *"As a former officer, I thought I knew how to react, but seeing my grandchildren crying in my arms, I felt emptiness and fear."* Residents simultaneously highlighted the critical role of emergency services in the initial response phase. One participant reported: *"The fire brigade arrived the fastest, and overall, the services performed well, considering the confrontation with such a violent natural force."* This juxtaposition illustrates the dual dynamics of the experience—initial mobilization and the effectiveness of intervention efforts contrasted with later disappointment arising from bureaucratic procedures and unequal access to assistance.

The subsequent phase—the first days and weeks following the flood—was characterized by shock, a sense of chaos, and institutional disorganization. The assistance provided by emergency services was highly valued, although gaps in coordination and information flow were noted. As a resident of Kłodzko stated: *"The hospital was partially flooded as well, and among the residents there was a sense that everyone was fighting alone—some provided generators, others offered food, but underlying it all was fear: what comes next?"* As the weeks progressed, feelings of frustration emerged, linked to bureaucracy and unequal access to aid. A resident of Szprotawa observed: *"The compensation application is a stack of papers, and people began to argue because some received aid quickly while others got nothing, but the frustration is entirely understandable."* Material losses were particularly painful—houses in many towns became uninhabitable, requiring drying and long-term renovations. As a resident of Jelenia Góra emphasized: *"Our house was full of mud and stench; everything—from the refrigerator to the children's books—was destroyed. Looking at it, I felt as if my whole life had to start over."* After the flood subsided, residents had to confront the consequences

of their homes being inundated and the loss of property. These difficult material experiences were accompanied by emotional strain resulting from the necessity of staying with relatives or friends for an extended period. As a resident of Kłodzko described: *"It was tragic to witness my own belongings destroyed, and it was frustrating to stay with family for so long, even though I felt fortunate, because not everyone had somewhere to go."* This statement illustrates the ambivalence of emotions—simultaneously experiencing loss and discomfort on one hand, and a sense of gratitude and solidarity on the other.

The analyzed narratives also reveal significant psychological and social consequences. Reports of insomnia, anxiety about future rainfall, and emotional problems among children were recurrent. Simultaneously, strong neighborhood solidarity was evident during the initial phase, although over time it began to give way to tensions and conflicts. As a retired police officer summarized: *"The community, which was once tightly knit and fought to protect the city by building flood embankments with their own hands, began to fragment, and the images of flooded homes kept returning at night."* A critical issue was the barriers to accessing psychological support, which stemmed less from availability than from entrenched social stereotypes and fears. As one resident of Szprotawa noted: *"I could have done it even over the phone, but I wasn't fully convinced… I kept worrying about what people would think, and eventually I gave up."* Such attitudes limited the effectiveness of available assistance and exacerbated social consequences. These accounts indicate that the impacts of the flood extended far beyond material losses, encompassing lasting changes in well-being, social relationships, and individuals' sense of security. Insights drawn from these narratives highlight the need to implement more effective early warning systems, improve communication between institutions and residents, and provide professional psychological support following natural disasters.

The experiences of residents from the studied towns align with findings in the literature on the consequences of natural disasters. Research on floods and other catastrophic events indicates that victims often go through three phases of response: a phase of disorientation and denial, a phase of mobilization and short-term social solidarity, and a phase of long-term consequences, including fatigue, frustration, and decreased trust in institutions.[20]

Accounts from residents of Jelenia Góra, Szprotawa, and Kłodzko illustrate the typical "dual-face" mechanism of social responses: on one hand, there is intense cooperation and communal solidarity, while on the other, conflicts over

[20] D. E. Alexander, *Natural Disasters*, London 2018, pp. 315 -318.

resources and inequalities in access to aid emerge.[21] Consistent with studies on the mental health of disaster victims, reported symptoms—such as insomnia, post-traumatic anxiety, and heightened vigilance toward subsequent rainfall—fall within the spectrum of disorders referred to as flood trauma.[22] At the same time, respondents emphasized inadequate coordination of institutional assistance, which, according to the literature, is a key factor exacerbating feelings of helplessness and prolonged stress.[23] The analysis of their narratives therefore confirms that effective crisis management should encompass not only infrastructural and material aspects but also social and psychological components, which are crucial for the community's resilience in the face of future crises.

Conclusions

Analysis of the research material indicates that the 2024 flood had a multidimensional impact on the lives of residents in southwestern Poland. On one hand, it caused material losses, including the destruction of homes and infrastructure; on the other, it resulted in significant psychological consequences, including feelings of helplessness, post-traumatic stress, and prolonged stress. In the initial phase of the crisis, strong social mobilization and neighborhood solidarity were evident, though over time these gave way to tensions and conflicts arising from limited access to assistance and growing frustration.

The research revealed significant deficiencies in the institutional system, including a lack of coherent coordination and excessive bureaucracy in the process of granting compensation. Despite the effective intervention of emergency services in the initial phase, subsequent actions did not provide residents with a sufficient sense of security. Procedural barriers were particularly burdensome for individuals from smaller towns or with lower educational levels—for example, rural residents with only primary education—who faced considerably greater difficulties in submitting applications and navigating the complex administrative system compared to those with higher education. Such disparities in administrative competencies directly affected subjective perceptions of safety and the ability to access state support. Additionally, the lack of adequate psychological support exacerbated the social and health consequences of the disaster.

In the context of the 2024 flood, it is evident that social resilience and crisis management operate in conjunction. Grassroots self-organization by residents—

[21] R. R. Dynes, *Organized Behavior in Disaster*, Lexington 2006, pp. 45–50.
[22] S. Tapsell, S. Tunstall, *The Health Impacts of Flooding: Traumatic Responses and Psychological Effects*, London 2008, pp. 112–118.
[23] K. Tierney, *Disaster Governance: Social, Political, and Economic Dimensions*, New York 2014, pp. 87–92.

for example, constructing temporary protective measures or providing mutual assistance—serves as an example of social resilience. At the same time, the unpredictability of the scale and dynamics of the disaster underscores the necessity of systemic crisis management measures, such as early warning, evacuation coordination, and institutional support. It is precisely this synergy between local adaptive capacity and formal safety structures that enables more effective responses to hazards and mitigates their long-term impacts.

At the same time, the findings confirmed the importance of social resilience—the capacity of residents to self-organize, provide mutual assistance, and rebuild their lives after the crisis—though this mechanism was not sufficiently strong to fully mitigate the long-term effects of the flood. The results also corroborate Marek Leszczyński's observations that social security is a cornerstone of genuine democracy, demonstrating that deficiencies in the support system following the 2024 flood led to feelings of marginalization and exclusion among certain citizens, which contradicts the fundamental democratic principle of societal equality.

The research further showed that individuals facing procedural barriers to accessing compensation or social assistance experienced reduced feelings of safety and lower trust in public institutions. A lack of fair and effective support weakened local community bonds, limited neighborhood cooperation, and reduced willingness to participate in civic activities. Empirical data thus confirm Leszczyński's theoretical proposition that the stability of democratic institutions and social cohesion largely depend on ensuring citizens' social security, and that deficits in this area can lead to the erosion of both social trust and state legitimacy.

In light of these analyses, it is necessary to implement a range of measures aimed at improving the functioning of the social security system in the face of natural disasters. First, the early warning system should be strengthened, and communication between public institutions and citizens improved, allowing residents to respond more quickly to imminent threats. At the same time, assistance and compensation procedures should be simplified and standardized to prevent situations that generate feelings of injustice and frustration among affected individuals.

A key area of action should also be the integration of professional psychological support into both emergency interventions and recovery processes, considering the needs of both adults and children, who are particularly vulnerable to the effects of disasters. Simultaneously, social resilience should be strengthened through support for local non-governmental organizations, mutual aid groups, and civic initiatives, which in the initial phase of a crisis can effectively complement state efforts and mitigate the limitations arising from barriers to formal psychological support.

Lastly, though peripheral to this study, the modernization of flood protection infrastructure remains a relevant consideration. Increasing water retention, reinforcing embankments, and adapting retention reservoirs to extreme weather events could significantly reduce material and social losses in the future. It should be noted, however, that this recommendation requires separate, in-depth analysis, as the present study focused primarily on the social and psychological aspects of the 2024 flood.

Referency

1. Ade M., *The menace of floods in the Benue Trough and vulnerability analysis: 2017 Flood*, "Geophysical Research Abstracts" 2018, no. 4.
2. Alexander D. E., *Natural Disasters*, London 2018.
3. Bathina K., ten Thij M., Bollen M. J., *Quantifying societal emotional resilience to natural disasters from geo-located social media content*, https://arxiv.org/pdf/2204.13210.
4. Dynes R. R., *Organized Behavior in Disaster*, Lexington 2006.
5. England A., *The Psychological Toll of Repeat Hurricane Exposure Should Not Be Over-looked. Strong winds wear down our resilience*, https://www.verywellmind.com/exposure-to-hurricanes-can-be-bad-for-mental-health-8727216?utm.
6. *Floods expose social inequities, and potential mental health epidemic in its wake*, https://www.sydney.edu.au/news-opinion/news/2022/03/23/floods-expose-social-inequities-and-potential-mental-health-epi.html?.
7. Leszczyński M., *Bezpieczeństwo socjalne jako obszar zainteresowania badawczego i składnik bezpieczeństwa państwa*, [in:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, ed. M. Lisiecki, Warszawa 2008.
8. Leszczyński M., *Kształtowanie bezpieczeństwa społecznego przez państwo,* "Prace naukowe uniwersytetu ekonomicznego we Wrocławiu" 2010, no. 102.
9. Norris F.H., Stevens S.P., B. Pfefferbaum, Wyche K.F., Pfefferbaum R.L., C*ommunity Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness*, "American Journal of Community Psychology" 2008, no. 41.
10. Raport z przeglądu i aktualizacji wstępnej oceny ryzyka powodziowego w 3 cyklu planistycznym. Załącznik nr 7. Powódź we wrześniu 2024 [Report on the review and update of the preliminary flood risk assessment in the third planning cycle. Appendix No. 7. Flood in September 2024], https://powodz.gov.pl/www/powodz/aWORP/3W-12_Raport_WORP_20250320_v1.00.pdf.
11. *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2014*, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf.
12. *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2020*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.
13. *Susza i powódź jednocześnie? Oto Polska w czasach zmiany klimatu*, https://ziemianarozdrozu.pl/susza-i-powodz-jednoczesnie-oto-polska-w-czasach-zmiany-klimatu/?.
14. Tapsell S., Tunstall S., *The Health Impacts of Flooding: Traumatic Responses and Psychological Effects*, London 2008.
15. Tierney K., *Disaster Governance: Social, Political, and Economic Dimensions*, New York 2014.
16. Ziarko J., *Uwarunkowania zarządczego podejścia do społecznej odporności na zagrożenia kryzysowe*, "Bezpieczeństwo. Teoria i Praktyka" 2024, no. 4.
17. Żelazo M., *Kwestionariusz wywiadu jako narzędzie badawcze*, "Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2013, no. 2 (6).

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 363–380

ISSN 2543-6961
e-ISSN 2720-3093

Wiktoria Trybuł
ORCID:0000-0002-9363-5173
Akademia Sztuki Wojennej w Warszawie

Irregular Migration to the Member States of the European Union as a Challenge to National and Regional Security in the 21st Century

Nieregularna migracja do państw członkowskich Unii Europejskiej jako wyzwanie dla bezpieczeństwa narodowego i regionalnego w XXI wieku

Abstract
Irregular migration to the Member States of the European Union constitutes one of the key challenges to national and regional security in the twenty-first century. The intensification of migratory pressure, particularly after 2015, has exposed the limitations of existing migration management mechanisms as well as the complexity of threats related to border protection, public order, and the stability of asylum systems. The abstract analyses EU migration policy from legal, institutional, and operational perspectives, with particular emphasis on the New Pact on Migration and Asylum, return procedures, readmission mechanisms, and the role of the Frontex agency. The research hypothesis assumes a shift in priorities towards strengthened border control and cooperation with third countries, at the expense of internal solidarity mechanisms and human rights protection standards. The conclusions indicate a growing fragmentation of EU migration policy and the need to balance security interests with the norms of international law and the fundamental values of the European Union.

Keywords: migration, irregular migration, security, European Union

Abstrakt
Nieregularna migracja do państw członkowskich Unii Europejskiej stanowi jedno z kluczowych wyzwań dla bezpieczeństwa narodowego i regionalnego w XXI wieku. Nasilenie presji migracyjnej, szczególnie po 2015 roku, ujawniło ograniczenia dotychczasowych mechanizmów zarządzania migracją oraz złożoność zagrożeń związanych z ochroną granic, porządkiem publicznym i stabilnością systemów azylowych. W streszczeniu analizie poddano politykę migracyjną UE w ujęciu prawnym, instytucjonalnym i operacyjnym, ze szczególnym uwzględnieniem Nowego Paktu o Migracji i Azylu, procedur powrotowych, mechanizmów readmisji oraz roli agencji Frontex. Postawiona hipoteza zakłada przesunięcie priorytetów w stronę kontroli granic i współpracy z państwami trzecimi, kosztem solidarności wewnętrznej i standardów ochrony praw człowieka. Wnioski wskazują na postępującą fragmentaryzację unijnej polityki migracyjnej oraz potrzebę wyważenia interesów bezpieczeństwa z normami prawa międzynarodowego i wartościami UE.

Słowa kluczowe: migracja, nieregularna migracja, bezpieczeństwo, Unia Europejska

Introduction

Irregular migration constitutes one of the most serious challenges to the security of the Member States of the European Union in the 21st century. The increase in migration flows, particularly after 2015, has highlighted the limitations of existing migration management instruments and revealed the complexity of the threats associated with this phenomenon. The influx of persons crossing the external borders of the European Union without the required legal authorisation has become not only an operational issue, but also a political and social concern.

The so-called "migration crisis" of 2015 demonstrated this vividly: frontline states such as Greece and Italy were confronted with an unprecedented inflow of asylum seekers and migrants, which overwhelmed reception capacities and created severe challenges for asylum procedures. In Greece, the sudden arrival of over 850,000 migrants in 2015 alone exposed the structural deficiencies of both national institutions and the Common European Asylum System (CEAS), while in Italy the disembarkations on Lampedusa and Sicily became a symbol of the Union's limited preparedness.[1] These pressures translated into internal political polarisation, including the rise of parties such as *Alternative für Deutschland* in Germany or *Lega Nord* in Italy, which explicitly linked irregular migration with threats to internal security and cultural identity.[2] At the same time, the disproportionate burden placed on southern Member States exacerbated divisions within the Union, as reflected in the failure to implement the 2015 relocation mechanism, which was legally challenged by several Central European governments. The crisis thus revealed the vulnerability of the EU's solidarity principle and intensified disputes over burden-sharing, directly undermining the cohesion of the Union.

The aim of this article is to identify the principal challenges associated with irregular migration to the Member States of the European Union and to examine the measures undertaken by the Union in response to threats to security, public order, and the integrity of the external borders. Within the EU framework, the integrity of external borders is understood not in terms of territorial sovereignty in the classical sense of international law, but rather as the effective control, management, and protection of the Union's external frontiers as a shared responsibility under the Schengen system. The Schengen Borders Code requires Member States to exercise such control in a manner that guarantees both security and the free movement of persons within the Union. In contrast to earlier scholarship that focused primarily on the 2014–2016 migration crisis, this paper extends the temporal scope to 2021–2025

[1] European Migration Network, *Annual Report on Migration and Asylum 2023 – Highlights*, European Commission, Brussels 2024, p. 33.

[2] C. Mudde, *The Far Right Today*, Cambridge 2019, pp. 4–7.

and situates irregular migration within the context of hybrid threats at the Union's eastern frontier and the gradual implementation of the New Pact on Migration and Asylum. The contribution of this study is twofold: first, it establishes a clear conceptual distinction between irregular border detections and asylum applications; second, it offers a concise comparative analysis of how two Member States have translated EU-level priorities into national practice under hybrid pressure.

Irregular migration challenges this integrity by undermining the effectiveness of border management systems, creating situations in which unauthorised crossings bypass formal entry procedures, thereby weakening the credibility of the EU's common legal framework. This phenomenon not only disrupts the functioning of the Schengen Area, as evidenced by the temporary reintroduction of internal border controls by several Member States since 2015, but it also raises questions about solidarity and trust between Member States, which are essential for the sustainability of the EU's border regime.

The research problem addressed in this study focuses on the extent to which the European Union's declared priorities in the field of irregular migration, including the reinforcement of border control instruments, return procedures and cooperation with third countries, as set out in documents such as the New Pact on Migration and Asylum, are being effectively implemented. The study also examines whether the institutional, legal and financial measures adopted at the EU and Member State levels are adequate to achieve these objectives, and how this shift in emphasis affects the balance between security considerations, intra-Union solidarity mechanisms and human rights protection standards.

This article is based on an analysis of European Union legal acts, strategic documents, statistical data (including Eurostat), and reports of EU institutions and international organizations. Before moving to the analysis of the EU's institutional and legal responses, it is necessary to clarify the terminology, as conceptual ambiguity often complicates both academic debate and political discourse on migration. The research applied a dogmatic-legal method, content analysis of policy documents, and a comparative analysis of solutions adopted within migration and asylum policy frameworks.

Terminological Aspects of Migration Issues

The precise definition of the phenomenon of migration constitutes a significant analytical challenge. This results primarily from the multidimensional and dynamic nature of migration processes, which are the subject of interest of many academic disciplines — ranging from demography, through sociology and political science,

to economics and security studies. The diversity of research approaches, differing operational definitions, and theoretical frameworks leads to the absence of a single, universally accepted definition of migration.[3] The term migration is the broadest concept and refers to the movement of populations within a given country or between different countries, aimed at changing the place of residence either permanently or temporarily,[4] driven by political, ethnic, religious, or economic factors.[5] Therefore, emigration can be defined as leaving one's homeland for material, religious, or political reasons and settling abroad. In this context, it is also important to address the issue of refugeeness. Under international law, a refugee is defined as a person who, "owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country; or who, not having a nationality and being outside the country of his former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling to return to it."[6]

The diversity of legal statuses of foreigners residing in a state of which they are not citizens constitutes a significant element of contemporary migration policy. This categorisation includes both individuals who migrate voluntarily — for employment, educational or family reasons — and those forced to leave their country of origin due to persecution, armed conflict, or humanitarian disasters. This category also encompasses the right to territorial asylum, which consists in "granting permission to enter and reside to foreigners who are discriminated against or persecuted for their beliefs, political activity, religious or scientific work. States have the discretion to grant asylum, which means that such a person cannot be subjected to extradition."[7]

The status of an asylum seeker in Poland is granted when it is necessary to ensure the protection of a foreign national and when it is justified by an important interest of the Republic of Poland.[8] The diversity of forms in which foreigners are present in the host state means that migration policy must take into account not only border and security issues, but also human rights, social integration, and

[3] S. Castles, H. De Haas, M. J. Miller, *The Age of Migration: International Population Movements in the Modern World*, Basingstoke 2014, pp. 28–30.

[4] According to the United Nations, short-term migration usually refers to stays between three months and one year, while long-term migration denotes residence exceeding twelve months. United Nations Statistics Division, *Recommendations on Statistics of International Migration*, Revision 1, UN, New York 1998.

[5] P. Lubiewski, *Nielegalna imigracja. Zagrożenia bezpieczeństwa część 1*, Szczytno 2016, p. 13.

[6] *Konwencja dotycząca statusu uchodźców sporządzona w Genewie dnia 28 lipca 1951r*. https://www.amnesty.org.pl/wp-content/uploads/2016/04/Konwencja_Dotyczaca_Uchodzcow.pdf [date of access: 20.06.2025].

[7] R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne. Wydanie 8 zmienione*, Warszawa 2005, p. 264.

[8] I. Malinowska, *Wymiar prawny uchodźctwa. Status uchodźcy z perspektywy praw człowieka*, [in:] *Uchodźcy w Europie. Uwarunkowania, Istota Następstwa*, eds. K.A. Wojtaszczyk, J. Szymańska, Warszawa 2017.

inter-institutional coordination. It is also important to define precisely what migration policy entails. Migration policy can be understood as the entirety of state actions related to the movement of people across space, both in the context of the admission of foreigners (immigration) and the policy towards its own citizens residing outside the country's borders — regardless of whether their stay is permanent or temporary. This policy includes measures concerning the integration of migrants, emigration policy, support for the return of nationals to their country of origin regardless of their legal status, as well as regulations related to the granting of citizenship[9].

The International Organization for Migration (IOM) defines migration policy as a set of legal norms, regulations, and measures established by states in order to manage migration flows. It encompasses matters related to the entry and stay of foreigners, their integration in the host country, as well as return to the country of origin and reintegration processes.[10] In public discourse, the concept of migration policy is often replaced by the term migration strategy. However, from a terminological perspective, policy is a broader concept from which strategy subsequently derives. This demonstrates that in EU law irregular migration is not only a legal category but also a policy instrument, shaping the scope of state obligations and the political framing of migration governance.

While the above categories capture the complexity of migration phenomena, the key concept for the purposes of this article is irregular migration. Within EU law, there is no single codified definition of irregular migration, but the term is used consistently across legal and policy documents. The Schengen Borders Code defines an "unauthorised crossing of the external border" as an entry outside authorised border crossing points or during unauthorised hours. Similarly, Directive 2008/115/EC on common standards and procedures in Member States for returning illegally staying third-country nationals uses the notion of "illegal stay" to describe the presence of a third-country national on the territory of a Member State without fulfilling the conditions of entry, stay or residence. In EU practice, therefore, irregular migration encompasses both illegal entry into the territory of the Union and illegal residence within it. This approach is complemented by the International Organization for Migration, which defines an irregular migrant as a person who enters or remains in a country without the necessary authorisation under national or international law.

[9] M. Duszczyk, *Ewolucja polskiej polityki migracyjnej w zakresie migracji zarobkowych po 1 maja 2004 r.*, [in:] *Migracje i polityka migracyjna. Polska w kontekście europejskim*, eds. M. Duszczyk, P. Kaczmarczyk, Warszawa 2013, pp. 19–21.

[10] International Organization for Migration (IOM), *Glossary on Migration*, „International Migration Law" 2019, no. 34, p. 146, https://publications.iom.int/system/files/pdf/iml_34_glossary.pdf [date of access: 10.06.2025].

Irregular Migration to the European Union as a Security Challenge for Member States in the 21st Century

In 2015, the European Union experienced a migration crisis.[11] In the media, this situation was portrayed as a refugee crisis or an asylum crisis. It should be emphasised that the European Union is once again facing the greatest challenge related to the influx of people since the end of the Second World War.[12] As a result, the term illegal migration or irregular migration has appeared in media discourse. In the academic literature, there is no consensus on a single clear definition of irregular migration. However, certain criteria have been adopted that help to structure the issue:

1. "the way irregularity arises (illegal border crossing, exceeding the permitted period of stay, refusal to apply for protection, breach of the obligation to leave the territory, unsuccessful deportation, birth of a child to parents with irregular status),
2. duration of stay (temporary or circular migration),
3. types of legal infringements (illegal entry, stay, or employment),
4. modes of migration (smuggling, trafficking, voluntary or forced irregular migration),
5. individuals and their motivations (family reasons, refugees, or unregulated labour migration.)[13]

The International Organization for Migration defines an irregular migrant as a person who enters or remains in the territory of a state in breach of that state's migration laws, regardless of the reasons for that situation.[14] This definition is particularly useful in the EU context, where the phenomenon is regulated through both international law and Union law, and where the distinction between "illegal entry" and "illegal stay" has direct policy consequences**.** The proposed definitions avoid terminology that could carry negative connotations and thereby provoke additional emotions within society.

In public discourse, particularly in the media, the term "illegal migration" is more commonly encountered and is often used as a tool for shaping a specific social narrative. This term is not neutral — it plays a role in constructing a particular image

[11] Crisis phenomena are an inherent element of the processes of European integration, and their increasing diversity and frequency result both from the hybrid nature of the European Union and from the exhaustion of the original visions and development strategies of the integration project, vide: K. A. Wojtaszczyk, J. Nadolska, J. F. Czub, *Kryzysy w procesie integracji europejskiej i sposoby ich przezwyciężania*, „Przegląd Europejski" 2014, no. 3(33), pp. 10–11.

[12] More precisely, it constitutes one of the greatest challenges in the domain of border security and societal cohesion, while other crises such as the financial downturn of 2008 or the COVID-19 pandemic posed different but equally systemic pressures.

[13] P. Lipold, *Nieregularna migracja do Unii Europejskiej. Tendencje i wyzwania*, Warszawa 2022, p. 30.

[14] International Organization for Migration (IOM), *Glossary on Migration*.., op. cit., p. 126.[date of access: 20.06.2025].

of the migration phenomenon, reinforcing associations with threats to public order or state security. In fact, from the perspective of international and EU law, the use of the term "irregular migration" is more appropriate, as it reflects the complexity of the legal situation of persons crossing borders without the required authorisation. Issues related to migration and in particular irregular migration have, for at least a decade, constituted one of the key areas of both internal and external policy of the EU Member States. This topic has also secured a lasting place in national and EU-level election campaigns, in which migration issues are used as a tool for mobilising the electorate. The practice of "fear-mongering" about migrants and refugees has, in many countries, become the norm in political rhetoric, serving to legitimise calls for tightening border policies and restricting the rights of foreigners. While irregular migration generates real challenges for border management and asylum systems, these risks are frequently amplified in political narratives, which present migration as an existential threat rather than a governance problem.

The European Union and its Member States are an attractive destination for migrants and refugees from various parts of the world, primarily from the Middle East, Africa, and Asia. Interest in particular EU countries varies, which is linked to the classic theory of migration push and pull factors. This theory divides the causes of migration into two groups: those that push people out of their place of residence and those that attract them to a new location.[15]

To better capture the scope of the phenomenon, it is important to distinguish between irregular border crossings and asylum applications. According to Frontex, more than 1.8 million irregular border crossings were detected in 2015, the highest number ever recorded in the EU.[16] Although the figures declined in subsequent years, they began to rise again in the early 2020s**,** indicating a renewed increase in migratory pressure rather than a new peak. These numbers illustrate the direct scale of unauthorised entries. However, they must be read together with asylum application figures, which reflect institutional pressures rather than border flows. The combined use of both indicators provides a fuller and more precise picture of migratory pressure.[17]

At the same time, another important indicator of migratory pressure is the number of asylum applications lodged in the EU.[18] The simultaneous use of data

[15] A. Kołodziejak, W.Trybuł, *Konsekwencje migracji do Unii Europejskiej*, [in:] *Rocznik bezpieczeństwa międzynarodowego*, eds. K. J. Helnarska, G. Motrycz, Warszawa 2017, p. 95.

[16] Frontex, *Risk Analysis for 2016*, Warsaw 2016, p. 5–6. https://www.frontex.europa.eu/assets/Publications/Risk_Analysis/Annula_Risk_Analysis_2016.pdf [date of access: 20.08.2025].

[17] Frontex, *Risk Analysis for 2023*, Warsaw 2023, p. 18; Frontex, *Annual Risk Analysis 2024*, Warsaw 2024, p. 12. https://www.frontex.europa.eu/assets/Publications/General/ARA_2023.pdf [date of access: 20.08.2025].

[18] European Migration Network (EMN), *Annual Report on Migration and Asylum 2023 – Highlights*, Brussels 2024, p. 33.

on irregular border crossings and asylum applications allows for a more nuanced understanding of migratory pressures, linking unauthorised entry flows with their institutional consequences for asylum systems. Although methodologically distinct, both indicators are frequently conflated in EU policy debates, where irregular entry statistics are often used interchangeably with asylum figures to justify restrictive measures. In this article, these two dimensions are treated as complementary but analytically separate, in order to ensure conceptual clarity and more accurate assessment of EU migration governance.

These data do not directly represent the number of irregular crossings, but they reflect the burden on asylum systems that results from irregular entries and subsequent secondary movements within the Union.

Table 1. Number of asylum applications submitted to EU Member States in 2020–2023

Country	2020	2021	2022	2023
Austria	13400	37800	109775	55605
Belgium	12905	19545	32100	29260
Bulgaria	3460	10890	20260	22390
Cyprus	7065	13260	21590	11660
Czechia	790	1055	1335	1130
Germany	102525	148175	217735	329035
Estonia	45	75	2940	3980
Greece	37860	22660	29125	57895
Spain	86380	62050	116135	160460
Finland	1445	1355	4815	4450
France	81735	103790	137510	145095
Croatia	1540	2480	2660	1635
Hungary	90	40	45	30
Ireland	1535	2615	13645	13220
Italy	21330	45200	77200	130565
Lithuania	260	3905	905	510
Luxembourg	1295	1365	2405	2615
Latvia	145	580	545	1625
Malta	2410	1200	915	490
Netherlands	13660	24730	35500	38320
Poland	1510	6240	7700	7720
Portugal	900	1350	1975	2600
Romania	6025	9065	12065	9875
Sweden	13595	9015	13180	8945
Slovenia	3465	5220	6645	7185
Slovakia	265	330	500	370
Norway	1325	1595	4650	5135

Source: European Migration Network (EMN), *Annual Report on Migration and Asylum 2023 – Highlights,* Brussels 2024, *p.33*, https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-publications/emn-annual-reports_en [date of access: 20.06.2025].

The distinction between border crossings and asylum applications is crucial. Taken together, these indicators provide a more complete picture of migratory pressure: crossings illustrate the scale of unauthorised entries, while applications show how Member States' asylum systems are affected in practice. This dual perspective also helps to explain the discrepancy between empirical data and political discourse, in which threats are often overstated or instrumentalised. Moreover, irregular border crossings represent an immediate challenge for border management authorities, whereas asylum applications reflect the longer-term institutional and financial burden associated with reception, adjudication, and integration processes. The correlation between these two indicators is not linear, as not all irregular entrants apply for asylum, and not all asylum applicants have crossed borders irregularly, which further complicates measurement and policy responses. Academic studies have emphasised that political actors frequently conflate these categories, using overall asylum figures as a proxy for irregular entries in order to strengthen securitised narratives. In reality, the two dimensions interact but remain analytically distinct, and a nuanced approach is required to avoid misleading generalisations. Recognising this distinction is essential for designing evidence-based policies that simultaneously uphold border integrity and safeguard the right to seek international protection.

The diversity of interest in individual EU Member States stems from multiple factors, including the presence of established diasporas, language, historical links, employment opportunities, and the accessibility of asylum procedures and administrative practices. Germany, France, Spain, and Italy have long received the highest numbers of applications for international protection within the EU, which is partly attributable to their economic strength and geographical location.[19]

Between 2023 and 2025, the Member States of the European Union undertook a range of measures aimed at strengthening the protection of the external borders, reducing irregular migration, and combating migrant smuggling. Particular importance was attached to infrastructure investments and legislative changes, which may serve as effective tools for controlling migration flows and enhancing internal security. Noteworthy in this context are the actions taken by Poland as a country that forms part of the EU's eastern border. The crisis at the Polish-Belarusian border, which began in the second half of 2021, represents an example of a complex phenomenon of a hybrid nature,[20] in which migration

[19] European Migration Network (EMN), *Annual Report on Migration and Asylum 2023 – Highlights*, Brussels 2024.

[20] "Belarus aimed to undermine the international standing of Poland, Lithuania, and Latvia by portraying them as countries reluctant to accept refugees and migrants. This was also an attempt to test the position of these three states within the EU and NATO. Moreover, the Belarusian diplomatic service undertook

flows were used as a tool of political pressure on the European Union.[21] These actions formed part of a broader strategy pursued by the Belarusian authorities in response to the sanctions imposed on Belarus due to human rights violations and breaches of democratic principles.

The instrumentalisation of migration consisted in facilitating the arrival of third-country nationals, primarily from the Middle East and Africa, onto the territory of Belarus and subsequently directing them towards the borders of the European Union's Member States, most notably Poland, Lithuania, and Latvia. Poland's response has been the subject of extensive criticism in reports issued by EU institutions, UNHCR, and human rights NGOs, which highlighted possible inconsistencies with both domestic and international legal standards. This assessment relies on secondary sources and does not include original fieldwork; the Polish case is therefore presented primarily as an illustrative example of the broader tensions within EU migration governance.

Poland's actions were repeatedly criticised by institutions such as the European Parliament and the UNHCR, which highlighted violations of the principle of non-refoulement. As the European Parliament explicitly stated, Member States must "ensure that EU asylum and return law and international human rights law are respected […] including access to asylum, legal aid and civil society organisations."[22] In its resolutions of 2021 and 2022, the European Parliament condemned the practice of push-backs at the Polish–Belarusian border as incompatible with EU and international obligations, stressing that access to asylum procedures must be guaranteed at all times.[23] Similarly, the UN High Commissioner for Refugees repeatedly urged Poland and other frontline Member States to respect the right to seek asylum, recalling that non-refoulement is a cornerstone of both the 1951 Geneva Convention and EU law.[24] Human rights NGOs, including Amnesty International and

a range of efforts to discredit, in particular, Poland and Lithuania in other international organisations, including the United Nations and the Organization for Security and Co-operation in Europe (OSCE)," see: A. M. Dyner, *Kryzys graniczny jako przykład działań hybrydowych*, https://www.pism.pl/publikacje/kryzys-graniczny-jako-przyklad-dzialan-hybrydowych [date of access: 20.06.2025].

[21] These actions are primarily targeted at Poland and Lithuania, that is, the countries that have actively supported the Belarusian opposition following the announcement of the election results and have provided shelter to Sviatlana Tsikhanouskaya after the 2020 presidential elections. See: B. Fraszka: *Sytuacja na granicy polsko-białoruskiej: przyczyny, aspekt geopolityczny, narracje*, https://warsawinstitute.org/pl/sytuacja-na-granicy-polsko-bialoruskiej-przyczyny-aspekt-geo-polityczny-narracje/ [date of access: 22.06.2025].

[22] European Parliament, *Resolution RC-B9-0482/2021 – At the border between Belarus and the EU*, Strasbourg, 6 October 2021, point 15, https://www.europarl.europa.eu/doceo/document/RC-9-2021-0482_EN.html [date of acces: 10.09.2025].

[23] *Joint motion for a resolution B9-0482/2021 – At the border between Belarus and the EU*, 6 October 2021, https://www.europarl.europa.eu/doceo/document/B-9-2021-0482_EN.html [date of acces: 10.09.2025].

[24] UNHCR, *UNHCR urges States to end stalemate at Belarus-EU border and avoid further loss of life*, 22.10.2021,

Human Rights Watch, also documented instances of summary expulsions and ill-treatment of migrants, which further intensified the debate on whether unilateral national responses undermine the Union's credibility in upholding its legal standards.

In contrast, Finland's measures were primarily framed as preventive and security-oriented, focusing on physical infrastructure, electronic surveillance, and the temporary closure of border crossings with Russia. These steps attracted comparatively less criticism regarding compliance with asylum guarantees than the practices observed in Poland. The Finnish case thus serves as a contrastive example of preventive rather than coercive measures, illustrating the diversity of instruments applied by Member States under conditions of migratory pressure.

Taken together, the two cases underscore the divergent ways in which Member States operationalise EU migration policy under hybrid pressure. Poland illustrates a coercive and securitised approach that has attracted sustained legal and humanitarian criticism, while Finland exemplifies a preventive and infrastructure-based strategy that, although restrictive, has provoked comparatively less controversy. The juxtaposition of these responses highlights both the adaptability and the fragmentation of the Union's migration governance, as well as the continuing tension between national sovereignty and supranational legal commitments. At the same time, the divergent national practices observed in Poland and Finland feed into a broader political dynamic within the Union. The handling of irregular migration has become increasingly intertwined with public perceptions of insecurity, contributing to a climate of mistrust and polarisation across Member States.

The community of European Union Member States is currently facing challenges that expose significant limitations in the capacity of institutions to effectively manage migration and refugee crises. In many EU countries, an increasingly prevalent discourse of fear and distrust can be observed, reflecting the so-called politics of fear — a phenomenon in which migration becomes a symbolic carrier of broader social, cultural, and identity-related tensions. The deepening ineffectiveness of joint crisis response efforts has contributed to a serious deficit of public trust in political elites and EU decision-making structures.[25] The interplay between real challenges, such as the management of asylum systems, and perceived threats, constructed in media and political rhetoric, contributes to the erosion of trust in EU institutions. This ambiguity is often exploited by radical movements to strengthen narratives of insecurity.

https://www.unhcr.org/news/news-releases/unhcr-urges-states-end-stalemate-belarus-eu-border-and-avoid-further-loss-life [date of accese 10.09.2025].

[25] P. Borkowski, *Wymiar polityczny uchodźctwa-wybrane problemy w kontekście europejskiego kryzysu migracyjnego*, [in:] *Uchodźcy w Europie*..., op. cit., p. 43.

In this context, the wave of refugees — particularly intensified after 2015 and following the Russian invasion of Ukraine in 2022 — began to be perceived not only as a humanitarian challenge but also as a threat to cultural identity and social security. Migrants became, in a sense, a "projection" of Europe's fears — both real and those shaped by the media. Immigrants and asylum seekers are very often portrayed as existential threats to an imagined homogeneous nation — to its culture, values, as well as to the security and stability of society.[26] The foreigner — whether a refugee or an immigrant — becomes a metaphor for the collapse of order, loss of control, ineffective governance, and a threat to social cohesion.[27]Although Poland was not directly affected by the consequences of the 2015 migration crisis, mainly due to its geographical location, these events marked the beginning of a shift away from the Europeanisation of migration policy towards its nationalisation. Migration issues were then incorporated into the current political agenda, which was linked to ongoing election campaigns. In place of the EU approach, a sovereigntist narrative was introduced, in which migrants were portrayed as an existential threat to the state and society.[28]

In recent years, the Member States of the European Union have witnessed a marked increase in Eurosceptic attitudes and radical tendencies. These processes are particularly evident in the context of social tensions related to migration and growing inequalities. The intensifying political radicalism takes various forms — from populism to nationalism — and is increasingly expressed in opposition to further European integration, criticism of liberal values, and the promotion of discriminatory and xenophobic attitudes.[29]

In the rhetoric of radical groups, migrants are portrayed as a threat to the socio-cultural order of host countries. Particular emphasis is placed on the alleged failure of migrants to conform to dominant social and moral norms, and on their reluctance to culturally adapt, especially with regard to Christian traditions, education, and democratic values. In this perspective, migration becomes not only a political challenge but also a symbolic one associated with a civilisational conflict and the potential loss of national identity.[30]

This process contributed to the erosion of the idea of European solidarity, which, although proclaimed, proved to be limited and fragmented in practical application. This was particularly evident in the lack of agreement on the relocation

[26] R. Wodak, *The Politics of Fear: What Right-Wing Populist Discourses Mean*, London 2015, p. 2.
[27] Ibidem, p. 81.
[28] A. Nitszke, *Poland's Response to the Migration Crisis*, „Athenaeum. Polish Political Science Studies" 2023, vol. 79(3), strona?.
[29] C. Mudde, op. cit. pp. 4-7.
[30] Z. D. Czachór, *Wzrost antyimigracyjnego radykalzimu i eurosceptycyzmu jako wyzwanie dla przyszłości Unii Europejskiej,* [in:] *Uchodźcy w Europie…*, op. cit., p. 232.

of refugees and the asymmetry of burdens between Member States. In the official EU policy discourse on integration, the concept of solidarity gradually lost its original meaning, shifting from a principle of collective responsibility to an instrument often used to legitimise national interests. The term, initially shaped by the founding fathers of the European Communities, conveyed the lofty idea of collective action in support of economic development and the deepening of political integration.

Over time, however, its use increasingly took on an instrumental character serving to legitimise the particular interests of Member States rather than genuine cooperation in the spirit of shared responsibility.[31] In moments of particular tension and destabilisation such as the migration crisis (2015–2016), the COVID-19 pandemic (2020–2022), or the energy crisis following the full-scale Russian aggression against Ukraine (from 2022 onwards), the idea of European solidarity was put to a severe test. Although formally it remains one of the foundations of the European Union, its practical implementation often became fragmented. Faced with crises, Member States increasingly acted in accordance with the principle of national interest, which resulted in the refusal to share responsibility or attempts to withdraw from previously accepted mechanisms of cooperation.

European migration policy

The migration policy of the European Union constitutes one of the most complex and dynamic areas of common policy, shaped in response to changing social, political and internal security conditions. Its primary objective is to manage migration flows in a manner that ensures a balance between the right to international protection and the need to safeguard the integrity of external borders and the security of Member States. This policy covers both issues related to legal immigration, the integration of foreigners and the protection of refugees, as well as measures aimed at counteracting irregular migration, migrant smuggling and human trafficking. European migration policy is implemented through a set of legal acts, political strategies and operational mechanisms, which include, among others, the Common European Asylum System, visa policy, return procedures, and cooperation with third countries in the field of migration control and readmission.[32] Solidarity mechanisms and responsibility-sharing among Member States play a key role

[31] T. G. Grosse, J. Hetnarowicz, *Solidarność – zapomniana wartość Unii. Kryzys uchodźczy(migracyjny) a podziały między państwami członkowskimi,* [in:] *Uchodźcy w Europie…*, op. cit., p. 221.

[32] European Commission, *New Pact on Migration and Asylum – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0609 [date of access: 20.06.2025].

in this context; however, as demonstrated by recent experience, their practical implementation has encountered significant challenges, particularly in the context of migration crises (2015–2016), the crisis at the EU's eastern border, and the consequences of the war in Ukraine.

The European migration policy is based on a set of harmonised legal frameworks and cooperation mechanisms aimed at ensuring consistency in the actions of Member States in managing migration flows and protecting external borders. One of the pillars of these efforts is the Common European Asylum System, designed to ensure a uniform approach to granting international protection, determining responsibility for examining asylum applications, and establishing minimum standards for the reception of asylum seekers. This system aims to limit so-called secondary movements and to promote a more equitable distribution of responsibilities among the Member States. An integral part of the EU migration policy is also the harmonised visa policy, aimed at ensuring transparency and uniformity in the rules governing entry into the Schengen area. This policy is supported by the implementation of information systems facilitating the exchange of visa data and more effective monitoring of the movement of persons across the EU's external borders.[33]

Return procedures and readmission measures concerning third-country nationals lacking legal residence within the European Union constitute a pivotal component of the EU's comprehensive migration management framework. This policy is founded upon harmonised return standards adopted across EU member states, fostering a coordinated approach to the return of third-country nationals who do not have legal grounds to remain within the Union. A key element of this framework is structured cooperation with countries of origin, aimed at facilitating the identification, issuance of travel documents, and readmission of their nationals. Furthermore, the policy is supported by the operational involvement of European Union agencies, most notably the European Border and Coast Guard Agency which provides logistical, technical, and human resources to member states, enhancing the efficiency and effectiveness of return operations. In recent years, the mandate of Frontex has been significantly expanded to include not only support in voluntary and forced return procedures but also in negotiating readmission agreements and return-related capacity-building in partner countries.[34]

[33] European Commission, *Common European Asylum System (CEAS) and Visa Policy*, https://home-affairs.ec.europa.eu/policies/migration-and-asylum/common-european-asylum-system_en [date of access: 22.06.2025].

[34] European Commission, *Return and Readmission*, https://home-affairs.ec.europa.eu/policies/migration-and-asylum/return-and-readmission_en [date of access: 24.06.2025].

The New Pact on Migration and Asylum, proposed by the European Commission in 2020 and gradually implemented by the Member States, reached an advanced stage of operationalisation of several of its core components by mid-2025. The Pact represents an attempt to establish a coherent and durable model of migration governance that balances the responsibilities of frontline states with mechanisms of solidarity and shared accountability across the European Union as a whole.[35] Among the significant achievements of the Pact is the introduction of enhanced identification and registration procedures for migrants at the EU's external borders. In particular, the implementation of mandatory screening procedures including identity verification, health checks, and the collection of biometric data has significantly improved the efficiency and coordination of migration management operations.[36] These measures are intended to facilitate swift decision-making on the applicable migration or asylum procedures and to strengthen security checks, thereby supporting both humanitarian and security objectives of the Union.[37]

It should be emphasised that while the New Pact establishes a common EU framework, the operational reality remains strongly shaped by national migration policies, which often prioritise security considerations and domestic political agendas. This coexistence of supranational objectives and unilateral national measures highlights the persistent fragmentation of the EU's migration governance system. As a result, the effectiveness of the Pact depends not only on legal harmonisation at the EU level, but also on the willingness of Member States to align national practices with common standards.

Irregular migration remains a significant and enduring challenge for the security of the European Union's Member States, requiring an integrated legal, institutional, and operational approach. The conducted analysis confirms that the EU migration policy is evolving towards strengthening border control instruments, improving return procedures, and intensifying cooperation with third countries. At the Union level, these priorities are explicitly articulated in the New Pact on Migration and Asylum and in successive European Council conclusions, which

[35] European Commission, *New Pact on Migration and Asylum – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2020) 609 final, Brussels 2020.

[36] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 introducing a screening of third-country nationals at the external borders (Screening Regulation), OJ L 330, 23.12.2022, pp. 1–31.

[37] European Commission, *Pact on Migration and Asylum: Commission report assesses progress and next steps halfway through 2025*, Brussels 11 June 2025, https://home-affairs.ec.europa.eu/news/pact-migration-and-asylum-commission-report-assesses-progress-and-next-steps-halfway-through-2025-06-11_en [date of access: 24.06.2025].

emphasise the need to reinforce the Schengen Borders Code, accelerate return procedures, and expand Frontex's mandate as a European Border and Coast Guard.[38]

The Common European Asylum System (CEAS) also provides a harmonised legal framework that defines common minimum standards for asylum procedures and reception conditions.[39] EU migration governance thus operates simultaneously at two levels: through Union-wide instruments such as the Pact, CEAS and Frontex, and through national policies shaped by domestic political agendas. This dualism creates a structural tension: while the Union strives to establish a coherent system based on solidarity and shared responsibility, Member States often privilege unilateral security-driven measures, particularly in times of crisis.[40]

The national examples cited in this article — for instance, Poland's response to the Belarus border crisis or Finland's construction of border barriers — are therefore intended to illustrate how Member States interpret and apply EU-level priorities in practice, highlighting both the convergence and fragmentation of European migration policy. The effectiveness of these instruments is contingent not only on formal adoption at the EU level but also on the political willingness of Member States to align their domestic practices, a condition which remains uneven and contested. As a result, the effectiveness of the EU framework depends not only on legislative harmonisation, but also on the political will of individual states to implement common standards faithfully, which remains a major challenge in the field of migration governance.[41]

The analysis has also shown that intra-EU solidarity mechanisms and solutions based on the protection of human rights encounter significant limitations in practice. The implementation of the New Pact on Migration and Asylum, although it serves as a tool for organising the EU's migration management framework, does not eliminate the asymmetry of burdens between Member States, nor does it resolve all tensions related to the distribution of responsibilities.

The measures undertaken indicate the need for further efforts to balance the security interests of Member States with humanitarian obligations, while ensuring that the measures applied comply with the EU's legal acquis and international

[38] European Council, *European Council Conclusions*, Brussels, 24–25 June 2021, EUCO 7/21; European Commission, *New Pact on Migration and Asylum – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2020) 609 final, Brussels 2020.

[39] European Commission, *Common European Asylum System (CEAS)*, https://home-affairs.ec.europa.eu/policies/migration-and-asylum/common-european-asylum-system_en.

[40] D. Thym, *European Realities of Migrant Reception: Solidarity and Security in the EU Legal Framework*, "Common Market Law Review" 2020, vol. 57, no. 5, pp. 1455–1492.

[41] N. Zaun, *EU Asylum Policies: The Power of Strong Regulating States*, „Journal of European Public Policy" 2018, vol. 25, no. 7, pp. 1069–1087.

legal standards. It remains essential to monitor the effects of the adopted legal and political solutions and to assess their impact on the cohesion of EU migration policy in the long term. Future research should therefore assess not only the quantitative outcomes of EU migration policy, such as reduced numbers of irregular entries, but also its qualitative implications for the rule of law, human rights standards, and the resilience of European integration. This calls for closer interdisciplinary cooperation between legal, political science and security studies approaches in order to capture the evolving nature of migration governance.

Bibliography

1. Bierzanek R., Symonides J., *Prawo międzynarodowe publiczne*, *8th edition*, Warszawa 2005.
2. Borkowski P., *Wymiar polityczny uchodźctwa – wybrane problemy w kontekście europejskiego kryzysu migracyjnego*, [in:] *Uchodźcy w Europie. Uwarunkowania, Istota, Następstwa*, eds. K. A. Wojtaszczyk J. Szymańska,, Warszawa 2017.
3. Castles S., De Haas H., Miller M.J., *The Age of Migration: International Population Movements in the Modern World,* Basingstoke, 2014.
4. Czachór Z.D., *Wzrost antyimigracyjnego radykalizmu i eurosceptycyzmu jako wyzwanie dla przyszłości Unii Europejskiej*, [in:] *Uchodźcy w Europie. Uwarunkowania, Istota, Następstwa,* eds. K.A. Wojtaszczyk, J. Szymańska, Warszawa 2017.
5. Dyner, A. M., *Kryzys graniczny jako przykład działań hybrydowych*, https://www.pism.pl/publikacje/kryzys-graniczny-jako-przyklad-dzialan-hybrydowych.
6. European Commission, *New Pact on Migration and Asylum – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM(2020) 609 final, Brussels, 23 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0609.
7. European Commission, 'EU sees 38% drop in irregular border crossings in 2024', 24 January 2025, https://home-affairs.ec.europa.eu/news/eu-sees-38-drop-irregular-border-crossings-2024-2025-01-24_en.
8. European Commission, *Annual Report on Migration and Asylum 2023 – Highlights*, Brussels 2024, https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-publications/emn-annual-reports_en.
9. European Union Agency for Asylum (EUAA), *Latest Asylum Trends*, https://euaa.europa.eu/latest-asylum-trends.
10. European Migration Network (EMN), *Annual Report on Migration and Asylum 2023 – Highlights*, European Commission, Brussels 2024.
11. European Parliament, *Resolution RC-B9-0482/2021 – At the border between Belarus and the EU*, Strasbourg, 6 October 2021, point 15, https://www.europarl.europa.eu/doceo/document/RC-9-2021-0482_EN.html.
12. Fraszka B., *Sytuacja na granicy polsko-białoruskiej: przyczyny, aspekt geopolityczny, narracje*, https://warsawinstitute.org/pl/sytuacja-na-granicy-polsko-bialoruskiej-przyczyny-aspekt-geo-polityczny-narracje.
13. Frontex, *Frontex publishes Risk Analysis for 2016*, 5 April 2016, https://frontex.europa.eu/media-centre/news/news-release/frontex-publishes-risk-analysis-for-2016-NQuBFv.
14. Frontex, *EU's external borders in 2022: number of irregular border crossings highest since 2016*, 13 January 2023, https://www.frontex.europa.eu/media-centre/news/news-release/eu-s-external-borders-in-2022-number-of-irregular-border-crossings-highest-since-2016-YsAZ29.

15. Frontex, *Significant rise in irregular border crossings in 2023, highest since 2016*, 26 January 2024, https://www.frontex.europa.eu/media-centre/news/news-release/significant-rise-in-irregular-border-crossings-in-2023-highest-since-2016-C0g-Gpm.16. Frontex, *Irregular border crossings into EU drop sharply in 2024*, 14 January 2025, https://www.frontex.europa.eu/media-centre/news/news-release/irregular-border-crossings-into-eu-drop-sharply-in-2024-oqpweX.
16. Grosse T.G., Hetnarowicz J., *Solidarność – zapomniana wartość Unii. Kryzys uchodźczy (migracyjny) a podziały między państwami członkowskimi,* [in:] *Uchodźcy w Europie. Uwarunkowania, Istota, Następstwa,* eds. K. A. Wojtaszczyk, J. Szymańska,, Warszawa 2017.
17. International Organization for Migration (IOM), *Glossary on Migration*, International Migration Law No. 34 (Geneva: IOM, 2019), https://publications.iom.int/system/files/pdf/iml_34_glossary.pdf.
18. *Joint motion for a resolution B9-0482/2021 – At the border between Belarus and the EU*, 6 October 2021. https://www.europarl.europa.eu/doceo/document/B-9-2021-0482_EN.html.
19. *Konwencja dotycząca statusu uchodźców sporządzona w Genewie dnia 28 lipca 1951r*. https://www.amnesty.org.pl/wpcontent/uploads/2016/04/Konwencja_Dotyczaca_Uchodzcow.pdf.
20. Kołodziejak A., Trybuł W., *Konsekwencje migracji do Unii Europejskiej*, [in:] *Rocznik bezpieczeństwa międzynarodowego*, eds. K. J. Helnarska, G. Motrycz, Warszawa 2017.
21. Lipold P., *Nieregularna migracja do Unii Europejskiej. Tendencje i wyzwania,* Warszawa 2022.
22. Lubiewski P., *Nielegalna imigracja. Zagrożenia bezpieczeństwa część 1*, Szczytno 2016.
23. Malinowska I., *Wymiar prawny uchodźctwa. Status uchodźcy z perspektywy praw człowieka,* [in:] *Uchodźcy w Europie. Uwarunkowania, Istota Następstwa*, eds. K. A. Wojtaszczyk, J. Szymańska, Warszawa 2017.
24. *Migracje i polityka migracyjna. Polska w kontekście europejskim*, eds. M. Duszczyk, P. Kaczmarczyk, Warszawa 2013.
25. Mudde C., *The Far Right Today,* Cambridge 2019.
26. Nitszke A., *Poland's Response to the Migration Crisis*, "*Athenaeum. Polish Political Science Studies" 2023*, vol. 79, no. 3, strony?.
27. Thym D., *European Realities of Migrant Reception: Solidarity and Security in the EU Legal Framework*, "Common Market Law Review" 2020, vol. 57, no. 5, strony.
28. Trybuł-Klein W., *Polish migration policy*, [in:] *Security Challenges in an Interconnected World,* Budapest/Arad rok wydania. Vasile Goldiș University Press / Trivent Publishing).
29. United Nations Statistics Division, Recommendations on Statistics of International Migration, Revision 1, UN, New York 1998.
30. Wodak R., *The Politics of Fear: What Right-Wing Populist Discourses Mean,* London 2015.
31. Wojtaszczyk K.A., Nadolska J., Czub J.F., *Kryzysy w procesie integracji europejskiej i sposoby ich przezwyciężania*, „Przegląd Europejski" 2014, no. 3(33), strony.
32. Zaun N., *EU Asylum Policies: The Power of Strong Regulating States*, "*Journal of European Public Policy" 2018*, vol. 25, no. 7, pp. 904–922.
33. UNHCR, *UNHCR urges States to end stalemate at Belarus-EU border and avoid further loss of life*, 22.10.2021 https://www.unhcr.org/news/news-releases/unhcr-urges-states-end-stalemate-belarus-eu-border-and-avoid-further-loss-life.

Reviews, reports

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 383–393

ISSN 2543-6961
e-ISSN 2720-3093

Kazimierz Kraj
ORCID: 0000-0002-9646-1383
Jan Kochanowski University in Kielce

Review: Piotr Ogrodowczyk, *Służby specjalne w systemach totalitarnych* [Special Services in Totalitarian Systems], Toruń 2025, 546 pp. [Adam Marszałek Publishing]

In 2025, the book market saw the publication of Piotr Ogrodowczyk's monograph *Special Services in Totalitarian Systems*. The book fits within the growing body of works related to the increasingly popular intelligence studies field in Poland. Like any publication, it requires not only editorial reviews but also a post-publication assessment that highlights its strengths and weaknesses.

Piotr Ogrodowczyk, as stated in the biographical note on the book cover, is a graduate of the Academy of Humanities and Economics in Łódź. He is described as an enthusiast deeply exploring the history of totalitarian systems and the secret services that formed their foundation [quote from the cover]. His main interests, as noted, focus on Russian security services, from the Oprichnina to contemporary times. He also runs the video blog *Polityka dla Opornych*. According to the authors of the note, he is able to present difficult issues in an accessible manner.

The reviewer attempted to obtain additional information about P. Ogrodowczyk but was unable to find details regarding the title of his doctoral dissertation written under the academic supervision of Marek J. Malinowski, nor the date and place of its defense (I checked, just in case, on the websites www.ck.gov.pl and the "List of Advancement Proceedings – RAD-on: REPORTS, ANALYSES, DATA"). On the Nauka Polska portal, in the list of doctoral candidates supervised by Professor M. J. Malinowski, there is no doctoral dissertation by P. Ogrodowczyk. Likewise, after checking the profiles of Professors Bogdan Chrzanowski and Andrzej Gąsiorowski – listed as reviewers of the book based on the dissertation (presumably the dissertation's reviewers) – no information concerning P. Ogrodowczyk was found.

I therefore turned to LinkedIn and managed to clarify some details about the author. He obtained his master's degree (2012) in political science within the field of public administration, and his bachelor's degree in European studies. He has an interesting professional résumé and has worked in many occupations,

including serving for seven years as an assistant to MP (now senator) Artur Dunin. He previously published academic articles, among others in *Civitas Hominibus* no. 13/2018 and *Studia Bezpieczeństwa Narodowego* no. 1/2013 vol. 4. These articles were based on the content of his doctoral dissertation in preparation.

The bibliography of the monograph under review is relatively extensive and comprises 354 items. The alphabetically arranged list of sources includes archival documents, printed documents, legal acts of various categories, studies, and scholarly articles, including those published on various online platforms. A weakness of the bibliography is the lack of hierarchical organization in accordance with established scholarly standards – such as classification into source editions, memoirs, press materials, or studies. Such structuring would have enabled the reader to more easily assess the scholarly and informational value of the sources used.

An analysis of the Russian-language works cited by the author reveals a fundamental weakness. These studies are several or even dozens of years old e.g., К. Дегтярев, *Смерш*, Москва 2008; А. Полянский, *Ежов (История «железного» сталинского наркома)*, Москва 2001; А. Колпакиди, *Империя ГРУ. Очерки истории российской военной разведки*, т. 1, Москва 1999). Furthermore, they constitute only a small fraction of the more than 350 referenced items. Referring to journalistic, popular works by Leonid Mleczin, such as *Ojcowie terroru. D Dzierżyński, Mienżyński, Jagoda*, vol. 1, Warszawa 2003, is at the very least questionable due to the lack of a solid source base in these works.

The bibliography also lacks significant collections of printed documents that should have been used, such as: *Ф.Э. Дзержинский председатель ВЧК–ОГПУ 1917-1926. Документы* (сост. А.А. Плеханов, А.М. Плеханов), Москва 2007; *Лубянка. Органы ВЧК-ОГПУ-НКВД-НКГБ-МГБ-МВД-КГБ. Справочник. Документы* (сост. А.И. Кокурин, Н.В. Петров), Москва 2003; or *В.Ч.К. Всероссийская чрезвычайная комиссия по борьбе с контрреволюцией и саботажем. Главные документы*, lacking place and year of publication. This document album was published jointly by the "Komsomolskaya Pravda" publishing house and the Public Council at the FSB of Russia.

In the section addressing Soviet special services (or, more precisely, state security organs), the author failed to use works by the most distinguished Russian experts in the field, such as Александр Плеханов, Владимир Хаустов, Олег Хлобустов, Александр Зданович, Олег Мозохин, Владлен Измозик, and Андрей Плеханов. Among Polish scholars, the omission of Leszek Pawlikowicz, a leading expert on the KGB, is particularly noticeable.

When we look at the literature used by the author to present the German security apparatus of the Third Reich and the GDR, the absence of German authors is striking. It is surprising that the memoirs of Reinhard Gehlen were not used, nor the study on the Stasi by Jens Gieseke, published in Poland, as well as works by other authors such as David Kahn. I do, however, appreciate the use of studies by Professor Karol Grünberg, perhaps the most eminent Polish expert on Hitler's biography and the security system of the Third Reich. Nevertheless, the bibliography lacks publications that would broaden the reader's knowledge, such as the works of Leszek Gondek, Henryk Ćwięk, or Roman Kilarski, which would enrich the general understanding of Hitler's intelligence services.

The literature used to present the problematics of the special services of the People's Republic of Poland also shows significant gaps. In my view, the author should have included, among others, the works of Sylwia Galij-Skarbińska, Arkadiusz Nyzio, Filip Musiał, Sławomir Cenckiewicz, or Witold Bagieński.

The reviewer does not deny the author's efforts in conducting source research; however, it is his duty to point out the authors or bibliographic works whose inclusion, in his view, would have enriched the substantive dimension of this interesting monograph. In the bibliography, the author should also indicate the source from which a given document was obtained – for example, see p. 526: *Dyrektywa GUKR Smiersz nr 38288 z 16 lipca 1943 roku – „Instrukcja organizowania i prowadzenia gier radiowych z wrogiem*", or p. 538: *Rozkaz MON nr 051* No. 051 of 4 April 1979. More such examples could be cited.

There are also other entries that are not entirely precise. On pp. 536-537 there is an entry suggesting that the author consulted Russian archives but did not mention this in the introduction:*Протокол заседания СНК от 7 декабря 1917, пункт 9: доклад Дзержинского об организации и составе комиссии по борьбе с саботажем. Государственный архив Российской Федерации, ф. Р-130, оп. 23, д. 2, л. 159, 161-162.*

Meanwhile, on pp. 533-534 we find the following entry: *Некрасов Василий Федорович, Вклад внутренних сил в дело победы советского народа в Великой Отечественной войне, «Военно-исторический журнал», nr 9/1985, Министерство обороны Российской Федерации (Минобороны России), Москва 1985.*

Yet, in 1985, the Ministry of Defence of the Russian Federation did not exist. Despite these remarks – both those articulated here and others not presented – the literature query conducted by Piotr Ogrodowczyk can generally be assessed positively. It undoubtedly provided a sufficient foundation for writing the monograph. Its greatest shortcoming is the lack of hierarchical differentiation of sources

and the absence of the most recent studies, as well as the failure to use works by researchers mentioned by the reviewer.

The monograph under review is divided into seven chapters and includes an Introduction, Conclusion, List of Abbreviations, and Bibliography. Unfortunately, from an editorial standpoint, it is poorly structured. The length of the individual chapters ranges from 19 to 136 pages, which is unacceptable. This discrepancy is not justified by the subject matter of the respective chapters. Why does the author devote 113 pages to the twelve-year period of the functioning of the Third Reich's security organs, while allocating only 19 pages to the forty-year history of the GDR's special services? Insufficient sources, perhaps? The Soviet state security organs are described over 136 pages, while the Polish ones occupy 104 pages. The author had incomparable access to Polish sources (particularly archival ones), as well as to numerous studies, books, and scholarly articles.

These examples point to gaps in the author's scholarly methodology. They also make it more difficult for the reader to fully grasp the content of the book. For instance, the author writes that the book was based on an analysis of available documents and sources – as if documents were not themselves sources, and indeed the most valuable ones, being primary. Having read the monograph, I can state that P. Ogrodowczyk synthesized the information he gathered in order to present it to the reader. Moreover, he employed the problem-oriented method, especially in the first three chapters, and the chronological-problem method in the remaining parts of the book. He also used biographical approaches to introduce figures he considered important for the functioning and analysis of the special services discussed.

Referring back to the shortcomings in the source inquiry, it must be emphasized that the author is aware of the issue of source reliability in relation to the chosen topic. Since he writes from a historical perspective and deals with services that have not existed for several decades, the possibility of obtaining reliable sources is relatively high.

The subject matter addressed in the reviewed book has been explored by many authors. In addition to those used by the author and those listed above by the reviewer, many more could be mentioned. Not all works are available in Polish, but both Polish and international literature in the field of intelligence studies is relatively extensive. I will list some of the authors whose works were not used by the author, but which, in the reviewer's opinion, would have been valuable for raising the scholarly level of the book. Among these authors are: Marek Berliński, Marek Słoń, Stanisław Wójcik, Robert Zulczyk, Władysław Bułhak, Jan Bury, Patryk

Dobrzycki, Justyna Doroszczyk, Roger Faligot, Rémi Kauffer, Andrzej Grajewski, Mariusz Antoni Kamiński, Monika Komaniecka-Łyp, Bogusław Pacek, John Barron, Milt Bearden, James Risen, Tennent H. Bagley, John Dziak, Edward Jay Epstein, Amy Knight, Александр Шевякин, Сергей Воронцов, Василий Христофоров, Олег Хлобустов, Евгений Бочков, Сергей Мироненко, Алексей Степанов, Сергей Веригин, and many others.

I would also recommend conducting a query of publications from the journals *За и против* and *Разведчик*, as well as articles published in the conference volumes of the *Общество изучения истории отечественных спецслужб* (Society for the Study of the History of Domestic Special Services).

The first chapter, *State Security in a Comprehensive Approach: Internal and External Aspects and Contemporary Threats* (34 pages), is divided into six subsections devoted to: the definition of security, state (national) security, state security management, internal security, information security, and security strategy.

The second part, *The Charisma of Power: The Evolution of the Concept and Its Significance for Leadership* (20 pages), contains three subsections addressing the understanding of charisma, the charisma of power in totalitarian and democratic systems (ideology), and the element of state governance constituted by special services.

The third chapter, titled *The Division and Scope of Activity of Special Services: A Historical and Definitional Perspective* (46 pages), is composed of as many as eleven sections. They address the following issues: the history of intelligence and information activities, the definition of intelligence, the acquisition and methods of operation of spies, disinformation, active measures, open-source intelligence, agents of influence, illegals, technical methods of intelligence collection, counterintelligence activities, and military intelligence and counterintelligence.

The fourth chapter is titled *The Special Services of Russia and the USSR – From Revolution to Totalitarianism* (136 pages). It is divided into four subsections, three of which contain further titled parts. The first subsection is dedicated to Joseph Stalin and the tools of his dictatorship. The second describes "faces behind the curtain," presenting the biographies of the following heads of the Soviet and Russian special services: Feliks Dzerzhinsky, Vyacheslav Menzhinsky, Genrikh Yagoda, Nikolai Yezhov, and Lavrentiy Beria. The third subsection discusses the structure and specializations, that is, the types of Russian and Soviet special services: the Cheka (VChK), the Unified State Political Administration (OGPU) and its direct predecessor GPU, the People's Commissariat for Internal Affairs, the Committee of Information, and the Committee for State Security under the Council

of Ministers. The fourth and final subsection is devoted to the strength and role of military special services in Soviet military doctrine and the actions of the Red Army, including the Registration Directorate, the Main Intelligence Directorate (GRU), and the military counterintelligence service SMERSH.

The fifth chapter, *Ruthless Instruments of Power: Special Services in the Third Reich* (113 pages), consists of three subsections, two of which are divided into smaller parts. The first subsection introduces Adolf Hitler and the security apparatus, its ideological foundations, and oversight by the Führer. The second subsection presents the profiles of the heads of the services: Hermann Göring, Heinrich Himmler, Reinhard Heydrich, and Wilhelm Canaris. The final subsection presents the structure and organization of German services, which the author divides into: the NSDAP Defensive Squadrons, the Reich Main Security Office, the Security Service of the Reichsführer SS, the Secret State Police, the Armed SS Units, special SS operational groups, and the Abwehr.

The next chapter, *The Repressive Apparatus in East Germany – An Analysis of the Ministry for State Security (STASI) 1950-1989* (19 pages), is divided into two parts: the first devoted to Erich Mielke and his role in the construction of the Ministry for State Security; the second addressing the organizational structures and operational divisions of the *Staatssicherheitsdienst*.

The seventh and final chapter, *The Shadow of Communism – The Evolution of Special Services in the People's Republic of Poland* (104 pages), is divided into three subsections, each further divided into smaller parts. The first subsection contains biographical notes on Bolesław Bierut, Władysław Gomułka, Stanisław Radkiewicz, and Czesław Kiszczak, presenting these politicians as the foundations of the system of repression and control in Poland. The second subsection is devoted to the organizational structure and evolution of the special services of the PRL and is divided into parts concerning the Department of Public Security, the Ministry of Public Security, the Committee for Public Security, and the Security Service. The final subsection presents the history, structure, and tasks of military special services, including the Internal Security Corps, the Main Directorate of Information of the Polish Army, the Military Internal Service, and the Internal Security Corps and Border Protection Troops.

The monograph opens with the Introduction and closes with Conclusion. The Introduction is conventional: it discusses, among other things, the contents of the monograph, provides a relatively general assessment of the sources, and addresses the issue of the biographies of J. Stalin, A. Hitler, and F. Dzerzhinsky, along with the sources used in presenting these figures. It ends with relatively extensive acknowledgements for assistance in writing the doctoral dissertation and in publishing this book. The Conclusion, in the reviewer's assessment, does

not particularly engage with the content of the book, does not identify topics that could not be addressed in the monograph, nor does it propose research areas related to the scope indicated in the title of the reviewed work. Instead, it consists of fairly loose reflections by the author on totalitarianisms and the threats present in the "information era," as well as on the new tools that special services possess or may possess. These services, in the author's view, form the foundation of every totalitarian system. The text is supplemented by a list of abbreviations, which, in the reviewer's opinion, could have been somewhat shorter. Many acronyms are widely known. Here are some examples: PZPR, LWP, AK, AL, GL, CIA, FBI, IPN, KGB, KPZR, MBP, MO, NATO, NKWD, NRD, NSDAP, ONZ, PRL.

In his friendly critique of the publication, the reviewer focuses on chapters four through seven, i.e., those presenting the special services of Russia and the USSR, Nazi Germany, the GDR, and the Polish People's Republic. From the first three chapters, which together comprise 100 pages, the author should have created a single chapter, limiting the discussion of security—described by him as "comprehensive"—and instead presenting the political and party systems of the states whose special service systems he examines. As a political scientist, the author should understand the role of the political and party system in authoritarian (totalitarian) states. The charisma of leaders, on which he elaborates at length, would have had little significance without a developed bureaucratic apparatus and ruling parties with a mass character (millions of members). On charisma alone, totalitarian (autocratic) systems could not have been built.

Moreover, each of the states described featured a different party system. In the USSR and Nazi Germany, these were single-party systems. In the Polish People's Republic, a hegemonic-party system functioned, supported by other parties (PZPR, ZSL, SD). Without going into detail, in the GDR, apart from the SED (Socialist Unity Party), four other parties (CDU, LDPD, DBD, and NDPD) also existed, whose representatives were part of the state authorities. Like ZSL and SD in Poland, these parties were dominated by the hegemonic party. The nature of the political system influenced the entire exercise of power, including its crucial component – the special services, that is, the state security apparatus analyzed by the author.

The lack of an analysis of the political-party system and its complex and diverse relations with the special services – changing over successive stages of the functioning of the respective political regimes – is undoubtedly a significant impoverishment of the topic undertaken. The author should be familiar with and understand the functioning of political and party systems, as well as their role and tasks in governing the state.

We will now turn to the chapter devoted to the special services of Soviet Russia and the USSR. The reviewer does not comment on the biographies of the selected heads of these services. However, since the author traces the history of the Soviet special services up to the early 1980s and discusses their operations, for example in Afghanistan, it is unclear why he does not present the biographies of at least two important heads of the KGB: Ivan Serov (whom he mentions several times) and Yuri Andropov, who held the position of chief of the most important Soviet special service for the longest period.[1] In describing KGB operations, the author most often refers uncritically to the book by Christopher Andrew and Oleg Gordievsky as his source. An example of their inaccuracies is the claim that Ivan Serov became an alcoholic and, after a heavy drinking binge, shot himself in the head in a side street near the Arbat.[2]

Similarly, in presenting the history of Soviet military intelligence, the author relies on the works of Viktor Suvorov (a defector, like Gordievsky) and Aleksandr Kolpakidi, while his discussion of wartime counterintelligence (SMERSH) depends solely on a relatively recent work by Vadim J. Birstein from 2017 – not, as stated in the bibliography (p. 522), by Vincent. Without denying the author's narrative skill, it must be noted that P. Ogrodowczyk uses facts rather loosely. For instance, on p. 236 he writes that the personnel of the KGB numbered about 400,000 officers, plus an additional 220,000 soldiers of the Border Troops. This information is inaccurate, since around 1991 the total number of officers and soldiers was approximately 480,000, including about 220,000 in the Border Troops and roughly 90,000 employees of the republican KGB branches. The author should have confronted his sources using, for example, the unused studies of Oleg Mozokhin or, regarding the size of the First Chief Directorate of the KGB, the relatively precise (and well-documented) data provided by Leszek Pawlikowicz.

I also do not understand what decisions Leonid Shebarshin could have made and implemented as the head of the KGB, since he held this position in an acting capacity for only one day (22 August 1991). The decisions the author attributes to him (such as providing reliable information) could have been made when he was deputy chairman of the KGB and head of the First Chief Directorate, from

[1] On the side, I leave out the figure of general Peter Ivashutin, who led the Soviet military intelligence for a quarter of a century. In addition, J. Andropov assumed full Power in the USSSR (General Secretary of the CPSU and Chairman of the Presidium of Supreme Soviet of the USSR).

[2] The English version was released in 1990. Since then, 35 years have passed until the publication of P. Ogrodowczyk's book, and our knowledge of the functioning of Soviet intelligence services has expanded dramatically, including through published collections of documents and studies by authors such as Александр Север, Владимир Лота, Клим Дегтярев. This also applies to the sources used to present the history of military intelligence and SMERSH. Indeed, I. Sierov died in July 1990.

February 1989 to 21 August 1991. When presenting the issue of the Committee of Information, the author oversimplifies its four-year history and does not even mention the so-called "small Committee of Information," chaired by Andrei Gromyko, from which the powerful KGB Directorate "A" dealing with disinformation emerged.

To write, for example, that the execution squad for Mikhail Tukhachevsky and other high-ranking officers was led by Ivan Serov is to repeat nonsense, probably after Robert Conquest. Tukhachevsky was executed in June 1937, while Serov[3] began his service in the security organs only in February (or January) 1939, as part of external recruitment ordered by Lavrentiy Beria. Among the several thousand people recruited from the ranks of the VKP(b) and Komsomol were several hundred graduates of military academies who were assigned to the NKVD by order. This is how Serov entered the organs. Likewise, during the period of activity described in Afghanistan, the KGB under the Council of Ministers of the USSR no longer existed; instead, the Committee for State Security of the USSR existed – a fact ignored by many authors, although it is important because it marked an elevation in the status of the institution.[4]

Chapters five and six are devoted to the special services operating in Germany. Chapter six presents, unfortunately in a telegraphic manner, the history of the security organs of the German Democratic Republic. The central figure used to illustrate the East German security apparatus is Erich Mielke, the long-time Minister for State Security. This short chapter is among the parts of P. Ogrodowczyk's publication that disappoint. It is impossible to present in a dozen pages more than forty years of the functioning of the security organs of the eastern occupation zone and later the GDR. The main source used is Heribert Schwan's book *Erich Mielke – Life in the Service of the Stasi* (Polish edition, 2001). Without even addressing the omission of Jens Gieseke's major monograph, the author could have based his work on Gieseke's extensive study included in the collective volume *Czekiści. Organy bezpieczeństwa w europejskich krajach bloku sowieckiego 1944 – 1989* (eds. K. Persak, Ł. Kamiński), Warszawa 2010, pp. 325-391, which also includes a list of German-language literature on the topic. As earlier, there is a casual approach to factual accuracy (p. 381, note 3). Mielke was a graduate of the International Lenin School of the Comintern, not of the Lenin Military-Political Academy in Leningrad, as is incorrectly attributed to him.

[3] Similarly, P. Ivashutin and General Vitaly Pavlov, who was the KGB representative in Poland for ten years, began their careers in the security services. Pavlov differed from Sierov and Ivashutin in that he was a student at a civilian university.

[4] This was related to the adoption of the new USSR constitution in 1977.

The earlier and more extensive chapter is devoted to the special services of Nazi Germany. In the reviewer's opinion, the author unnecessarily became entangled in describing the armed SS units (Waffen-SS) and the SS operational groups, while devoting too little space to the Abwehr, a service that deserved a broader treatment due to its importance for the expansionist policy of the Third Reich and its military successes. Furthermore, the author should have chosen a different set of service chiefs or supplemented it with figures such as Heinrich Müller, Ernst Kaltenbrunner, and Walter Schellenberg. The use of literature in this chapter can, however, be positively assessed – it is relatively diverse compared to the earlier chapters.

The final chapter of the monograph is devoted to the special services of the Polish People's Republic. This topic may be relatively familiar to readers due to the abundance of published studies, documents, and public discussions. A drawback is the omission of Agnieszka Grabowska-Siwiec's monograph *Kontrwywiad a władza, Od Departamentu II MSW do Zarządu Kontrwywiadu UOP*, Warszawa 2024. The content of the chapter does not introduce any new or noteworthy findings regarding the transformation and functioning of the PRL's special services. As noted earlier, the selection of personnel is not entirely accurate. In the reviewer's view, between Władysław Radkiewicz and Czesław Kiszczak, two individuals should have been characterized – Mieczysław Moczar and Mirosław Milewski – whose influence on the nature and functioning of the special services was significant. A flaw of the chapter is its very brief and superficial presentation of military special services, beginning with the Main Directorate of Information, through the Military Internal Service (WSW), and the omission of military intelligence. Also unnecessary, in the reviewer's view, is the presentation of the Internal Security Corps (KBW) and its tasks. The KBW was not a special service; it formed part of the broader category of public security organs.

The author did not make the effort to present lesser-known espionage and counterintelligence operations of the Security Service to the reader. I have in mind, for example, the infiltration of diplomatic facilities by counterintelligence officers, intelligence operations directed against the Vatican, or the illegal intelligence of the PRL. Instead, he repeats descriptions of operations or spy scandals from many earlier publications.

The classical principle of writing a review requires the presentation of conclusions and research postulates for the future. In addition to the conclusions already included in the present text of the review, and assuming that the author may wish to publish this work again, I propose the following changes:

1. Editorial refinement of the book's structure (including a more proportional arrangement of its parts).
2. Rewriting the first three chapters and supplementing them with a chapter devoted to the political and party systems in the respective states, as well as to the role of the ruling party and its bureaucratic apparatus in shaping the relations with, and importance of, the special services referred to in the title.
3. A thorough authorial revision of the study with regard to the facts cited, combined with proper source criticism.
4. Supplementing the literature and refining its editorial form. The same should be done with the footnotes. The bibliography should include all sources cited in the notes (at present, for example, the work of Krzysztof Surdyk is missing; see p. 94).
5. Adding an index of names.
6. Conducting an in-depth editorial review of the revised version of the monograph.
7. Attempting to prepare an appendix in the form of organizational charts of the structures of the services discussed.

The monograph by Piotr Ogrodowczyk under review, as stated at the beginning, fits within the growing series of publications by Polish authors in the field of intelligence studies. According to the reviewer's knowledge, it is the first academic Polish work attempting to present the role of special services in totalitarian systems in this manner, analysing and depicting them across several selected states, thereby enabling readers to compare them. Despite the shortcomings highlighted in the review, as well as those not mentioned, I consider the book worthy of reading. However, both readers with broader knowledge of the subject and beginners should approach the text with distance and critical caution, especially in places where they may sense that the author becomes more of a popularizer of knowledge than a detached scholar adhering to the principle of scientific objectivity.

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 395–399

ISSN 2543-6961
e-ISSN 2720-3093

Tomasz Marcinkowski
ORCID: 0000-0002-3568-5068
Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim

Report from the 9th Cross-Border Scientific Conference in the series "Development on the Periphery?"

Sprawozdanie z IX Transgranicznej Konferencji Naukowej z cyklu „Rozwój na peryferiach?"

Keywords: European Union, geopolitics, Polish-German relations, crisis, conference

On 29–30 May 2025, the Aula of Jacob of Paradies University in Gorzów Wielkopolski hosted the ninth edition of the scientific conference in the series "Development on the Periphery?". The theme of this year's edition was framed by the title "Nothing Will Ever Be the Same Again! The Polish Presidency, Germany, and the European Union in the Face of Transformations in the International Order." The event was organized by the Academic Center for German and European Studies of Jacob of Paradies University and the Konrad Adenauer Foundation. The conference was held under the honorary patronage of Professor Elżbieta Skorupska-Raczyńska, Rector of Jacob of Paradies University, Marek Cebula, Voivode of the Lubuskie Province and Jacek Wójcicki, Mayor of Gorzów Wielkopolski.

Partners of the conference included the Faculty of Law and Security of Jacob of Paradies University, the European Centre of the University of Warsaw, the Euroregion Pro Europa Viadrina, the Western Chamber of Industry and Commerce, the Polish European Studies Association (branches in Gorzów Wielkopolski and Rzeszów), the Polish Political Science Association (Gorzów branch), and the Polish European Community Studies Association (PECSA).

The aim of the conference was to provide space for reflection and debate on the role of Poland, Germany, and the European Union in the context of dynamic changes in the global order. Participants analyzed the challenges facing European foreign and security policy, and discussed both the opportunities and risks associated with Poland's presidency of the EU Council amid growing geopolitical tensions. A number of more specific issues were also addressed, including EU policies, the policies of Poland and Germany, as well as developments in the

Polish-German border region. Poland's presidency of the Council of the European Union represents a key moment for national and regional politics, offering an opportunity to shape the EU agenda and strengthen Poland's position on the international stage. The conference provided a platform for interdisciplinary exchange of views on the challenges and opportunities arising from Poland's assumption of this important and prestigious role.

The conference was opened by Professor Małgorzata Trocka, Vice-Rector for Education at Jacob of Paradies University, who emphasized the continuity of the event and its focus on important current issues affecting the region, Poland, and Europe. Subsequently, Marek Cebula, Voivode of the Lubuskie Province, addressed the audience, underlining the significance of the topics under discussion. On behalf of the Faculty of Law and Security of Jacob of Paradies University, the guests were welcomed by the Dean, Professor Beata Orłowska. Dr. Piotr Womela, representing the Konrad Adenauer Foundation, then spoke about the history of cooperation in the implementation of joint projects with the Gorzów university. The final speaker during the opening session was Professor Zbigniew Czachór, Director of the Academic Center for German and European Studies at Jacob of Paradies University, who expressed his gratitude to the University authorities, partners, co-organizers, and members of the Organizing Committee. Following the opening speeches, the inaugural lecture was delivered by Dr. Kai-Olaf Lang from the Stiftung Wissenschaft und Politik in Berlin. His presentation, entitled "What Shall We Do About It? Poland and Germany in Search of Lost Security," sought to address the central question posed in the title of the conference. The lecture was followed by a discussion.

Panels on the First Day

The first panel was chaired by Professor Beata Orłowska, Dean of the Faculty of Law and Security atJacob of Paradies University. The first speaker was Professor Tomasz Kubin from the University of Silesia in Katowice, who addressed the question of whether the Visegrad Group still exists in the context of the war in Ukraine. He was followed by Professor Agnieszka Bielawska from Adam Mickiewicz University in Poznań, who spoke about German leadership in the European Union's foreign policy. The third presentation was delivered by Professor Zbigniew Czachór of Jacob of Paradies University, who discussed the process of creating a communicative security community, drawing on the work of Karl Wolfgang Deutsch. At the end of the panel, the speakers responded to questions from the audience.

After the coffee break, the second panel began under the moderation of Professor Joanna Lubimow, Vice-Dean of the Faculty of Law and Security at Jacob of Paradies University. The first presentation was delivered by Professor Beata Przybylska-Maszner from Adam Mickiewicz University in Poznań, who discussed the Common Security and Defence Policy of the EU in the context of transformations of the international order. She was followed by Dr. Piotr Womela from the Konrad Adenauer Foundation in Warsaw, who addressed the timely and important topic of challenges facing the new Chancellor of the Federal Republic of Germany, Friedrich Merz. The third speaker was Professor Aleksandra Szczerba of Jacob of Paradies University, also representing Team Europe Direct and the Polish European Community Studies Association (PECSA). Her presentation focused on the issue of "Soft Power or Girl Power? The European Union as a Promoter of Non-Discrimination in the Age of (American) Backlash Against Gender Equality." After the final presentation, the panelists answered questions from the audience and engaged in a lively discussion.

After the lunch break, the third panel of the conference took place, moderated by Dr. Tomasz Marcinkowski, Deputy Director of the Academic Center for German and European Studies at Jacob of Paradies University. The session focused on more practical issues. The first speaker was Krzysztof Szydłak, Director of the Euroregion Pro Europa Viadrina Office in Gorzów Wielkopolski, who presented examples of Polish-German cross-border cooperation over the past 30 years of the Euroregion's activity. He was followed by Joanna Szymańska-Bica (Regionalexpertin im Bundesverband, Region West, Polnischer Sozialrat e.V., Berlin), whose presentation, entitled "From the Community of Policies to a Policy of Community: Evaluation of Diaspora Policy 20 Years after Poland's Accession to the European Union in the Case of Germany – New Challenges, New Needs?" examined the evolution of diaspora policy. The third presentation was delivered by Kamila Szwajkowska, Director of the Western Chamber of Industry and Commerce in Gorzów Wielkopolski, who analyzed the challenges and opportunities of cross-border cooperation among entrepreneurs. Following the presentations, the speakers answered questions and participated in a discussion.

The final panel of the first day was moderated by Dr. Ryszard Bodziacki from Adam Mickiewicz University in Poznań. The first presentation was delivered by Dr. Arkadiusz Machniak from the University of Rzeszów, who addressed the issue of left-wing terrorism in Europe, both in the past and today. He was followed by Dr. Arkadiusz Sójka from Adam Mickiewicz University, whose presentation focused on the relationship between the European Green Deal and the EU's

security and defence policy. The next speaker, Dr. Jacek Jaśkiewicz from Jacob of Paradies University, analyzed the objectives and challenges of the European Union's cohesion policy for the years 2021–2027.

In the final part of the panel, Dr. Joanna Lubimow, Dr. Łukasz Budzyński, and Dr. Tomasz Marcinkowski from Jacob of Paradies University presented the latest publication of the university's academic press. The volume, entitled "Ukrainian Refugees in Their Own Words"[1] contains the testimonies of refugee women who fled to Gorzów Wielkopolski following Russia's attack on Ukraine. The collection is supplemented with interviews with individuals engaged in providing assistance to war refugees in Gorzów, as well as scholarly articles. The panel concluded with a discussion.

Panels on the Second Day

The second day of the conference was held in the conference hall of the Main Library of Jacob of Paradies University. The session was opened by Professor Beata Orłowska, Dean of the Faculty of Law and Security at Jacob of Paradies University, and Professor Zbigniew Czachór, Director of the Academic Center for German and European Studies and President of the Polish European Studies Association. The first panel was moderated by Dr. Piotr Womela from the Konrad Adenauer Foundation in Warsaw. The first speaker was Professor Aleksandra Kruk from the University of Zielona Góra, who analyzed narratives about Germany on the example of Olaf Scholz's coalition (2021–2025). She was followed by Dr. Maciej Dudziak from Jacob of Paradies University, whose presentation entitled "When Authoritarianism Knocks at the Door: The Cunning of Anti-Reason" addressed the dangers of rising authoritarian tendencies. The panel concluded with a presentation by Oliwia Radkiewicz, MA from Jacob of Paradies University, who delivered a comparative analysis of climate policy in the election programs of Polish presidential candidates. The session ended with a discussion.

The second panel was chaired by Oliwia Radkiewicz, MA. The first presentation was given by Dr. Albin Skwarek from Jacob of Paradies University, who discussed changes in the international order and their impact on the security of Poland and Europe. He was followed by Dr. Tomasz Marcinkowski, also from Jacob of Paradies University, who presented his theses on the emergence of a new (or perhaps old?) security order in Europe. After the presentations, a discussion was held, followed by the formal closing of the conference proceedings.

[1] *Ukraińscy uchodźcy własnym głosem o sobie*, eds. Ł. Budzyński, T. Marcinkowski, J. Lubimow, Gorzów Wielkopolski 2024.

Conclusion

The ninth edition of the Gorzów conference in the series "Development on the Periphery?" was, in the opinion of both participants and organizers, an engaging and important academic event. The debates addressed current issues concerning the Polish-German borderland, Poland and Germany, as well as the European Union in the context of transformations of the international order. The inspiring presentations of the speakers and the discussions of their research findings constituted a valuable contribution to the broader debate on contemporary social and political processes.

Conclusion

Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 403–411

ISSN 2543-6961
e-ISSN 2720-3093

Tomasz Marcinkowski
ORCID: 0000-0002-3568-5068
The Jacob of Paradies University in Gorzów Wielkopolski

Juliusz Sikorski
ORCID: 0000-0002-0579-0158
The Jacob of Paradies University in Gorzów Wielkopolski

Instead of an ending... Tempus crisium, tempus mutationis

The analyses assembled in this volume clearly indicate that Europe is entering a period of qualitatively new security challenges, in which the longstanding paradigms of stability, predictability, and the dominance of the liberal order are losing their explanatory power. As emphasised in the introduction, contemporary crises - military, energy, economic, informational, and migratory - overlap and mutually reinforce one another, producing an environment of multidimensional uncertainty. Security is thus increasingly understood as a category encompassing hard and soft dimensions simultaneously, as well as domains that only a decade ago were rarely framed in terms of systemic threats. This volume reflects that transformation, both in its diagnosis of geopolitical processes and in its analysis of the mechanisms through which states and institutions respond.

The authors of Part I demonstrate that Europe's "new" security environment is not merely an accumulation of separate crises, but rather a system of interdependencies linking geopolitical pressure, infrastructural vulnerabilities, and constraints on institutional agency; consequently, an adequate response must be strategic, operational, and resilience-oriented at the same time. Marco Marsili traces the European Union's adaptation to hybrid conflicts, treating Russia's full-scale war against Ukraine as a catalyst accelerating reforms in crisis management, cybersecurity, energy resilience, and counter-disinformation measures. In his account, hybrid pressure operates in a distinctly "networked" manner: it targets institutional and societal nodes, tests decision-making cohesion, and compels rapid coordination - particularly at the EU–NATO interface - while remaining shaped by the interests and actions of external actors such as Russia, the United States, and China. This "top-down" diagnosis is further developed by Radoslava Brhlíková and Radoslav Ivančík, who frame the post-2022 challenges facing the Common Security and Defence Policy as a tension between rising ambition

and limited implementation capacity. They argue that instruments such as the Strategic Compass and efforts to strengthen defence capabilities and technological-industrial sovereignty are necessary responses to a deteriorating security environment, yet their effectiveness continues to be constrained by political fragmentation, divergent member-state preferences, coordination barriers, and persistent gaps between declaratory objectives and financing, timelines, and measurable implementation benchmarks. At this juncture, the volume makes a significant "operational turn": António Gonçalves Alexandre shifts attention to the EU's south-western flank and demonstrates that European security is increasingly shaped by seemingly peripheral processes at the intersection of maritime security, economic stability, and human mobility. He shows that piracy, smuggling, and illegal, unreported and unregulated (IUU) fishing in the Gulf of Guinea generate a chain of indirect effects - undermining coastal livelihoods, fuelling criminality, and, over time, intensifying migratory pressures along Atlantic routes, including those leading towards the Canary Islands. Crucially, Alexandre links this mechanism to the need for sustained development of EU frameworks and instruments for protecting maritime infrastructure and maintaining maritime presence, arguing that failure to address upstream drivers of instability ultimately produces security costs at the Union's "frontiers."

Against this backdrop, it becomes clearer that Europe's threats are simultaneously peripheral and "core": alongside pressures emerging from the south-western maritime approaches, a hard military–hybrid problem persists on the eastern flank. Zdzisław Śliwa analyses the Kaliningrad Oblast as a space that, in peacetime, may function as an instrument of pressure and asymmetric action, and, in crisis, as a potential vector of escalation and a forward hub for military operations. He draws attention to the implications of the oblast's militarisation – including the significance of A2/AD capabilities and air-defence and strike components – while at the same time emphasising the practical logic of deterrence: risk reduction requires continuous monitoring of indicators of preparation, the strengthening of national capabilities, the building of societal resilience, and the maintenance of a credible, coordinated allied presence. These conclusions align with a logic of "deterrence-enabled resilience": modernisation alone is insufficient if it is not accompanied by political cohesion and the capacity to act through shared procedures.

The infrastructural and economic dimension of security is developed by Anna Zaccaro, who presents the Baltic States – Estonia, Latvia, and Lithuania – as a "laboratory" of solutions aimed at enhancing the EU's energy resilience.

She argues that supply diversification, the expansion of LNG terminals, the synchronisation of electricity grids with the European system, and accelerated investment in renewables and energy storage carry not only economic and climate significance but also a strictly strategic one: they reduce the scope for energy to be used as an instrument of coercion and strengthen the stability of the EU's market and critical infrastructure. At the same time, she stresses that successful diversification should translate into a broader portfolio of dependencies – rather than a simple shift from one supplier to another – if the objective is genuine autonomy and systemic resilience.

A synthetic perspective is offered by Albin Skwarek, who frames the transformation of the international order as a process of erosion of multilateral mechanisms and intensifying great-power rivalry, reinforced by the war in Ukraine and hybrid instruments of pressure. In his argument, this entails the need to recalibrate the assumptions underpinning security policy, shifting emphasis towards resilience (energy, economic, infrastructural, and informational) and towards developing the capacity to act under conditions of potential weakening of transatlantic ties, while preserving the continuing relevance of alliances and formats of collective defence.

Part I concludes with Radoslava Brhlikova's contribution which – drawing on the thought of Milan Hodža – introduces the theme of regional agency in Central and Eastern Europe as a potential complement to the existing security architecture. The author treats regional integration not as a straightforward alternative to current structures, but as a prospective "pillar" capable of strengthening interest coordination, reducing vulnerability to a sphere-of-influence logic, and enhancing the region's stabilising resources in times of crisis. In this way, Part I arrives at a coherent overarching conclusion: in an era of overlapping crises, European security requires the simultaneous reinforcement of resilience (across infrastructure, energy, and society), operational capabilities (including maritime and defence capacities), and coordination mechanisms – both at the level of the EU and alliances and through regional initiatives that can increase the agency of states most exposed to strategic pressure.

In Part II, entitled New Forms of Confrontation, the contributors trace a contemporary "shift" of the battlespace towards modes of confrontation that blur the classical boundaries between war and peace, coercion and persuasion, and between the author of an operation and its "ostensible" executor. In the opening study, Sanshiro Hosaka identifies as the central analytical problem the fiction of agency attributed to alleged non-state actors under conditions of plausible

deniability and disinformation operations. He demonstrates that established conflict typologies – including reclassification criteria based on identifying the "main combatant" and assessing operational dominance – break down where an intervening state deliberately obscures its involvement and presents local structures as autonomous separatists. In response, Hosaka proposes shifting the evidentiary emphasis from purely quantitative measures of intensity to an analysis of political agency: who constitutes the actor, how it is organised, how deeply it is embedded in local elites, and whether it is in fact subordinate to an external decision-making centre. Practically, this entails treating "quasi-non-state actors" as instruments of state policy rather than as co-equal parties to a conflict – a move that carries implications both for interpreting the Russian–Ukrainian war prior to 2022 and for broader debates on attribution and responsibility in conflicts conducted "below the threshold" of conventional war.

The perspective of external interstate confrontation is complemented by an analysis of internal security threats which – although less spectacular than in the late twentieth century – continue to shape the stability of democratic systems. Arkadiusz Machniak reconstructs the origins and evolution of left-wing terrorism in Europe, situating it within a historical framework (including references to successive "waves" of terrorism) and highlighting the continuity of its core components: an anti-system ideological nucleus, the selective choice of targets, and the instrumentalisation of violence as a form of "political communication." At the same time, he emphasises changes in organisational forms and tactics – an evolution from the classic structures of the "neo-left" wave (e.g., the RAF, the Red Brigades, Action Directe) towards looser anarchist and autonomist configurations, which more frequently operate through low-cost modalities (sabotage, arson, IEDs, and acts of vandalism) directed against state institutions and infrastructure or actors associated with the "system." The contemporary dimension is linked to empirical data and observations regarding both extremist activity and EU member-state responses, leading Machniak to argue that, even if left-wing terrorism does not dominate today's security agenda, it remains an erosive factor whose salience may be amplified by processes of radicalisation and crisis-driven socio-political dynamics.

The next two contributions focus on confrontation in the informational and cognitive domains, treating them as arenas in which "soft" means can generate hard political effects. Marco Marsili examines the European Union's democratic resilience to disinformation through two case studies: the COVID-19 "infodemic" and interference in electoral processes. At the core of his analysis lies an assessment of

the EU's institutional and regulatory toolbox – among others, the Code of Practice on Disinformation, the Digital Services Act, the development of analytical capacity through the European Digital Media Observatory (EDMO), and coordination and early-warning mechanisms – alongside the question of their effectiveness in a digital environment characterised by fragmentation, platform logics, and the rapid "learning" capacity of hostile actors. Marsili highlights both the EU's achievements (building accountability frameworks for platforms, expanding fact-checking cooperation networks, and strengthening procedures for protecting electoral integrity) and persistent weaknesses: uneven implementation, the limitations of voluntary instruments, and the accelerating pressure of new technologies (including automation and AI) that increase the scale, speed, and apparent credibility of manipulation. His conclusion is explicitly systemic: democratic resilience requires combining regulation with adaptive governance, media literacy, and sustained cooperation among public authorities, academia, civil society, and the platform sector.

Juliusz Sikorski, in turn, closes Part II with an analysis of the influence architecture characteristic of cognitive warfare, in which proxy sources function as indirect, ostensibly independent nodes for transmitting and legitimising influence content. He reconstructs the mechanics of information laundering as a sequence (placement → layering → integration), demonstrating that intermediaries are not merely channels of content replication but structures that enable the "normalisation" of narratives in the public sphere through amplification, local "anchoring," and the lowering of audiences' thresholds of scepticism. Drawing on case studies (including Ghostwriter and NewsFront), Sikorski proposes a set of diagnostic indicators – recurrent "link bridges" to distribution hubs, short-window temporal convergence of publication, multilingual narrative calques, and legitimisation loops – as well as institutional recommendations that combine cognitive prevention (prebunking) with audits of distribution networks and intermediary accountability. These measures include proportionate interventions at the level of distribution infrastructure, provided they are embedded in transparent procedures and subject to meaningful avenues of appeal.

In Part III, the contributors demonstrate that the capacity of states and the European Union to respond to crises increasingly depends not only on "hard" resources, but also on the quality of legal frameworks, administrative procedures, and the effectiveness of the institutions responsible for applying them. The study by Roman Martyniuk, Oleksii Datsiuk, and Mykola Romanov provides an important reference point in this regard: the authors examine Ukraine's 2018 Law On

National Security of Ukraine as a foundational instrument of the regulatory order governing the security and defence sector, while simultaneously identifying its "bottlenecks" – above all terminological inconsistencies, an imprecise delineation of competences, and tensions between functions of command and coordination within the architecture of power (including the role of the presidential centre and coordinating bodies). In their view, the problem lies not in the very idea of comprehensive regulation, but in the risk that definitional ambiguity and overlapping competences reduce the predictability of state action under crisis pressure.

Maria Hapunik then shifts the focus to the EU's internal dimension, arguing that cross-border police cooperation has become one of the key "resilience instruments" in response to networked security threats: organised crime, cybercrime, migration crises, and hybrid interference. She points to the growing importance of institutional tools (such as Europol and EMPACT), the interoperability of information systems, and the deployment of new technologies (including AI and biometrics), while stressing a crucial condition of effectiveness: the expansion of operational capacity cannot occur at the expense of fundamental-rights protection and privacy standards, which in practice necessitates a continuous balancing of security imperatives and individual freedoms.

The institutional and procedural strand is further deepened by Robert Siuciński, who examines EU Regulation 2024/3015 prohibiting the placing on the Union market of products made with forced labour. He shows that, in response to human-rights violations, the EU increasingly relies on administrative instruments of a public-policy character, built on a risk-based approach and multi-stage procedures (a preliminary assessment phase, investigations, decisions, and enforcement), with a meaningful division of competences between the European Commission and the authorities of the Member States. As a result, the regulation is not merely a "ban" but a procedural architecture designed to enable the identification of risks in supply chains and the enforcement of market standards while safeguarding due-process guarantees for economic operators.

The subsequent contribution by Zbigniew Czachór addresses the EU's most fundamental institutional layer: the rule-of-law crisis and the conditionality mechanism for protecting the EU budget. He situates the issue within the post-2020 political and legal dynamics (including the framework of the Multiannual Financial Framework (MFF) and NextGenerationEU) and demonstrates that the rule of law is not solely an axiological category but a prerequisite for sound public financial management. Judicial independence, the effectiveness of oversight and prosecution of abuses, and the practical enforceability of judicial decisions

directly determine the EU's capacity to protect its financial interests. In this sense, the conditionality mechanism functions as an "institutional safety valve" in times of crisis, when normative coherence becomes an element of systemic security.

The notion of security is subsequently "brought down" to the level of everyday market relations by Mira Malczyńska-Biały, who argues that information constitutes one of the key components of consumer safety. Information asymmetries between professional market actors and consumers create vulnerabilities to unfair practices; consequently, effective protection requires both legal instruments (information duties, labelling standards, and prohibitions of misleading conduct) and organisational and educational measures that enable consumers to make rational choices and pursue claims effectively. The author traces the continuity of this logic in consumer policy programmes from the European Economic Community to the contemporary EU, thereby embedding "information security" within a broader architecture of socio-economic resilience.

Part III is concluded by Martyna Kaczmarczyk's contribution, which links security to technological transformation. She discusses ethical, moral, and security risks associated with AI systems in light of emerging European regulations, emphasising that the pace of technological development may generate tensions around human rights, democracy, and the rule of law. This, in turn, requires legal frameworks capable of being updated in step with technological progress – particularly with regard to liability for harm and the effective enforcement of standards. Taken together, Part III yields a coherent conclusion: in an era of crises, the security of states and the EU increasingly depends on the quality of law (definitions, competences, and procedures), the interoperability of institutions and information systems, and regulatory capacity to address new sources of risk – from war and crime, through supply chains, to algorithms and market information.

Part IV of the volume convincingly brings the issue's overall narrative to a close by demonstrating that, in times of crisis, security is increasingly "experienced socially" – as an intersection of risks to health and livelihoods, the stability of local communities, and the EU's political and normative cohesion. Tomasz Marcinkowski examines health security in the European Union during the implementation of the COVID-19 vaccination strategy, emphasising that the effectiveness of crisis-response measures had two inseparable dimensions: a "hard" one (ensuring vaccine quality, efficacy, and safety, alongside the adaptation of regulatory procedures) and a "soft" one (social trust built through transparent communication and countering disinformation). He shows how technocratic and institutional solutions – such as accelerated assessment and authorisation

mechanisms for medicinal products and strengthened post-marketing safety monitoring – played a crucial role in this architecture, while also arguing that the pandemic exposed prior limitations of supranational competences in the area of public health. The conclusion is distinctly systemic: even the most "medical" security policy fails without social legitimacy, and that legitimacy depends on institutional credibility and the quality of communication in an environment marked by informational polarisation.

This line of argument is deepened in Oliwia Radkiewicz's study, which – using the September 2024 flood in Poland as a case – reveals how an infrastructural crisis can evolve into a social crisis. She demonstrates that natural disasters produce multidimensional consequences, ranging from material losses to long-term psychological effects and the erosion of social ties, and that the ultimate security balance depends on the quality of the "interface" between institutions and citizens. Her qualitative research suggests that initial mobilisation and neighbourhood solidarity may, over time, give way to tensions – particularly when public assistance is perceived as inconsistent, burdened by excessive bureaucracy, and unequal in access. Especially salient is her observation of "procedural barriers" that disproportionately affect residents of smaller localities and individuals with lower educational capital, directly shaping subjective perceptions of security and trust in the state. Radkiewicz therefore argues for combining bottom-up resilience (self-organisation and mutual aid) with improved crisis management (early warning, coordinated evacuation, streamlined procedures, and psychological support), since only such synergy can reduce the long-term social costs of disasters.

Wiktoria Trybuł-Klein, in turn, frames irregular migration as a challenge that in the twenty-first century destabilises security not only in terms of borders and public order, but also with regard to political cohesion and intra-EU solidarity. She shows that rising migratory pressure – particularly after 2015 and, subsequently, amid hybrid threats on the eastern flank – has exposed the limitations of existing migration and asylum governance mechanisms, while also revealing a tendency within the EU to shift priorities towards border control, return procedures, and cooperation with third countries. At the same time, she stresses that this turn generates enduring tensions: between security and human-rights protection standards, between operational effectiveness and the principle of solidarity, and between national policy logics and the need for coherence within the Schengen regime. In consequence, Part IV culminates in a conclusion about the "social sensitivity" of security systems: health crises, natural disasters, and migratory pressures demonstrate that the resilience of states and the EU is a function not

only of institutions and resources, but also of trust, equality of access to support, and the capacity to sustain collective legitimacy under conditions of axiological disputes and political polarisation.

The analyses brought together in this volume demonstrate that European security has reached a critical juncture at which established response models no longer match the scale and complexity of contemporary threats. A common thread running through all the studies presented here is the conviction that Europe's resilience will depend not only on military capabilities, but also on the quality of its institutions, social cohesion, transparent regulatory frameworks, and the capacity to cooperate across national borders and sectoral divides. The volume shows that security must be approached as a multidimensional category – encompassing geopolitics, law, technology, the economy, and the social sphere – and that an effective response to emerging challenges requires continuous learning, adaptive governance, and strategic imagination. The future of Europe's security architecture will therefore be shaped as much by political will as by a shared responsibility for the character of the common order.