Studia Administracji i Bezpieczeństwa
nr 19 (2025)
s. 193–218

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.