Information resilience of society and sustainable democratic development in the context of political transformations

Sergii Balan[*], *Vadym Vorotynskyy*[**], *Valerii Patalakha*[***], *Iryna Rybak*[****], *Volodymyr Tarasiuk*[*****]

Abstract

The study analyzes information resilience in Ukrainian and German societies and assesses its implications for political transformations and sustainable democratic development. Using comparative public policy analysis, content analysis of legislative initiatives, and evaluations of media literacy and public resistance to disinformation, the research compares state and societal responses. Findings show that in Ukraine, information resilience is shaped by hybrid warfare and sustained information attacks, with polarization and low trust in official sources as key constraints. In Germany, policy prioritizes countering online extremism, preventing foreign interference, and regulating digital platforms under the Network Enforcement Act, yet election-period disinformation remains impactful despite higher media literacy. Consistent information policy and close collaboration with civil society and international partners can enhance adaptive capacity, protect democratic deliberation, and sustain institutional trust.

Keywords: disinformation, media literacy, propaganda, sustainable development, polarisation.

First submission: 23/09/2025, accepted: 27/11/2025

[*] Department of Interdisciplinary and Comparative Legal Studies, V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine, Kyiv, Ukraine.
** Department of Interdisciplinary and Comparative Legal Studies, V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine, Kyiv, Ukraine.
*** Department of Interdisciplinary and Comparative Legal Studies, V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine, Kyiv, Ukraine.
**** Department of International Relations and Journalism, "KROK" University, Kyiv, Ukraine.
***** Department of Interdisciplinary and Comparative Legal Studies, V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine, Kyiv, Ukraine.

Rivista di Studi sulla Sostenibilità, (ISSNe 2239-7221), 2025, 2 Thematic Issue

Doi: 10.3280/riss2025oa21091

1. Introduction

The relevance of this study lies in the need for a comparative analysis of Ukraine's and Germany's approaches to information resilience, with the aim of identifying their respective strengths and weaknesses. In the modern world, the information space has become a battleground of global competition, where traditional channels of influence intersect with hybrid warfare tactics, disinformation, opinion manipulation, and coordinated information operations. Information resilience, information security, and media literacy are separate but interrelated concepts. Information resilience refers to a society's ability to withstand and recover from harmful information threats, ensuring the continuity of democratic processes and social cohesion. Information security, on the other hand, focuses on protecting the integrity, confidentiality, and availability of information systems from cyberattacks and other technological threats. Media literacy is the individual and collective ability to critically approach and evaluate media content, recognizing bias, misinformation, and manipulation. While information resilience encompasses both society's response to disinformation and the protection of information, media literacy is a tool within this framework that empowers people to navigate and counter harmful narratives, making it a key component of building resilience.

According to V. Georgievskaya et al. (2021), a society's information resilience is the ability of governmental institutions, civil society, and media organisations to oppose detrimental information influences, stop misleading information, and maintain democratic stability. This idea is becoming more relevant, especially for countries undergoing political upheaval or external involvement, due to rising information threats. The issue is severe in Ukraine.

After 2014, Ukraine's information policy focused on countering disinformation, propaganda, and information sovereignty, according to D.V. Nelipa and V.E. Turenko (2024). These efforts included establishing specialised state bodies like the Centre for Countering Disinformation (CCD) under the National Security and Defence Council (NSDC) and the Centre for Strategic Communications and Information Security under the Ministry of Culture and Information Policy, as well as active collaboration with international cybersecurity and information hygiene partners.

Germany is not in open war, but information threats have increased, affecting its domestic politics, media trust, and information security. O. Churanova and V. Romaniuk (2023) note that external players, particularly the Russian Federation, have used disinformation campaigns, social media manipulation, fake news, and cyber operations to influence. Under martial

law, media management has been crucial to information resilience in Ukraine. Y. Bidzilya et al. (2024) warn that excessive governmental participation in the media may lead to censorship and weaken public trust in official information sources, balancing national security with democratic values of free expression.

The Ukrainian and German information resilience strategies demonstrate the need for a comprehensive approach that incorporates legislative regulation, digital literacy improvement, and cybersecurity tools. According to O. Butyrsky (2024), modern information policy should promote thought plurality, high-quality media material, and public trust in official sources. Ukraine and Germany share information policy tendencies despite different threat situations.

This study analyses information resilience in Ukraine and Germany, focussing on key factors affecting information security and its impact on political transformations, democratic institutions, and social cohesion. The study's main goals are to theoretically examine "information resilience" and information security principles, assess the impact of political crises and transformation processes on state information resilience, accounting for internal and external factors, and develop recommendations to strengthen national information resilience.

2. Materials and Methods

This study employed a comprehensive interdisciplinary approach to analyze societal information resilience amid political transformations. Conducted in three phases from September 2024 to January 2025, it focused on Ukraine and Germany due to their distinct information security challenges. Ukraine confronts extensive disinformation campaigns caused by the war with Russia, hybrid threats, and social polarization. Conversely, Germany faces significant external disinformation pressures related to the migration crisis, electoral processes, and extremist influences.

The study employed content analysis, comparative analysis, and case study methodology. Content analysis was applied to examine regulatory frameworks and strategic initiatives, including the Digital Services Act (2022), the Network Enforcement Act (2017), Presidential Decree No. 685/2021 of Ukraine "On the Decision of the National Security and Defense Council of Ukraine "On the Information Security Strategy", and the 2022 Decree on implementing a unified information policy under martial law. Analytical sources such as reports from the Federal Ministry of the Interior (2024a, 2024b), digital technology overviews from Data Reportal

(Kemp, 2025), studies by the Open Society Institute – Sofia (Lessenski, 2022, 2023), and analyses from Media Detector (2024) were also reviewed. This allowed for the identification of key policy domains and institutional measures aimed at safeguarding the information space.

Comparative analysis was employed to examine Ukraine's and Germany's responses to disinformation, with a focus on media literacy initiatives and institutional resilience. The study reviewed reports from international organizations, including the Council of Europe (Doublet, 2019) and Freedom House (2024), as well as media monitoring projects by Reporters Without Borders (2024), StopFake (2025), VoxUkraine (2025), and Correctiv (2025). The case study method was used to investigate specific instances of disinformation and propaganda, including findings from EU DisinfoLab (2025), interference in the 2025 German elections (Litnarovych, 2025; Escritt, 2025; Reuters, 2025), manipulative coverage of the refugee issue (Morris and Oremus, 2022), and information attacks on Ukraine (Mykhailiv, 2025; Oliarnyk, 2022). This enabled the identification of dominant narratives and instruments of information influence, as well as institutional response mechanisms.

The research was conducted in three stages. The first involved collecting and classifying regulatory and institutional frameworks, including national legislation and documents from international organizations. The second stage focused on content analysis of strategies, laws, and analytical reports, followed by the interpretation of prevailing approaches. The third stage employed comparative analysis and case studies to examine models of information resilience in Ukraine and Germany. This analysis enabled the identification of key trends in the development of sustainable information environments and an assessment of the effectiveness of existing mechanisms within the context of international coordination. The review of primary sources also revealed significant limitations, including the absence of unified response standards, weak institutionalization of intergovernmental cooperation, and fragmentation across national strategies.

3. Results

3.1. The role of information resilience in ensuring democratic stability

Information resilience is a multidimensional concept that reflects a society's capacity to withstand harmful informational influences while preserving institutional stability and maintaining the secure functioning of its information environment. It encompasses political, social, and security

dimensions that interact to shape a society's overall resistance to information threats. From a political perspective, information resilience is closely linked to the role of state policy and institutions in safeguarding the information space. The effectiveness of governance depends on the state's ability to design and implement strategies that address both external and internal threats. In the context of hybrid warfare and information attacks, legislative and institutional frameworks are essential for enhancing societal resistance to destabilizing narratives.

Information resilience is a complex concept that can be partially operationalized using cross-national indices such as media literacy and trust levels, but it is more effectively understood as a contextual phenomenon shaped by historical and political conditions. While indices can provide valuable comparative data, they do not always fully reflect the nuances of resilience development in different socio-political contexts. For example, the challenges Ukraine faces in relation to hybrid warfare and disinformation campaigns may require different resilience strategies than those needed in Germany, where external interference plays a more prominent role. Therefore, while cross-national indicators provide useful information, information resilience must be adapted to the specific political and historical context of each country to take into account its unique vulnerabilities and needs.

The sociological perspective emphasises how information processes affect social cohesion, public opinion, and stability. Information technology's rapid progress has made deception and manipulation easier, potentially fuelling societal conflict. Security approaches regard information resilience as essential to national security (Varnaliy et al., 2016). Information is now a strategic factor that can cause technology failures, military conflicts, public administration disturbances, and other problems. Social polarisation and distrust of governmental institutions make citizens more susceptible to manipulation during political crises (Destek et al., 2025; Ketners, 2025). People who distrust authorities accept other sources of information, regardless of authenticity. Fear appeals are dangerous cognitive tactics because manipulators employ them to induce emotional rather than intellectual reactions (Khoma et al., 2024).

German misinformation techniques were similar during the 2015-2016 refugee crisis and Russia's 2022 invasion of Ukraine. German society was misled about immigration by deceptive narratives about refugee crimes and manipulative narratives regarding the energy crisis and Ukraine support (Morris and Oremus, 2022). The 2016 narrative about "Lisa", a Russian-speaking Berlin youngster purportedly molested by migrants, was invented. Although police denied the claim, the disinformation sparked protests and

influenced politics (Meister, 2016). Disinformation's widespread delegitimisation of state institutions threatens democratic governance long-term. Public distrust in elections, judges, and law enforcement can contribute to election rejection, civic disengagement, and societal instability (Perbawa et al., 2024). These processes may accelerate authoritarian drift, as governments use disinformation to justify censorship, limit free speech, and control the media.

In Germany, legislative measures, most notably the Network Enforcement Act (NetzDG, 2017), have contributed to mitigating information attacks on digital platforms. While Ukraine lacks a dedicated law on countering disinformation, institutional efforts have intensified. In 2021, the Centre for Countering Disinformation (CCD) was established under the National Security and Defence Council to monitor threats and respond to disinformation. The same year, the Centre for Strategic Communications and Information Security (CSCIS) was created within the Ministry of Culture and Information Policy to coordinate strategic communications and enhance societal resilience. In December 2024, the CSCIS was restructured into an independent institution, strengthening Ukraine's strategic communication infrastructure.

EU research show that voters with stronger digital and media literacy are better able to get verified information and resist manipulation, which increases election turnout (Doublet, 2019). Pre-election periods are extremely risky for deceptive campaigns, thus information resilience is crucial. German experience shows that better digital advertising transparency rules and social media misinformation control can dramatically reduce external electoral involvement. Despite encouraging improvements in Ukraine, anonymous information campaigns and bot farm activity highlight the need to refine information security policies.

Media literacy helps citizens spot manipulative content, disinformation, and critical engagement with information flows (Iasechko et al., 2020). The NGO Detector Media yearly publishes a Media Literacy Index in Ukraine to assess the population's ability to resist informational impact and adapt to changing media. Media literacy is assessed via sociological surveys, content analysis, and expert judgements. KIIS and USAID-Internews surveys examine public trust in media, ability to spot misinformation, and critical engagement with content. Detector Media, StopFake, and VoxCheck give qualitative media literacy examinations to uncover information ecosystem weaknesses.

Ukraine's information security strategy combats disinformation, promotes independent media, critical thinking, and digital literacy. International rankings and analytical assessments on freedom of expression

and the information climate examine such policies. Freedom House (2024) rates media independence, availability to objective information, and journalist pressures annually. Reporters Without Borders (2024) tracks journalist threats and state censorship worldwide. The European Digital Media Observatory (EDMO) studies disinformation's social impact and recommends information security policies.

Information stability, as described in the context of political transformation and democratic development, is closely linked to Jürgen Habermas' concept of the public sphere and his theory of deliberative democracy. Habermas emphasizes the role of rational discourse in the public sphere, where citizens can participate in informed debates, shaping public opinion and influencing political decision-making. Within this framework, information resilience becomes a decisive factor in preserving democratic debate.

It ensures that society is able to critically evaluate and counteract disinformation, allowing citizens to participate in constructive discourse. For example, efforts in Ukraine and Germany to combat disinformation through legislative measures, media literacy programs, and civil society engagement reflect the need to create a robust public sphere in which diverse viewpoints can be expressed free from manipulation. Thus, strengthening information resilience is essential for maintaining a democratic space in which deliberative democracy can flourish, ensuring that citizens can fully participate in political processes without being influenced by external or internal information threats.

Societal information resilience underpins stability through the coordinated interaction of state policy, civic activism, and security measures. Its advancement demands a systematic strategy focused on enhancing media literacy, reinforcing legal frameworks against disinformation, and adapting to evolving information threats.

3.2. Comparative analysis of information stability: The experience of Ukraine and Germany

In Ukraine, following the 2014 Revolution of Dignity and the onset of the war with Russia, information attacks intensified significantly. These multifaceted assaults encompassed cyberattacks targeting government agencies, financial institutions, and media outlets, alongside widespread disinformation campaigns, public opinion manipulation, and information-psychological operations. For instance, in February 2022, a large-scale Distributed Denial of Service (DDoS) attack targeted the websites of the Ministry of Defence and two major banks, PrivatBank and Oschadbank

(Oliarnyk, 2022). The strategic objectives of disinformation campaigns typically focus on undermining the state's decision-making capacity, which is vital for stability and security. These attacks erode citizens' trust in democratic processes, diminish social capital, and weaken institutional effectiveness. Additionally, they foster uncertainty and fear, heightening social tensions and destabilizing society. Framed within a sustainability perspective, information resilience contributes to the social sustainability of democracy by preserving the continuity of public deliberation, institutional reliability, and social cohesion over time (Kharchenko et al., 2017).

Russia is the main disinformation supplier in Ukraine. Russia spends approximately $1 billion on media propaganda annually. The 2025 Russian draft state budget allocates over RUB 137 billion (USD 1.4 billion) for state propaganda, up 13% from 2024. These funding focus on discrediting Russia's international and domestic policy. Russian propagandists portray Ukraine as a burden on the EU to ruin its worldwide image. Russian media falsely reported that a Ukrainian soldier killed his partner to defame the Ukrainian army and state (Mykhailiv, 2025). Information attacks cause public unrest, social polarisation, and state institution collapse, threatening national security. Disinformation and manipulation decrease information resilience, reducing citizens' ability to critically analyse and objectively evaluate events. Crisis coordination is complicated by critical infrastructure cyberattacks that interrupt government operations, banking systems, and communication routes (Mikhnevych et al., 2023; 2024). Germany amid the 2015-2016 migration crisis and Russia's global disinformation effort during its 2022 invasion of Ukraine are examples.

From 2022 to 2023, Germany faced significant disinformation attempts to erode popular support for Ukraine and exacerbate social tensions. Russian propaganda aimed to disparage Ukrainian refugees, erode government trust, and incite xenophobia. Operation "Doppelganger" (EU DisinfoLab, 2025) saw many bogus websites imitate Western media outlets like The Guardian, Bild, and Der Spiegel. These sites spread anti-Western myths to undermine Ukraine and European government policy. To lend legitimacy to fake content, the effort mostly used typosquatting, or registering domain names that resembled official ones. Fake social media profiles boosted the reach and impact of misinformation.

The German government increased disinformation detection and countermeasures. A unit to counteract information attacks was established by the Federal Ministry of the Interior and the Ministry of Foreign Affairs in 2024 (Federal Ministry, 2024b). At the same time, authorities tightened social media regulations, requiring fast removal of falsehoods. Operation

"Doppelganger" shows the complexity of modern information threats and the need for constant attention to protect public opinion and national security.

Multiple large-scale disinformation initiatives tried to destabilise democratic processes and alter electoral opinion before the 2025 German federal elections. The CeMAS analytical centre found a Russian campaign boosting the far-right Alternative for Germany (AfD) while criticising major political parties in January 2025 (Litnarovych, 2025). This campaign, linked to the Russian "Doppelganger" operation, used fake news sites to undermine Ukraine and boost economic fears.

In February 2025, researchers discovered over 700 bogus social media profiles called "Geist" that spread pro-Russian disinformation about conservative chancellor candidate Friedrich Merz. The network employed fake photos and anti-conservative messaging to damage his brand and voter support (Escritt, 2025). German Interior Ministry warned of Russian misinformation effort targeting Hamburg and Leipzig elections with false social media videos. This operation, linked to the pro-Russian "Storm-1516" network, used pseudo-media sites and false social media accounts to spread misinformation to subvert democratic processes (Reuters, 2025).

In the face of hybrid threats, state policy is essential for information resilience. Ukraine has established several strategic papers to preserve the information environment, promote media literacy, and combat damaging information influence since 2014. Ukraine's Information Security Strategy requires an early warning system for information threats, improved coordination between state institutions, media, and civil society, and support for independent journalism (Decree of the President..., 2021). For disinformation countermeasures, especially during wartime, the National Security and Defence Council's Strategic Communications Centre and the Ministry of Culture and Information Policy's Centre for Strategic Communications and Information Security are crucial to this strategy.

Ukraine strengthened its information security after the 2022 invasion. Blocking Russian propaganda channels, sanctioning media and information attackers, and creating state communication platforms were among the measures (Decree of the President..., 2022). These activities changed Ukraine's information ecosystem, boosted media trust, and raised disinformation awareness. Along with population media literacy changes, social networks became the main news source (Table 1).

Data analysis reveals a general decline in public trust in the president from 2022 to 2024, reflecting the prolonged military conflict and shifting public sentiment amid the ongoing crisis. However, since reaching a low of 52% trust in December 2024, confidence in President Zelenskyy has gradually increased, rising to 74% by May 2025 (Grushetsky, 2025). Notable shifts

have also occurred in media consumption: while television remained a primary information source in 2022, by 2024 social networks – particularly Telegram and YouTube – surpassed it.

Table 1 - The impact of disinformation on Ukrainian society (2022-2024)

Year	Level of trust in the president	Most popular media resources	Percentage of citizens who consider disinformation to be a serious problem	Level of media literacy
2022	90%	Television, social networks (Telegram, Youtube, Facebook)	61%	81%
2023	77%	Social networks (Telegram, Youtube)	90%	76%
2024	59%	Social networks (Telegram, Youtube)	89%	No data

Source: Compiled by the authors based on Detector Media (2024), EU Neighbours East (2024), Ukrinform (2024), A. Grushetsky (2025).

The paradox of declining trust in political leaders, despite growing awareness of disinformation, can be understood by recognizing that increased awareness often leads to greater skepticism about the reliability of official sources of information. As citizens become more aware of the pervasiveness of disinformation, they may begin to question the reliability of all information, including that provided by political leaders and institutions. This decline in trust occurs because disinformation campaigns exploit existing vulnerabilities in public trust, making people more likely to view state-sanctioned narratives as biased or manipulated rather than reliable sources of truth. Consequently, while recognizing disinformation is crucial, it may inadvertently reinforce public cynicism, thereby undermining trust in institutions rather than strengthening it.

At the federal level, several ministries collectively shape media literacy policy by addressing different facets of the information environment. The Federal Ministry of Digital and Transport regulates digital platforms, while the Federal Ministry of Education and Research supports educational initiatives that enhance media literacy. The Federal Department for Media Harmful to Young Persons manages age-related content restrictions, and the Federal Centre for Health Education runs campaigns on digital hygiene and

mental health. At the state level, the Standing Conference of Ministers of Education and Cultural Affairs develops educational standards, ensuring the integration of media literacy across general, vocational, and higher education curricula. Together, these institutions foster a comprehensive approach to media literacy, emphasizing critical thinking, information analysis, and the ability to evaluate sources, thus contributing to overall information resilience.

Several German laws control the digital environment. The 2017 Act to Improve Law Enforcement in Social Networks was the first significant European law to tackle illegal digital materials like disinformation, hate speech, and extremism. Major German technology corporations must remove blatantly illegal content within 24 hours and seven days for more difficult circumstances under this rule. Failure to comply can result in a EUR 50 million fine. The Digital Services Act (2022) was heavily influenced by the Law to Improve Law Enforcement in Social Networks, which advanced European digital legislation. The former focusses on material removal, whereas the Digital Services Act requires platforms to moderate content, disclose algorithmic transparency, and prevent foreign intervention in democratic processes. A more balanced regulatory approach is promoted by the Act's improved reporting and collaboration procedures between digital platforms and public agencies. Regional educational programs, state-funded media literacy projects, and strict legislation have improved societal information resilience in Germany (Table 2).

Analysis of disinformation's impact on German citizens between 2022 and 2024 reveals a steady rise in public concern over information threats alongside declining trust in political leadership. The gradual erosion of trust in the chancellor appears linked to systematic disinformation campaigns aimed at delegitimizing state institutions. While the Law to Improve Law Enforcement in Social Networks (2017) and the Digital Services Act (2022) set frameworks to control harmful content, their success hinges on state institutions' enforcement capacity and digital platforms' cooperation. At the EU level, combating information manipulation is complicated by the pervasive influence of Russian propaganda, which exploits social media as a hybrid warfare tool – particularly amid rising concerns over foreign interference in democratic processes such as elections and public discourse.

Table 2 - The impact of disinformation on citizens in Germany in the period 2022-2024

Year	Level of trust in the chancellor	Most popular media resources	Percentage of citizens who consider disinformation to be a serious problem (%)	Media Literacy Index, (0-100*)
2022	30%	Television, social networks (WhatsApp, Instagram, Facebook)	77%	62
2023	20%	Television, social networks (WhatsApp, Instagram, Facebook)	84%	61
2024	18%	Television, social networks (WhatsApp, Instagram, Facebook)	81%	No data

*Note: *Media Literacy Index, which determines the level of media literacy in an EU country, is calculated on a 100-point scale.*
Source: Compiled by the authors based on M. Lessenski (2022, 2023), E. Başay (2024), S. Kemp (2025).

Comparative results between Ukraine and Germany show that, although media literacy initiatives and regulatory approaches are crucial for strengthening information resilience, their effectiveness can vary depending on the context and political situation. In Ukraine, where external disinformation campaigns and social polarization are widespread, media literacy programs have helped the public recognize false narratives, although regulatory measures aimed at combating disinformation have also played an important role in controlling external threats.

In Germany, where foreign interference is a serious problem, regulatory frameworks such as the Network Enforcement Act have proven effective in combating harmful content, while media literacy initiatives have strengthened the public's ability to critically evaluate information. The study's findings suggest that a combined approach, in which media literacy programs empower citizens to critically evaluate information and regulatory frameworks ensure the accountability of digital platforms, may be a more sustainable model for resilience. However, the success of this dual strategy depends on the level of public trust, the effectiveness of enforcement mechanisms, and the adaptability of both approaches to emerging information threats.

3.3. Key challenges to information resilience in Ukraine and Germany

Internal socio-political processes and external information attacks polarise Ukraine's information ecosystem. People only read "information bubbles" that support their ideas due to polarisation. Fractionation inhibits public discussion and deepens social divides, which could destabilise the state. In entrenched ideological blocs, social groups reject alternatives and preserve opposing views, especially on national security. A Razumkov Centre (2021) study found that 21% of eastern Ukrainians desire Russian-Ukrainian unity, compared to 0.4% in western Ukraine.

Also polarised is foreign policy. Ukrainian support for Euro-Atlantic integration decreased substantially after 2022. Over 82% of individuals backed NATO in 2024, up from 47.8% in 2021 (Razumkov Centre, 2024). Another issue is poor trust in state media due to oligarchic media control, political meddling in editorial decisions, and inefficient state communication strategies that fail to respond to information threats. While censoring pro-Russian propaganda and punishing destructive content are important for national security in the wake of a full-scale invasion, Reporters Without Borders and the OSCE have warned against free expression abuses in Ukraine.

Germany struggles with foreign electoral intervention and influence. Russia and China have expanded social media disinformation tactics and supported fringe political groups to influence public opinion and politics since early 2016. Russian propaganda manipulates migration, energy security, and European integration with bogus news and history. The Russian-linked "Alley of Angels" propaganda effort was revealed in 2025 to undermine German support for arming Ukraine (Saito et al., 2025). The campaign included emotional images of children supposedly murdered in the conflict and was partly organised and distributed by a Russia-affiliated network. European intelligence found that Russian agents worked to influence German protests and politics.

A February 2025 Bitkom study found that approximately 90% of Germans are apprehensive about foreign influence in the next national elections, mostly from Russia (45%) and the US (42%), with China (26%) and Eastern Europe (8%) registering less anxiety. The people is more conscious of the risks foreign influence poses to democracy. Germany's Federal Office for the Protection of the Constitution (BfV) formed a working group to prevent foreign intervention in the 23 February 2025 early federal elections (Federal Ministry of the Interior, 2024a). This followed threats of Russian espionage and sabotage. The BfV noted that disinformation,

cyberattacks, espionage, and sabotage might influence elections to discredit or support politicians.

Regulating online platforms in Germany involves complex legal and technological dimensions. The 2017 Law to Improve Law Enforcement in Social Networks was among Europe's earliest regulations targeting illegal content. However, it has generated debate among human rights advocates, digital technology experts, and platform operators. A central concern involves algorithmic modeling and automated content moderation, as many platforms employ artificial intelligence and machine learning to identify potentially illegal material (Işık et al., 2025).

State abuse of the law is another issue. Journalists warned that a government proposal to strengthen the 2017 Law to Improve Law Enforcement in Social Networks could censor political opponents in 2022. A proposed amendment compelled platforms to remove content and provide user data with the Federal Criminal Police Office (European Audiovisual Observatory, 2023), raising data privacy and law enforcement misuse concerns. Germany needs legal reform to address filtering, excessive moderation, and disinformation migration to unregulated platforms.

External assistance from organizations such as the EU, NATO, and the OSCE can strengthen democratic stability by providing technical support, facilitating dialogue, and reinforcing the rule of law, without undermining national sovereignty or domestic legitimacy. However, the key to success lies in how such assistance is formulated and implemented. When external actors cooperate with local institutions, respecting national priorities and ensuring local ownership of reform processes, this can strengthen democratic resilience without compromising sovereignty. Risks arise when external support is perceived as imposing foreign interests or ignoring the national context, which can lead to resistance from domestic actors. Therefore, a balanced approach that aligns external assistance with a country's democratic aspirations is crucial for maintaining both stability and sovereignty.

4. Discussion

The findings support the idea that democratic systems must curb viral disinformation through proportionate measures that preserve media pluralism and civic voice. This explains why content removal alone may harm discourse in Ukraine and Germany. 2024 (de La Brosse & Holt). Ott's sustainability-oriented literacy paradigm emphasises long-term capacity building by integrating critical and civic literacies into formal education and

public communication, enhancing citizens' source evaluation, reducing manipulative narratives, and promoting democratic resilience (Ott, 2024). The sociological dimension, according to N. Myers (2021), emphasises media literacy, critical thinking, and citizen involvement with information. This study supports their media literacy centrality claim but also shows its variation in society.

In the security-oriented perspective, E. Humprecht et al. (2020) view information threats as hybrid warfare and political destabilisation tools. This study agrees with their findings, especially with digital foreign meddling. However, our research supports including internal vulnerabilities such social fragmentation and low institutional trust in the security system. Political crises often lead to disinformation campaigns and deteriorating faith in state institutions, reducing information resilience (Bashtannyk et al., 2020). Crisis makes citizens more susceptible to external and internal manipulation, according to R.P. Bagozzi et al. (2023). Social tensions, distrust of official sources, and instability foster disinformation, propaganda, and panic. When manipulative narratives are used to change public opinion and promote destabilising political views, the threat increases (Tsurkan-Saifulina et al., 2019).

Russia has launched hybrid warfare-related information strikes on Ukraine since 2014, causing military conflict, political instability, and societal discontent. D. Geissler et al. (2023) found that Russia uses state and proxy media, social media, botnets, troll farms, and conspiracy theories to spread disinformation. These attacks aim to undermine trust in governmental, military, volunteer, and disinformation-fighting media. Disinformation efforts in Germany have varied in strength and concentration depending on the political climate. Russian propaganda spread misleading accusations of refugee-related crimes and the imposition of Islamic values on European society during the 2015 migration crisis, according to Piguet (2021).

Despite efforts to improve information resilience, both countries confront major problems, this study revealed. Deep social polarisation, low trust in state media, and legislative risks from excessive information space control are major issues in Ukraine (Fedorchenko et al., 2020; Tsurkan-Saifulina and Dudchenko, 2018). Krykavska et al. (2023) agree that information restrictions may be appropriate during warfare, but a long-term balance between security and free speech is necessary. Kampfner (2020) found that Russia and China interfere in German elections and media. Regulation of online platforms is complicated, with regulations like the 2017 Law to Improve Law Enforcement in Social Networks criticised for censorship and content moderation transparency. The political and historical situations of

Ukraine and Germany differ, yet both governments are implementing thorough disinformation suppression tactics. During the crisis, Ukraine prioritises external threats, whereas Germany prioritises digital legislation and online platform monitoring.

5. Conclusions

Research suggests that media literacy, counter-disinformation measures, independent media, digital regulation, and social cohesion are crucial for societal information resilience during political changes. Media literacy in Ukraine was 81% in 2022 and 76% in 2023, while public acknowledgement of disinformation as a severe problem rose from 61% to 90% to 89% in 2024. Trust in the president fell from 90% in 2022 to 59% in 2024, then recovered to 74% by May 2025. Germany's media literacy scores were 62/100 in 2022 and 61 in 2023, but concern about disinformation rose from 77% to 84% and stayed high. Trust in the chancellor declined from 30% to 20% to 18% in 2024. Rising threat awareness and falling political trust suggest information environment structural vulnerabilities.

In reaction to hybrid warfare, internal polarisation, and low faith in state media, Ukraine has implemented legislative efforts, platform sanctions, and increased strategic communications. Germany prioritises preventing foreign meddling and extremist content under the Law to Improve Law Enforcement in Social Networks and the EU Digital Services Act, but balances free expression with platform accountability as manipulation tactics evolve. Both incidents demonstrate that technical takedowns alone are insufficient without public capability and credible communication. Sustainable democratic development relies on resilient information ecosystems to ensure access to verified knowledge, institutional trust, and media pluralism, aligning with SDG 16. Policy design should prioritise sustainability indicators including stable trust, consistent funding for media and fact-checking, transparent enforcement, algorithmic accountability, and targeted inclusion of vulnerable populations.

References

Bagozzi, R.P., Mari, S., Oklevik, O., Xie, C. (2023). Responses of the public towards the government in times of crisis. *British Journal of Social Psychology*, 62(1), 359-392. Doi: 10.1111/bjso.12566.

Başay, E. (2024). Germans losing trust in government, political institutions: Survey. -- https://www.aa.com.tr/en/middle-east/germans-losing-trust-in-government-political-institutions-survey/3100530#.
Bashtannyk, V., Buryk, Z., Kokhan, M., Vlasenko, T., Skryl, V. (2020). Financial, economic and sustainable development of states within the conditions of industry 4.0. *International Journal of Management*, 11(4), 406-413. Doi: 10.34218/IJM.11.4.2020.040.
Bidzilya, Y., Haladzhun, Z., Solomin, Y., Georgiievska, V., Sydorenko, N. (2024). Ukrainian journalism and media security in conditions of full-scale Russian aggression. *Health, Science and Technology – Conference Series*, 3, 769. Doi: 10.56294/sctconf2024.769.
Butyrsky, O. (2024). Methodological basis of Ukraine's state information policy. *Economics. Management. Innovations*, 2(35), 182-195. Doi: 10.35433/ISSN2410-3748-2024-2(35)-12.
Churanova, O., Romaniuk, V. (2023). Anti-EU narratives through the Russian-Ukrainian war in the light of StopFake.org's debunks. In: D. Catalan-Matamoros (Coord.), *Disinformation and Fact-Checking in Contemporary Society* (pp. 39-61). Madrid: Dykinson. -- https://www.researchgate.net/publication/376516799_Disinformation_and_Fact-Checking_in_Contemporary_Society.
Correctiv (2025). *About us*. -- https://correctiv.org/ueber-uns/.
de La Brosse, R., & Holt, K. (2024). Sustainability of the Democratic System Versus Viral Disinformation Campaigns. *Contemporary Mediterranean*, 3(1), 1-14.
Decree of the President of Ukraine "On the Decision of the National Security and Defense Council of Ukraine "On the Implementation of a Unified Information Policy under Martial Law"" (2022). -- https://zakon.rada.gov.ua/laws/show/152/2022?lang=en#Text.
Decree of the President of Ukraine No. 685/2021 "On the Decision of the National Security and Defense Council of Ukraine of 'On the Information Security Strategy'" (2021). -- https://www.president.gov.ua/documents/6852021-41069.
Destek, M.A., Usman, M., Saqib, N. 2025. Do political cooperations and regulations manage Africa's sustainable mineral policy?. *Resources Policy*, 102, 105494. Doi: 10.1016/j.resourpol.2025.105494.
Detector Media (2024). Media literacy index of Ukrainians: 2020-2023 fourth wave. -- https://en.detector.media/post/media-literacy-index-of-ukrainians-2020-2023-fourth-wave.
Digital Services Act (2022). -- https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.
Doublet, Y.M. (2019). *Disinformation and electoral campaigns*. Strasbourg: Council of Europe Publishing. -- https://rm.coe.int/disinformation-and-electoral-campaigns-research/16809f1618.
Escritt, T. (2025). Friedrich Merz targeted by pro-Russian disinformation before German vote, researchers say. -- https://www.reuters.com/world/europe/friedrich-merz-targeted-by-pro-russian-disinformation-before-german-vote-2025-02-20/.

EU DisinfoLab (2025). *What is the Doppelganger operation? List of resources*. -- https://www.disinfo.eu/doppelganger-operation/.

EU Neighbours East (2024). *Public opinion poll for the EU Advisory Mission Ukraine*. -- https://euneighbourseast.eu/news/publications/public-opinion-survey-for-the-eu-advisory-mission-ukraine/.

European Audiovisual Observatory (2023). *Cologne Administrative Court: New Network Enforcement Act provisions breach EU law*. -- https://merlin.obs.coe.int/article/9442.

Federal Ministry of the Interior (2024a). *Protecting the 2025 federal election from hybrid threats and disinformation*. -- https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation-bei-bt-wahl/desinfo-bei-bt-wahl-artikel.html.

Federal Ministry of the Interior (2024b). *What is the Federal Government doing to protect the 2025 Bundestag elections from illegitimate foreign influence*. -- https://www.bmi.bund.de/SharedDocs/faqs/EN/topics/disinformation/bt_wahl_2025/6_protection_from_influence.html.

Fedorchenko, N.V., Shymon, S.I., Vyshnovetska, S.V., Mikhnevych, L.V., Bazhenov, M.I. (2020). Community Organisation as a Subject of Civil Relations According to Law of Ukraine and CIS Countries. *Memoria E Ricerca*, 1, 353-370. Doi: 10.4478/98143.

Freedom House (2024). Countries and territories. -- https://freedomhouse.org/countries/freedom-net/scores?sort=desc&order=Total%20Score%20and%20Status.

Geissler, D., Bär, D., Pröllochs, N., Feuerriegel, S. (2023). Russian propaganda on social media during the 2022 invasion of Ukraine. *EPJ Data Science,* 12, 35. Doi: 10.1140/epjds/s13688-023-00414-5.

Georgievskaya, V., Bidzilya, Y.M., Solomin, Y.O., Shapovalova, H.V., Poplavska, N.M. (2021). The stability of State information in the face of terrorist threats. *Political Issues*, 39(70), 250-269.

Grushetsky, A. (2025). *Dynamics of trust in president V. Zelensky in 2019-2025*. -- https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1496&page=1.

Humprecht, E., Esser, F., Van Aelst, P. (2020). Resilience to online disinformation: A framework for cross-national comparative research. *International Journal of Press/Politics*, 25(3), 493-516. Doi: 10.1177/1940161219900126.

Iasechko, S., Haliantych, M.K., Skomorovskyi, V.B., Zadorozhnyi, V., Obryvkina, O., Pohrebniak, O. (2020). Contractual relations in the information sphere. *Systematic Reviews in Pharmacy*, 11(8), 301-303.

Işık, C., Ongan, S., Islam, H., Yan, J., Alvarado, R., Ahmad, M. (2025). The nexus of economic growth, energy prices, climate policy uncertainty (CPU), and digitalization on ESG performance in the USA. *Climate Services*, 38, 100572. Doi: 10.1016/j.cliser.2025.100572.

Kampfner, J. (2020). Media influence. In: J. Kampfner, *Russia and China in Germany* (pp. 11-14). London: Royal United Services Institute. -- http://www.jstor.org/stable/resrep41859.6.

Kemp, S. (2025). Digital 2025: Germany. Doi: https://datareportal.com/reports/digital-2025-germany.
Ketners, K. (2025). Adaptation of State Security to Modern Military Operations and Terrorist Risks in the World. *Space and Culture India*, 13(1), 1-5. Doi: 10.20896/e3p2jm77.
Kharchenko, V., Ponochovnyi, Y., Qahtan, A.-S.M., Boyarchuk, A. (2017). Security and availability models for smart building automation systems. *International Journal of Computing*, 16(4), 194-202.
Khoma, I., Fedushko, S., Kunch, Z. (2024). *Media manipulations in the coverage of events of the Ukrainian revolution of dignity: Historical, linguistic, and psychological approaches*. Doi: 10.48550/arXiv.2407.17425.
Krykavska, I., Povalena, M., Muzyka, O.Z. 2023. Information threats on the Internet in the conditions of war in Ukraine: Problematic issues of legal regulation. *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences*, 10(3(39)), 82-87. Doi: 10.23939/law2023.39.082.
Law to Improve Law Enforcement in Social Networks (2017). -- https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html.
Lessenski, M. (2022). *Media literacy index 2022: Main findings and possible implications*. Sofia: Open Society Institute – Sofia. -- https://www.osce.org/files/f/documents/0/4/534146.pdf,
Lessenski, M. (2023). *Media literacy index 2023: Measuring vulnerability of societies to disinformation*. Sofia: Open Society Institute – Sofia. -- https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf.
Litnarovych, V. (2025). Russia targets German election with disinformation campaign, backs far-right AfD. -- https://united24media.com/latest-news/russia-targets-german-election-with-disinformation-campaign-backs-far-right-afd-5225.
Meister, S. (2016). The "Lisa case": Germany as a target of Russian disinformation. -- https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html.
Mikhnevych, L., Luchko, I., Gahramanova, N., Dubova, O., Myskovets, I. (2024). The Role of Legal Mechanisms in Ensuring Biodiversity at National and International Levels. *Evergreen*, 11(4), 2806-2817. Doi: 10.5109/7326925.
Mikhnevych, L., Vasylchuk, L., Hryhorenko, A., Rud, Y. (2023). Constitutional model of parliamentary immunity: Ukrainian and European experience. *JUS Rivista di Scienze Giuridiche*, 2023(3), 210-229. Doi: 10.26350/18277942_000133.
Morris, L., Oremus, W. (2022). Russian disinformation is demonizing Ukrainian refugees. -- https://www.washingtonpost.com/technology/2022/12/08/russian-disinfo-ukrainian-refugees-germany/.
Myers, N. (2021). Information sharing and community resilience: Toward a whole community approach to surveillance and combatting the "infodemic". *World Medical & Health Policy*, 13(3), 581-592. Doi: 10.1002/wmh3.428.
Mykhailiv, V. (2025). "Ukraine is becoming a burden for the EU". A review of Russian propaganda for January 20-26, 2025. --

https://detector.media/monitorynh-internetu/article/237670/2025-01-29-ukraina-peretvoryuietsya-na-tyagar-dlya-ies-oglyad-rosiyskoi-propagandy-za-2026-sichnya-2025-roku/.
Nelipa, D.V., Turenko, V.E. (2024). Key aspects of humanitarian policy as a counteraction to the information warfare of the Russian Federation. *Political Life*, 1, 94-99. Doi: 10.31558/2519-2949.2024.1.14.
Oliarnyk, M. (2022). *Hackers attacked PrivatBank. Has Ukraine become a training ground for a cyberattack on NATO?* -- https://zaborona.com/hakery-atakuvaly-pryvatbank-ukrayina-stala-polem-dlya-trenuvan-kibernapadu-na-nato/.
Ott, B. L. (2024). Communicating for Sustainability in the Digital Age: Toward a New Paradigm of Literacy. *Challenges*, 15(2), 29. Doi: 10.3390/challe15020029.
Perbawa, K.S.L.P., Hanum, W.N., Atabekov, A.K. (2024). Industrialization of Election Infringement in Simultaneous Elections: Lessons from Sweden. *Journal of Human Rights Culture and Legal System*, 4(2), 477-509.
Piguet, E. (2021). The "refugee crisis" in Europe: Shortening distances, containment and asymmetry of rights – A Tentative interpretation of the 2015-16 events. *Journal of Refugee Studies*, 34(2), 1577-1594. Doi: 10.1093/jrs/feaa015.
Razumkov Center (2021). Assessment by Ukrainian citizens of the main theses of V. Putin's article "On the historical unity of Russians and Ukrainians" (July-August 2021). -- https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-gromadianamy-ukrainy-golovnykh-tez-statti-v-putina-pro-istorychnu-iednist-rosiian-ta-ukraintsiv.
Razumkov Center (2024). *Citizens' support for Ukraine's accession to the European Union and NATO. Attitudes towards foreign states. Attitudes towards peace negotiations* (September 2024). -- https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/pidtrymka-gromadianamy-vstupu-ukrainy-do-yevropeiskogo-soiuzu-ta-nato-stavlennia-do-inozemnykh-derzhav-stavlennia-do-myrnykh-peregovoriv-veresen-2024r.
Reporters without Borders (2024). *Global monitoring of press freedom*. -- https://rsf.org/en/index.
Reuters (2025). *Germany warns of Russian disinformation targeting election*. -- https://www.reuters.com/world/europe/germany-warns-russian-disinformation-targeting-election-2025-02-21/.
Saito, M., Hummel, T., Zverev, A., Nikolskaya, P., Tsvetkova, M. (2025). *Russia-linked propaganda campaign pushes to undercut German support for Ukraine*. -- https://www.reuters.com/investigations/russia-linked-propaganda-campaign-pushes-undercut-german-support-ukraine-2025-02-18/.
Shelton, J. (2025). *Germany: Nearly 90% of voters fear manipulation*. -- https://www.dw.com/en/germany-nearly-90-of-voters-fear-foreign-manipulation/a-71528481.
StopFake (2025). *About us*. -- https://www.stopfake.org/uk/pro-nas/.
Tsurkan-Saifulina, Y.V., Dudchenko, V.V. (2018). Authority of law system formation: Applied analysis of legal system unity. *Journal of Legal Ethical and Regulatory Issues*, 21(Special Issue 1), 1-11. --

https://dspace.onua.edu.ua/server/api/core/bitstreams/d685f29d-f42a-43a5-a717-d790a82a1928/content.
Tsurkan-Saifulina, Y.V., Vitman, K.M., Kolodin, D.A. (2019). Certain aspects of interaction between the state and civil law in CIS countries. *Asia Life Sciences*, 2, 697-717.
Ukrinform (2024). *The main sources of information for most Ukrainians are Telegram channels and YouTube*. -- https://www.ukrinform.ua/rubric-society/3920830-osnovnimi-dzerelami-informacii-dla-bilsosti-ukrainciv-e-telegramkanali-ta-youtube.html.
Varnaliy, Z., Onishchenko, S., Masliy, A. (2016). Threat prevention mechanisms of Ukraine's economic security. *Economic Annals-XXI*, 159(5-6), 20-24. Doi: 10.21003/ea.V159-04.
VoxUkraine (2025). *Vox Ukraine idea*. -- https://voxukraine.org/about-us.