DOI: http://doi.org/10.31617/1.2025(164)03
UDC 351.86(477)"2021/2024"=111

SHKUROPADSKA Diana
https://orcid.org/0000-0002-6883-711X

PhD (Economics), Associate Professor
at the Department of Economics
and Competition Policy
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
diana.shkuropadska2016@knute.edu.ua

LEBEDEVA Larysa
https://orcid.org/0000-0001-8632-5460

PhD (Economics), Associate Professor,
Associate Professor at the Department
of Economics and Competition Policy
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
l.lebedeva@knute.edu.ua

INFORMATION RESILIENCE OF UKRAINE: 2021–2024

The escalation of russia's hybrid warfare, particularly its disinformation campaigns, has created critical threats to national security in Eastern Europe. Ukraine represents a unique case, where information resilience has become both a defensive necessity and a strategic tool in safeguarding sovereignty, maintaining democratic development, and mobilizing international support. The aim of the research is to identify the main directions of russia's information warfare against Ukraine and to assess the domains of ensuring information resilience. The hypothesis of this article is put forward that the information resilience of a state is contingent upon the balanced interplay of societal, institutional-legal, media, and digital dimensions, which collectively determine the capacity of society to withstand disinformation and other manifestations of hybrid warfare. The research applies the Disinformation Resilience Index (DRI) as the primary analytical tool. This index measures resilience across such key dimensions as social, legal, institutional, media and digital resilience. Comparative analysis was conducted for Ukraine, Visegrad countries, belarus, Moldova, Armenia, Azerbaijan, and Georgia during 2021–2024. Findings indicate that Ukraine has significantly improved resilience across all three dimensions,

ШКУРОПАДСЬКА Діана
https://orcid.org/0000-0002-6883-711X

доктор філософії, доцент кафедри економічної
теорії та конкурентної політики
Державного торговельно-економічного
університету
вул. Кіото, 19, м. Київ, 02156, Україна
diana.shkuropadska2016@knute.edu.ua

ЛЕБЕДЕВА Лариса
https://orcid.org/0000-0001-8632-5460

к. е. н., доцент, доцент кафедри економічної
теорії та конкурентної політики
Державного торговельно-економічного
університету
вул. Кіото, 19, м. Київ, 02156, Україна
l.lebedeva@knute.edu.ua

ІНФОРМАЦІЙНА СТІЙКІСТЬ УКРАЇНИ: 2021–2024 РР.

Ескалація гібридної війни росії, зокрема її дезінформаційних кампаній, створює критичні загрози національній безпеці у країнах Східної Європи. Україна є унікальним прикладом, де інформаційна стійкість стала не лише засобом захисту, але й стратегічним інструментом збереження суверенітету, підтримки демократичного розвитку та мобілізації міжнародної підтримки. Метою дослідження є виявлення основних напрямів інформаційної війни росії проти України та оцінювання сфер забезпечення інформаційної стійкості. Висунуто гіпотезу, що інформаційна стійкість держави залежить від збалансованої взаємодії суспільної, інституційно-правової, медійної та цифрової складових, які разом визначають здатність суспільства протистояти дезінформації та іншим проявам гібридної війни. Основним аналітичним інструментом є Індекс стійкості до дезінформації (DRI), що охоплює такі ключові виміри: суспільну, правову та інституційну, а також медійну й цифрову стійкість. Порівняльний аналіз проведено для України, країн Вишеградської групи, білорусі, Молдови, Вірменії, Азербайджану та Грузії за період 2021–2024 рр. Дослідження показало, що Україна суттєво підвищила рівень інформаційної стійкості в усіх сферах, головним чином у відповідь на повномасштабне вторгнення

largely as a response to russia's full-scale invasion in 2022. Governmental and societal initiatives, ranging from cyber defense, international communication campaigns, to digital literacy programs, have enhanced Ukraine's ability to counter disinformation. In contrast, Visegrad countries showed mixed results, with notable regress in Hungary, while belarus demonstrated a sharp decline across all indicators, reflecting its informational dependence on russia. The analysis highlights that countries that directly border russia or have long been subject to its political, economic, or cultural influence tend to be more vulnerable to information manipulation.

Keywords: information resilience, disinformation, hybrid threats, Ukraine, national security, Disinformation Resilience Index.

росії у 2022 р. Серед ключових заходів – посилення кіберзахисту, міжнародні інформаційні кампанії, розвиток цифрової грамотності та медійної стійкості. На відміну від України країни Вишеградської групи мають суперечливі результати, зокрема значний регрес в Угорщині, тоді як білорусь показала різке послаблення усіх компонентів стійкості через інформаційну залежність від росії. Результати аналізу свідчать, що країни, які безпосередньо межують з росією або тривалий час перебували під її політичним, економічним чи культурним впливом, зазвичай є більш вразливими до інформаційних маніпуляцій.

Ключові слова: інформаційна стійкість, дезінформація, гібридні загрози, Україна, національна безпека, Індекс стійкості до дезінформації.

JEL Classification: D83, F52, L86, O52.

Introduction

Russia's full-scale armed aggression against Ukraine is accompanied by large-scale information and psychological operations aimed at undermining national unity, demoralizing the population, discrediting state institutions, and distorting reality in the international information space. The information sphere has turned into a separate theatre of military operations, where technologies of social consciousness manipulation, disinformation, cyber threats, and other instruments of hybrid warfare are widely employed. Under the conditions of intensive hostile information attacks, the need to ensure information resilience as one of the key elements of the country's national security is steadily increasing.

Ukrainian and foreign scholars are actively researching the issue of information resilience and the mechanisms for ensuring it. The study of information resilience, the factors shaping it, and the existing threats has been addressed in the works of Bilynska and Korolchuk (2018). Horbulin (2009) focuses on the issues of information operations and their influence on social security, Koval (2019) discusses approaches to defining evaluation criteria of Ukraine's information and psychological resilience. Kyrychenko et al. (2025) conducted an analysis of how information attacks, disinformation, and propaganda affect public consciousness and national security, identifying them as key threats to information resilience. Gladysh et al. (2023) examine the information resilience of Ukraine and the European Union in the context of russian aggression, emphasizing the communicative aspects of information resilience, focusing on countering hostile content that threatens the cognitive stability of Ukrainian citizens rather than solely on technological cybersecurity measures.

Gnatiuk et al. (2022) analyze the stability and resilience of national information infrastructure, highlighting how modern cyber threats and incidents impact the continuity and robustness of critical communication systems.

Oleksiyuk (2025) highlights the importance of proactively disclosing verified information to counter disinformation and maintain societal stability

during crises, with recommendations to strengthen legislation, digital infrastructure, and official communication systems to enhance societal resilience.

The research of information resilience emphasising the capability to maintain information integrity and usability amid misinformation, disinformation, cyber-attacks, or other threats has been done by Uusikylä et al. (2024) and Dragomir et al. (2024).

Information resilience as a way for managing difficulties in different environmental and social conditions benween workers is reflected in the works of Bronstein (2019), Lloyd (2015), Nicol et al. (2022).

Sadiq et al. (2022) argue that information resilience includes not only responsible approaches, such as proper data governance, safeguarding privacy, and ensuring ethical use of information, but also adaptive approaches, which involve developing flexible strategies, responding promptly to shifts, and maintaining agility in managing information.

The hypothesis of this research puts forward that the information resilience of a state is contingent upon the balanced interplay of societal, institutional-legal, media, and digital dimensions, which collectively determine the capacity of society to withstand disinformation and other manifestations of hybrid warfare.

The aim of the research is to identify the main directions of russia's information warfare against Ukraine and to assess the domains of ensuring information resilience.

To achieve the aim, the combination of general scientific and specific methods was applied. Content analysis was used to examine the narratives and tools of russian information warfare against Ukraine. Comparative analysis was applied to assess the results of the Disinformation Resilience Index for Ukraine and selected Central and Eastern European countries. Statistical analysis was employed to interpret numerical indicators of information resilience across societal, institutional-legal, media, and digital domains. In addition, the case study method was used to illustrate specific examples of disinformation campaigns, while systematization and generalization allowed for the identification of key directions and mechanisms of ensuring information resilience.

The structure of the article is as follows: first, the directions and measures of russia's information warfare against Ukraine are analyzed; then, a comparative analysis of the results of the Disinformation Resilience Index for Ukraine and the countries of Central and Eastern Europe is conducted, namely the Czech Republic, Hungary, Poland, Slovakia, Moldova, belarus, Armenia, Azerbaijan, and Georgia; finally, the conclusions of the study are presented.

1. Directions of russia's information warfare against Ukraine

In contemporary conditions, information warfare is an integral component of hybrid warfare, which combines traditional military actions with non-military methods such as information operations, cyberattacks,

economic pressure, political destabilization, and psychological warfare. Since at least 2014, russia has employed the full spectrum of aggressive tools against Ukraine, particularly targeting public opinion. The main directions of russia's information warfare against Ukraine are presented in *Table 1*.

Table 1

Directions and measures of russia's information warfare

Directions	Measures
Disinformation	Spreading fake news about the Ukrainian army, politics, economy, and international relations; staging and fabricating events that never occurred in order to discredit Ukraine; using deepfake videos and photomontage
Propaganda	Promoting Kremlin narratives; glorifying russian soldiers and devaluing the Armed Forces of Ukraine
Undermining national unity	Inciting hostility between regions, linguistic, and religious groups; fostering distrust in the government, doubts about Ukraine's victory, and fuelling panic; supporting pro-russian political forces and media
Cybercrime and cyberattacks	Hacking government websites and posting fake information; spreading malware through phishing attacks; injecting disinformation into social networks via bots and trolls
Information-psychological operations (IPSO)	Manipulating citizens' emotions, creating an effect of "betrayal" or "war fatigue"; intimidating the population with missile strikes, mobilization, and narratives of "inevitable defeat"
International disinformation	Shaping a false image of Ukraine abroad as a "corrupt" or "ungrateful" state; attempting to discredit Ukrainian refugees and spreading stereotypes in Europe; disseminating pro-Kremlin rhetoric through russia-friendly media outlets in other countries

Source: compiled by the authors.

The capacity to counteract the consequences of disinformation largely depends on information resilience, which can be understood as a society's capability to maintain reliable societal institutions and systems, uphold knowledge-producing organizations that inspire trust, and foster citizenship by promoting media and information literacy that enhances people's skills in recognizing credible sources. A core element of this understanding of information resilience is the presence of healthy level of trust (Staender & Humprecht, 2022).

Disinformation constitutes a de facto restriction of people's rights to access information, to freely form and express opinions, and, more broadly, undermines trust in democratic institutions and justifies war crimes and crimes against humanity. Russia's long-term disinformation campaign against Ukraine violates human rights, as it endangers people's security and lives (RPR, 2023, June 6).

According to international law, disinformation and propaganda constitute violations of the right to freedom of expression, particularly when they promote discrimination or hostility against certain groups, threaten public health, undermine democratic societies, or obstruct individuals' ability to access and exchange information. Such actions contravene multiple international human rights conventions, including Article 19 of the Universal

Declaration of Human Rights, and Articles 19 and 20 of the International Covenant on Civil and Political Rights.

Russian propaganda violates people's right to access impartial and comprehensive information, thereby distorting the perception of reality. Russian propagandists infringe on fundamental human rights by spreading fake news about evacuations from Ukrainian cities under attack, by concealing the crimes of russian troops, and by fabricating reports on the functioning of hospitals during hostilities. Such disinformation exposes people to physical danger: believing it, an individual may remain in a city where it is unsafe to stay, or, conversely, may come under shelling after following false evacuation instructions. Currently, russian propaganda continues to violate the right of individuals to receive unbiased and comprehensive information, thereby distorting societal perceptions of reality (Ukrainian Radio, 2024, July 13).

Russia is also conducting a targeted, multi-level campaign aimed at undermining the national unity of Ukrainian society. Alongside armed aggression, a significant role is played by information-psychological operations designed to fuel social, linguistic, and cultural divisions. The kremlin systematically manipulates issues of language policy, promoting the perception of alleged discrimination against russian-speaking populations and fostering the image of Ukraine as divided into "East" and "West". The religious factor is likewise exploited as a tool of influence, particularly through the support of controlled religious institutions capable of disseminating pro-russian messages among believers. Such actions are directed at weakening social resilience, as they reduce the level of societal cohesion and intensify mutual distrust.

At the same time, an active campaign is underway to discredit government authorities and the Armed Forces of Ukraine by constructing the image of a "weak and corrupt Ukraine" in order to diminish support both domestically and from international partners (Center for Countering Disinformation, n. d.). To achieve this, agents of influence are widely employed, including collaborators, politicians, journalists, bloggers, and opinion leaders, who amplify pro-russian narratives and deepen doubts and divisions within society.

The undermining of national unity is closely linked to the technological instruments of the aggressor, as information manipulation is often reinforced by cybercrime and large-scale cyberattacks aimed at destabilizing the state and eroding trust in its institutions. *The World Cybercrime Index* represents the first global project to rank countries by the level of cybercriminal threat based on expert assessments. It was developed by researchers at the University of Oxford and UNSW Canberra. In April 2024, the results of the World Cybercrime Index were published for the first time, showing that a relatively small group of countries accounts for the majority of global cybercrime threats. Russia topped the ranking, followed by Ukraine, China, the United States, Nigeria, and Romania. The United Kingdom ranked eighth (*Table 2*).

Table 2

World Cybercrime Index in 2024

Ranking	Country	Score	Ranking	Country	Score
1	russia	58.39	11	Iran	4.78
2	Ukraine	36.44	12	belarus	3.87
3	China	27.86	13	Ghana	3.58
4	United States	25.01	14	South Africa	2.58
5	Nigeria	21.28	15	Moldova	2.57
6	Romania	14.83	16	Israel	2.51
7	North Korea	10.61	17	Poland	2.22
8	United Kingdom	9.01	18	Germany	2.17
9	Brazil	8.93	19	Netherlands	1.92
10	India	6.13	20	Latvia	1.68

Source: World Cybercrime Index (University of Oxford, 2024, April 10).

Ukraine's position as the second-ranked country in the World Cybercrime Index can be explained by a combination of structural vulnerabilities and war-related factors. On the one hand, russia's ongoing aggression has made Ukraine a primary target of coordinated cyberattacks, ranging from large-scale assaults on critical infrastructure to constant phishing campaigns and disinformation injections via social media. On the other hand, Ukraine's significant IT sector and its integration into global digital networks make it both a high-value target and a source of potential cybercriminal activity. The ranking thus reflects not only Ukraine's victimization by hostile state-sponsored operations but also the exploitation of its digital environment by transnational cybercriminal groups.

In the context of the russian-Ukrainian war, the positions of russia and Ukraine in the World Cybercrime Index acquire additional significance, since the high rankings of both countries are explained not only by criminal activity but also by military objectives and cyber operations that often blur the line between crime and state strategy. Russian hacker groups, including the well-known Sandworm, Fancy Bear, and others, conduct coordinated attacks on Ukrainian government agencies, energy infrastructure, media outlets, and banks. Some cybercriminal groups operate with tacit approval or under the direct control of intelligence services, using their skills as instruments of cyber espionage, sabotage, and disinformation. Cybercrime and cyberattacks frequently provide the foundation for information-psychological operations, as stolen information, compromised resources, or disrupted communication channels are actively employed to spread disinformation and manipulate public consciousness.

Information-psychological operations (PSYOP) represent a distinct form of information operations, which in practice involve a complex set of coordinated and interconnected forms, methods, and techniques of psychological influence. They consist of political, military, economic, diplomatic, and information-psychological measures directed at individuals or groups with the aim of implanting alien ideological and social constructs, shaping

false behavioral stereotypes, and transforming attitudes, feelings, and will in a desired direction (Derkachenko, 2016).

Russia employs a wide spectrum of information-psychological operations. It disseminates false and manipulative messages aimed at distorting the real picture of events. Examples include fabricated claims about the "surrender of Ukrainian cities", "betrayal by military command", and "massive losses" of the Armed Forces of Ukraine. The main channels of dissemination are anonymous Telegram channels, fake news websites, and forged social media accounts. The objective of such PSYOP is to undermine the morale of both military personnel and the civilian population. Specific tactics include sending SMS and messenger notifications containing intimidation, false information about the deaths of relatives, or calls for capitulation. It is important to note that domestic PSYOP are complemented by an external dimension, as russia simultaneously conducts a large-scale international disinformation campaign aimed at shaping a favorable narrative of the war and discrediting Ukraine in the eyes of the global community.

Russian international disinformation is a multi-level, systemic, and well-financed instrument of hybrid warfare. It is disseminated through russian state-controlled media such as RT and Sputnik, social networks and bot farms, pseudo-experts and sympathetic foreign journalists, as well as third-country media outlets that are formally unconnected to russia. The core narratives include claims of "denazification" and "protection of russian speakers", shifting responsibility for the war onto the West, discrediting Ukrainian statehood, portraying sanctions as more harmful to Europe than to russia, and calling for negotiations with russia as an "inevitable" partner.

Thus, the examined directions of russia’s information warfare are interrelated and mutually reinforcing, forming a multi-layered hybrid warfare strategy designed to weaken Ukraine’s defence capacity. The analysis of these directions further underscores the necessity of developing robust mechanisms for ensuring Ukraine’s information resilience and strengthening international cooperation in the field of countering disinformation.

2. The analysis of Disinformation Resilience Index

Information resilience is defined as the capacity of individuals, communities, and societies to withstand and recover from misinformation, disinformation, and other forms of information manipulation (Rantamäki et al., 2024). To assess the level of a country’s information resilience, it is appropriate to apply the Disinformation Resilience Index (DRI), developed by the EAST Center think tank in cooperation with a network of partners, including *Ukrainian Prism*.

The DRI study covers countries of Central and Eastern Europe, namely Ukraine, the Czech Republic, Hungary, Poland, Slovakia, Moldova, belarus, Armenia, Azerbaijan, and Georgia. The composite index of a

country's resilience to disinformation is constructed from three components: societal resilience, legal and institutional resilience, and media and digital resilience. In 2024, the DRI measures the degree of progress or regression in the information resilience of the assessed countries compared to 2021 (*Figure 1*). The Disinformation Resilience Index (DRI) was constructed on the basis of an expert web survey, which provided assessments of different countries' capacity to resist disinformation.

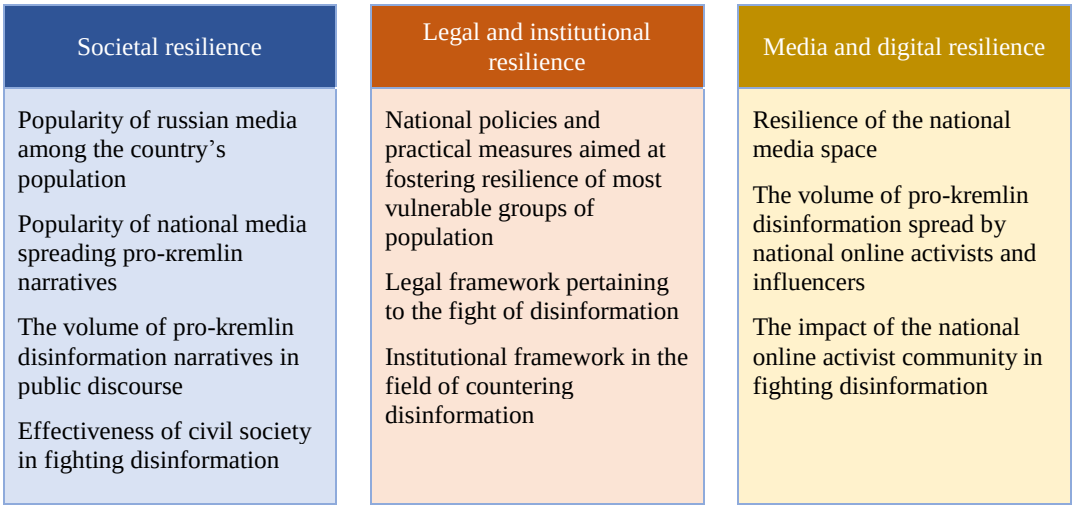

Figure 1. Disinformation Resilience Index (DRI) structure

Source: association for international affairs (2024, December).

The selection of countries for calculating the Disinformation Resilience Index (*Table 3*) was not arbitrary, but based on clear rationale. First, the analysis includes the Visegrad Group states, which, while being members of the European Union, represent a key region for assessing the effectiveness of information security in Central Europe. Second, the Index covers several post-Soviet countries that share historical legacies with russia, geographical proxymity, and remain primary targets of its systemic disinformation campaigns.

Table 3

Disinformation Resilience Index 2024
(The extent and direction of changes since 2021, web-based expert survey)

Countries	Societal resilience	Legal and institutional resilience	Media and digital resilience
Ukraine	1.2	0.8	1
Armenia	1.2	0.3	0.4
Azerbaijan	0.5	0.9	0.6
Moldova	0.3	0.8	0.2
Georgia	0	0	0.3
Poland	0	0.6	–0.3
Czech Republic	–0.2	0.4	0
Slovakia	–0.6	–0.3	0
belarus	–0.6	–1.1	–0.2
Hungary	–0.7	–1.1	–0.5

Source: association for international affairs (2024, December).

The findings reveal a heterogeneous dynamic of disinformation resilience across the assessed states. Ukraine demonstrated substantial progress across all three dimensions: societal resilience increased by +1.2, legal and institutional resilience by +0.8, and media and digital resilience by +1. Notably, under conditions of russia's full-scale invasion, Ukraine introduced a comprehensive set of measures aimed at enhancing resilience in both military and civilian domains, including:

- strengthening the mandates of the State service of special communications and the Ministry of digital transformation for cyber defense of critical infrastructure;
- active engagement of governmental and military press centers to provide timely and reliable information to both domestic and international audiences;
- consistent use of English-language resources to communicate factual accounts of the war globally;
- development of mobile applications such as *Diia* and *Armiia+*, which include educational modules on resilience, cybersecurity, and media literacy;
- cooperation with international partners in the field of cyber defense (NATO, EU, USA);
- mobilization of international technical assistance for upgrading digital infrastructure and securing communications.

Armenia, Azerbaijan and Moldova also registered notable improvements in their DRI scores. For instance, Armenia achieved a considerable increase in societal resilience (+1.2), while making moderate gains in the legal-institutional (+0.3) and media-digital (+0.4) dimensions. Azerbaijan and Moldova, by contrast, recorded more significant progress in legal and institutional resilience, accompanied by smaller advances in societal and media-digital resilience.

In recent years, russia has actively disseminated disinformation in the information sphere of Armenia, Azerbaijan, and Moldova, employing hybrid warfare tools aimed at influencing political stability, public opinion, and the foreign policy orientation of these countries. In Armenia, the main focus has been on campaigns discrediting the government and fuelling social tensions, particularly through the spread of fake news about domestic political conflicts and the security situation along the border with Azerbaijan (Brailian, 2023, October 13) In Azerbaijan, russian media outlets and social networks have been used to disseminate manipulative messages about foreign policy initiatives and interethnic conflicts, aiming to undermine public trust in state institutions and international partners. In Moldova, disinformation campaigns have focused on distorting information related to European integration, corruption scandals, and protest movements, thereby weakening social and political stability (Kennedy & Dunbar, 2025, July).

Georgia has also been a target of russian disinformation campaigns, which rely on manipulating public opinion, fuelling political and social tensions, and spreading fake news concerning the country's foreign policy trajectory and security situation. Russia has paid particular attention to

discrediting government institutions, fostering negative attitudes toward Western integration, and amplifying pro-russian narratives in the media space (Sikharulidze, 2025, March 13). Street protests in Georgia, which began on March 7, 2023, in response to the parliament's support of a "foreign agents" law resembling russian legislation, provided an additional platform for the spread of disinformation and further intensified social tensions. These developments also affected Georgia's position in the Disinformation Resilience Index. Specifically, there were no changes in societal resilience (0) and legal-institutional resilience (0), while only a slight improvement was recorded in media and digital resilience (+0.3).

With respect to the Visegrad Group countries, they demonstrated lower results in the Disinformation Resilience Index. This is likely due to the fact that these states experience a less direct impact from russian disinformation campaigns. Moreover, the Czech Republic, Poland, Slovakia, and Hungary are members of the European Union, which provides them with additional mechanisms of collective protection and access to European platforms for the coordination of information security (Shkuropadska et al., 2024)

Poland's position in the area of societal resilience remained unchanged (0), while the other Visegrad Group countries demonstrated regression. In terms of legal and institutional resilience, Poland (+0.6) and the Czech Republic (+0.4) showed progress, whereas Slovakia (–0.3) and Hungary (−1.1) experienced decline. All countries, except for the Czech Republic (0), recorded regression in the domain of media and digital resilience. The most significant regression was observed in Hungary, where all components declined, indicating a substantial weakening of its ability to counter russian disinformation.

A similar negative trend is evident in belarus, where societal resilience stands at −0.6, legal and institutional resilience at −1.1, and media and digital resilience at −0.2. Overall, russia has transformed belarus into an information-dependent state, where disinformation is used not only as a tool of domestic control but also as an instrument in the broader geopolitical struggle (Polovyi, 2022).

Thus, a comparative analysis of the Disinformation Resilience Index shows that countries of Eastern Europe and the Caucasus, particularly Ukraine, Moldova, Armenia, and Azerbaijan, improved their positions between 2021 and 2024, while the Visegrad Group countries present mixed results, and Hungary and belarus revealed a significant weakening across all resilience components.

Conclusions

Ukraine's information resilience constitutes a crucial element of national security and the state's capacity to counter hybrid threats. An analysis of the main directions of russia's information warfare has revealed that russia employs a multidimensional approach, encompassing propaganda, the undermining of national unity, cybercrime, information-psychological operations, and large-scale international disinformation campaigns aimed at discrediting Ukraine and reducing international support.

Research based on the Disinformation Resilience Index demonstrates that Ukraine has significantly enhanced its level of information resilience across all dimensions. The full-scale russian invasion in 2022 appears to have been a decisive factor prompting Ukraine to intensify its efforts in countering disinformation threats. At the same time, a comparative perspective with other Central and Eastern European countries highlights the uniqueness of Ukraine's experience and underlines the necessity of continually improving mechanisms that ensure societal resilience, legal and institutional resilience, and media and digital resilience, thereby confirming the article's proposed hypothesis.

It is worth noting that one of the key factors determining the scope and effectiveness of russian disinformation activities is the geographical proximity and historical ties of states with russia. Countries that directly border russia or have long been subject to its political, economic, or cultural influence tend to be more vulnerable to information manipulation. In such contexts, disinformation functions not only as a tool for shaping public opinion but also as a mechanism for fostering political dependence, undermining sovereignty, and obstructing democratic transformations.

A promising area for further research lies in the assessment of international cooperation instruments that can enhance information resilience and reduce the vulnerability of democratic institutions to external influence.

REFERENCE / СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Association for International Affairs. (2024, December). *Disinformation Resilience Index 2024*. https://www.amo.cz/wp-content/uploads/2024/12/DRI_2024_edition.pdf	
Bilynska, M. M., & Korolchuk, O. L. (2018). National resilience (stress resistance). Public administration. NAPA.	Білинська, М. М., & Корольчук, О. Л. (2018). Національна резильєнтність (стресостійкість). Публічне управління. НАДУ.
Brailian, Y. (2023, October 13). Armenia Might Become the Next Ukraine: *How russian propaganda reacts to Nagorno-Karabakh issue*. Detector Media. https://en.detector.media/post/armenia-might-become-the-next-ukraine-how-russian-propaganda-reacts-to-nagorno-karabakh-issue?	
Bronstein, Je. (2019). Reframing integration: Information marginalization and information resistance among migrant workers. *Journal of Documentation, 76*(1), 27–48. https://doi.org/10.1108/JD-06-2019-0108	
Center for countering disinformation. (n. d.). *How russia is undermining Ukraine from within*. https://cpd.gov.ua/main/yak-rosiya-pidryvaye-ukrayinu-zseredyny/	Центр протидії дезінформації. (б. д.). *Як росія підриває Україну зсередини*. https://cpd.gov.ua/main/yak-rosiya-pidryvaye-ukrayinu-zseredyny/
Derkachenko, Ya. (2016). Informative and psychological operations as a modern instrument of geopolitics. *Global Organization of Allied Leadership*. https://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/	Деркаченко, Я. (2016). Інформаційно-психологічні операції як сучасний інструмент геополітики. *Глобальна організація союзницького лідерства*. https://goal-int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/
Dragomir, M., Rúas-Araújo, J. & Horowitz, M. (2024). Beyond online disinformation: assessing national information resilience in four European countries. *Humanit Soc Sci Commun* (11), 101. https://doi.org/10.1057/s41599-024-02605-5	

Gladysh, M., Pakhomenko, S., & Kuchyk, O. (2023). The information resilience of Ukraine and the EU in terms of russian aggression. *Language Culture Politics*, (1), 227–245. https://doi.org/10.54515/lcp.2023.1.227-245

Gnatiuk, S., Bakalynsky, A., Myalkovsky, D., & Pakholchenko, D. (2022). Resilience and constantly of information infrastructure functioning within the national resilience system. *Political Science and Security Studies Journal, 3*(1), 26–31. https://doi.org/10.5281/zenodo.6385602

Horbulin, V. P. (2009). *Information operations and the security of society: Threats, counteraction, modeling*. Kyiv: Intertekhnolohiia.	Горбулін, В. П. (2009*). Інформаційні операції та безпека суспільства: загрози, протидія, моделювання*. Київ. Інтертехнологія, 164 с.

Kennedy, J., & Dunbar, W. (2025, July). *Countering russian influence: Support for Armenia, Georgia, and Moldova in the "Waiting Room of the West"*. RAND. https://www.rand.org/pubs/commentary/2025/07/countering-russian-influence-support-for-armenia-georgia.html

Koval, Z. (2019). Approaches to defining the criteria for assessing Ukraine's information and psychological resilience. *Actual Problems of Public Administration, 1*(77), 49–53.	Коваль, З. (2019). Підходи до визначення критеріїв оцінки інформаційно-психологічної стійкості України. *Актуальні проблеми державного управління, 1*(77), 49–53.
Kyrychenko, Yu., Sergiienko, T., & Slastin, V. (2025). Information Wars as a Tool of Hybrid Aggression: The Ukrainian Experience. *Visnyk NTUU "KPI". Politology. Sociology. Law, 1*(65), 89–95. https://doi.org/10.20535/2308-5053.2025.1(65).332563	Кириченко, Ю., Сергієнко, Т., & Сластін, В. (2025). Інформаційні війни як інструмент гібридної агресії: український досвід. *Вісник НТУУ "КПІ". Політологія. Соціологія. Право, 1*(65), 89–95. https://doi.org/10.20535/2308-5053.2025.1(65).332563

Lloyd, A. (2015). Stranger in a strange land; enabling information resilience in resettlement landscapes. *Journal of Documentation, 71*(5), 10291042. https://doi.org/10.1108/JD-04-2014-0065

Nicol, E., Willson, R., Ruthven, I., Elsweiler, D., & Buchanan, G. (2022), Information Intermediaries and Information Resilience: Working to Support Marginalised Groups. *Proceedings of the Association for Information Science and Technology*, (59), 469–473. https://doi.org/10.1002/pra2.654

Oleksiyuk, T. (2025). The right to access official information as a resilience-improving tool: Ukrainian lessons during wartime. *Social Sciences & Humanities Open*, (11), 101549. https://doi.org/10.1016/j.ssaho.2025.101549

Polovyi, T. (2022). The influence of russian propaganda on Belarusian society. *Visnyk of the Lviv University. Series Philosophical and Political Studies*, (41), 163–170. https://www.fps-visnyk.lnu.lviv.ua/archive/41_2022/21.pdf	Польовий, Т. (2022). Вплив російської пропаганди на білоруське суспільство. *Вісник Львівського університету. Серія філософсько-політологічні студії,* (41), 163–170. https://www.fps-visnyk.lnu.lviv.ua/archive/ 41_2022/21.pdf

Rantamäki, A., Uusikylä, P., & Jalonen, H. (2024). Information resilience in networks: an analysis of a national security legislation evidence base. *Scandinavian journal of public administration*, *28*(2), 1–20. https://doi.org/10.58235/sjpa.2023.14068

Reanimation package of reforms. (2023, June 6). *Disinformation as a human rights violation in the context of russia's invasion of Ukraine:* A professional report. https://rpr.org.ua/news/dezinformatsiia-iak-porushennia-prav-liudyny-v-konteksti-rosiyskoho-vtorhnennia-v-ukrainu-fakhovyy-zvit/	Реанімаційний пакет реформ. (2023, 6 червня). *Дезінформація як порушення прав людини в контексті російського вторгнення в Україну*: фаховий звіт. https://rpr.org.ua/news/dezinformatsiia-iak-porushennia-prav-liudyny-v-konteksti-rosiyskoho-vtorhnennia-v-ukrainu-fakhovyy-zvit/

Sadiq, Shazia, Aryani, Amir, Demartini, Gianluca. et al. (2022). Information Resilience: the nexus of responsible and agile approaches to information use. The *VLDB Journal*, (31), 1059–1084. https://doi.org/10.1007/s00778-021-00720-2

Shkuropadska, D., Tokar, V., Purdenko, O., Lotariev, A., & Savchuk, K. (2024). Digital Resilience of the Bucharest Nine and Ukraine. *International Journal of Economics and Financial Issues*, *15*(1), 24–31. https://doi.org/10.32479/ijefi.17233

Sikharulidze, V. (2025, March 13). Russian influence operations in Georgia: a threat to democracy and regional stability. *Foreign policy research institute*. https://www.fpri.org/article/2025/03/russian-influence-operations-in-georgia-a-threat-to-democracy-and-regional-stability/

Staender, A., Humprecht, E. (2022) Content analysis in the research field of disinformation. In: Oehmer-Pedrazzi F, Kessler SH, Humprecht E, et al., (eds). *Standardisierte Inhaltsanalyse in der Kommunikationswissenschaft–Standardized Content Analysis in Communication Research*. Springer VS, Wiesbaden, pp. 339–348.

Ukrainian Radio. (2024, July 13). Russian propaganda has largely moved online – Tsybulska. *Radio Kultura.* https://ukr.radio/news.html?newsID=104812

Українське радіо. (2024, 13 липня). Російська пропаганда перемістилася переважно в онлайн – Цибульська. *Радіо Культура*. https://ukr.radio/news.html?newsID=104812

University of Oxford. (2024, April 10). *World-first "Cybercrime Index" ranks countries by cybercrime threat level.* https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level

Uusikylä, P., Jalonen, H., Kallunki, V., Keinänen, A., & Sommarberg, S. (2024). Introduction to Information Resilience in the Context of National Preparedness. In: Uusikylä, P., Jalonen, H., Jokipii, A. (eds). *Information Resilience and Comprehensive Security. Information Technology and Global Governance. Palgrave Macmillan, Cham*. https://doi.org/10.1007/978-3-031-66196-9_1

Conflict of interest. The authors certify that don't they have no financial or non-financial interest in the subject matter or materials discussed in this manuscript; the authors have no association with state bodies, any organizations or commercial entities having a financial interest in or financial conflict with the subject matter or research presented in the manuscript. Given that one of the authors is affiliated with the institution that publishes this journal, which may cause potential conflict or suspicion of bias and therefore the final decision to publish this article (including the reviewers and editors) is made by the members of the Editorial Board who are not he employees of this institution.

The authors received no direct funding for this research.

Shkuropadska, D., & Lebedeva, L. (2025). Information resilience of Ukraine: 2021–2024. *Scientia fructuosa, 6*(164), 38–51 http://doi.org/10.31617/1.2025(164)03

Received by the editorial office 28.08.2025.
Accepted for printing 02.10.2025.
Published online 16.12.2025.