



Countering Disinformation in the Hybrid Information Environment: A Cross-Sectoral Analysis of Public Policy, Education, and Media Strategies

Bozhena Ivanytska*

Department of Journalism and Mass Communication, Lviv Polytechnic National University,
Lviv, Ukraine
<https://orcid.org/0000-0002-9500-3823>

Taras Kobets

Department of Political Science, Faculty of History, Politology and International Relations,
Vasyl Stefanyk Carpathian National University, Ivano-Frankivsk, Ukraine
<https://orcid.org/0009-0001-2179-321X>

Viktor Savchenko

Department of Spacial Operations Forces, Command and Staff Institute of Troops (Force)
Employment, National Defence University of Ukraine, Kyiv, Ukraine
<https://orcid.org/0009-0008-7492-7438>

Volodymyr Pugachov

Food Department, National Scientific Centre "Institute of Agrarian Economics", Kyiv, Ukraine
<https://orcid.org/0000-0002-5456-5862>

Oleksandr Kursyk

Department of National Security and Political Science, Institute of International Relations and
National Security, National University of Ostroh Academy, Ostroh, Ukraine
<https://orcid.org/0009-0008-6806-4074>

*Corresponding author: bivanytska@gmail.com

Abstract

Background: In the context of contemporary hybrid warfare, disinformation poses a significant threat to national security, civic cohesion, and democratic stability. The widespread use of social media, artificial intelligence, and visual content has amplified its influence on public opinion. **Objective.** This study aims to evaluate the effectiveness of current strategies for countering disinformation within the public policy, education, and media sectors.

Methods. The research is grounded in a content and quantitative analysis of 16 peer-reviewed scientific sources, selected from the international databases *Scopus* and *Springer* using relevant keywords.

Results. The analysis reveals that the education sector demonstrates the most dynamic progress, particularly through the promotion of digital literacy and integration of critical thinking into curricula. Public policy has achieved consistent improvements due to national cybersecurity initiatives. In contrast, the media sector remains less responsive, highlighting the need to support independent fact-checking and strengthen media infrastructures.

Conclusions. The findings support the development of an aggregated model to assess the impact of various strategies on societal information resilience.

Unique Contribution: The study's practical value lies in its potential application for shaping public policy, designing educational frameworks, and creating digital tools to detect and mitigate disinformation. The novelty of this research lies in its integrated cross-sectoral perspective, which combines public policy, education, and media approaches within a unified analytical model of information resilience. This enhances the applicability of the findings for both scholars and practitioners seeking to develop sustainable strategies against hybrid information threats.

Key Recommendation: To build comprehensive societal information resilience against disinformation, we strongly recommend a cross-sectoral strategy prioritizing investment in three key areas: (1) enhancing digital literacy and integrating critical thinking into educational curricula; (2) sustaining national cybersecurity initiatives within public policy frameworks; and (3) strategically supporting independent fact-checking networks to strengthen the responsiveness and infrastructure of the media sector.

Keywords: disinformation; information security; information hygiene; digital literacy; hybrid warfare; media literacy; fact-checking; digital education.

Introduction

Information has proven to be one of the most important strategic assets in the digital age, and its strategic manipulation has become an extremely potent instrument in hybrid wars. The pace and the scale of disinformation have been enhanced by social media platforms, instant messengers, and algorithm-based news feeds, influencing people's opinions, destabilising democratic institutions, and impeding civic trust (Ng et al., 2024). As many studies affirm, the speed at which fake news and deepfakes are disseminated can lead to long-term changes in collective behaviour and erode societal resilience (Fujs et al., 2025; Gray & Furnell, 2024). The prevalence of artificial intelligence in content creation only increases the threats because it facilitates an automated disinformation campaign that targets emotional vulnerabilities.

These challenges have been intense in Ukraine, which has operated under active military aggression and information and psychological operations simultaneously, in hybrid warfare. The disinformation is intentionally utilised to undermine the population, create a lack of trust or distrust towards state institutions, and divide civil solidarity. In Ukrainian reality, the issue of hybrid warfare is not only a geopolitical conflict but also an information-based one, where the fight over the population's perception is as important as the fight on the ground (Tolmach et al., 2024). An example is the coordinated activity in social networks and Telegram channels from 2022 to 2023,

when conspiracy theories, fake expertise, and panic-inducing messages spread. This is demonstrated in these scenarios, where disinformation proves to be an instrument of strategic influence, with direct consequences for national security.

Simultaneously, the scientific community worldwide is adopting a holistic and cross-sectoral approach to these issues, integrating education, public policy, and media action (Rod et al., 2025; Katsarakis et al., 2024). Nonetheless, even in light of the dramatic progress, there is no unified research that compares the effectiveness of these strategies across various sectors of society. Specifically, the long-term outcomes of educational programs aimed at wartime resilience to disinformation are not well understood.

Hence, this paper aims to investigate the effectiveness of current measures aimed at combating disinformation in the areas of public policy, education, and the media, and to review how these measures will be implemented from 2021 to 2025. The aims are to determine the primary spheres of influence of disinformation and to organise the indicators of the counter-strategy operation to make recommendations about improving the information hygiene of the population.

This research aims to assess the effectiveness of strategies in countering disinformation across three domain areas: public policy, education, and media. To accomplish this, the hypotheses that guide the research are as follows:

- Public policy - national regulatory and information security policies should show a consistent yet average performance, as the institutions adjust gradually to hybrid information threats.
- Education, Formal and informal digital literacy programs are theorised to have the most dynamically developing growth in efficacy, as they directly impact the process of the development of critical thinking and information hygiene.
- Media fact-checking and journalism are likely to experience slower improvement because of the limited resources and the fast development of disinformation technologies.

These hypotheses present a guideline for connecting the aims of the study to quantifiable signs of change over the period of 2021-2025. The analysis will also seek to compare the relative performance of the three sectors as well as to determine the cross-sectoral synergies that can enhance societal resilience to manipulation.

Literature Review

Within the framework of research on information security and hygiene in the context of hybrid warfare, the relevance of the topic is confirmed by the growing number of scientific works devoted to issues of disinformation, digital literacy, and state information policy. Many researchers focus on the changing information environment caused by the influence of social networks, artificial intelligence, and algorithmic personalisation of content (Bansal et al., 2025; Ng et al., 2024). These studies underscore the importance of critical thinking and the need for innovative approaches to digital education. Significant contributions to understanding the mechanisms of disinformation dissemination have been made by studies focusing on digital channels of influence, in particular, the use of bots, fake accounts, and deepfake technologies (Menichetti & Ranieri, 2024; Gray & Furnell, 2024; Fujs et al., 2025). They demonstrate that young people and active users of digital

space are most vulnerable to such influences. The studies also provide examples of information attacks that actively exploit the emotional and cognitive weaknesses of the audience.

Among systemic studies, those that consider disinformation as a multifaceted phenomenon requiring a cross-sectoral response stand out: through education policy, government regulation, and the development of ethical journalism (Tolmach et al., 2024). The works of these authors demonstrate the advantages of combining formal education and informal community initiatives to build information resilience. Also important are works that form the conceptual basis for digital inclusion, particularly concerning involving vulnerable groups in the process of information hygiene (Katsarakis et al., 2024; Gray & Furnell, 2024). These studies support the thesis of social justice as a component of information security. At the same time, authors such as Gupta and Furnell (2022) draw attention to the potential of social robots and interactive platforms in educational campaigns.

Several publications emphasise the engineering and technical aspects of digital security, including information flow management models that can be applied in educational settings (Oliynyk et al., 2021). This enables the integration of humanitarian and technological approaches in the study of information hygiene. Thus, the scientific discourse demonstrates a growing interest in the problem of disinformation, as well as the expansion of methodological research tools. There is a consensus on the need to combine technical, pedagogical, and social strategies in countering information threats (Tin et al., 2023). This opens up prospects for further interdisciplinary research aimed at developing an integrated model of information hygiene in the context of hybrid threats.

Interdisciplinary approaches to digital education deserve special attention in the analysis of publications, where innovative teaching methods that can be integrated into information hygiene are considered. Ead and Abbassy (2022) cite the example of the potential of gamification in digital skill formation. Jauernig (2023) proposes a philosophical and cognitive approach to analysing artificial intelligence, which would provide a more appropriate understanding of the mechanisms of narrative manipulation in the digital space. There have also been significant contributions in the area of the human factor in technological environments. In addition, Gupta and Furnell (2022) analyse the role of social robots in communication and learning, opening up prospects for the implementation of autonomous systems in the fight against fake news. The works of Tin et al. (2023), although focused on medicine, demonstrate the application of analytical and deep neural network models that can be adapted to detect disinformation.

However, despite the diversity and multifaceted nature of contemporary research, there remain problems that need to be addressed. First, there is no unified model for assessing the effectiveness of information hygiene in real digital environments. Second, the mechanisms by which disinformation influences emotional regulation and collective behaviour in crises have not been sufficiently studied.

Research Methods

The study uses content and quantitative analysis of 16 scientific and analytical publications for 2021–2025, selected from the international scientific databases Scopus and Springer using the

keywords: disinformation strategies, media literacy, state policy, information resilience, fact-checking, and education. The author analysed the following indicators by comparing them: the existence of targeted state or educational programs, audience coverage, the level of involvement of public, educational, and media institutions, the sustainability of the results achieved, and their dynamics. The materials were systematised in a table with a 5-point scale to visualise changes in effectiveness over the years, which made it possible to build an aggregate model of information resilience development in three key sectors: public policy, education, and media. Additionally, elements of comparative analysis of digital channels for the dissemination of disinformation, based on the typology of platforms, audiences, and instruments of influence, were used to form general conclusions.

Results

In the context of hybrid warfare, which combines military, political, economic, and informational-psychological means of influence, the concept of information security is critical to preserving national sovereignty, social stability, and democratic institutions. Information security encompasses the protection of critical information infrastructure, data, communication channels, and the information awareness of citizens from external and internal influences aimed at destabilisation (Bansal et al., 2025). According to an international report by Check Point Research (2024), the average level of cyberattacks worldwide increased by 38% compared to the previous year. Ukraine ranked among the top countries in terms of the number of recorded attacks on government institutions and media resources. The main vectors of attacks were phishing, infection through botnets, DDoS attacks, and cyber extortion. About 70% of attacks were accompanied by disinformation campaigns, indicating a high level of synchronisation of technical and psychological influence on the population. In turn, information hygiene is a system of behavioural norms, knowledge, and skills that enable users of the information space to recognise fakes, manipulation, cognitive attacks, and maintain critical thinking in conditions of information noise and disinformation. It is a component of digital culture and an integral element of civic education in the digital age (Katsarakis et al., 2024; Gray & Furnell, 2024).

In the context of hybrid aggression against Ukraine, disinformation campaigns are often aimed not only at undermining trust in state institutions but also at creating panic among the population and stimulating divisions in society, which is particularly dangerous in times of war. Therefore, strengthening information hygiene and ensuring sustainable information security is not only a matter of cybersecurity, but also of national security as a whole.

The modern digital environment has significantly changed the mechanisms for spreading disinformation. Whereas traditional media used to be the primary channels of influence, social networks, messengers, video hosting services, and even artificial intelligence tools have now become the top priorities. Particularly dangerous is the ability of the latest technologies to create deepfake content, automatically generate disinformation messages, shape emotional narratives, and manipulate users' digital behaviour (Table 1).

Table 1. Main digital channels and techniques for spreading disinformation

Channel or platform	Tools for spreading disinformation	Main audience	Examples of influence
Social media (Facebook, X, Instagram, TikTok)	Bots, fake accounts, algorithmic polarization	Young people, active users	Spreading fake news and emotional videos
Messengers (Telegram, WhatsApp, Viber)	Anonymous channels, mass mailings, pseudo-patriotic slogans	All age groups	Conspiracy theories, fake appeals
YouTube, video hosting sites	Manipulative video content, pseudoscientific lectures	Students, middle class	Video with distorted facts
AI platforms (ChatGPT, image generators)	Generation of fake news, deepfake videos, substitution of quotes	Journalists, educators, young people	Fictitious quotes, impersonation of personalities
Anonymous forums and websites	Conspiracy theories, incitement to hatred, pseudo-expertise	Radicalized groups	Coordination of information attacks
Online gaming platforms (chat services, streaming)	Influence through gaming narratives, “jokes” with fake content	Teenagers	Viral memes with misinformation

Source: created by the author based on (Fujs et al., 2025; Ng et al., 2024; Katsarakis et al., 2024)

As can be seen from the table, disinformation adapts to each channel, changing its forms and emphasis according to the target audience. The greatest threat comes from tools that combine personalised content selection with visual or emotional manipulation. In particular, algorithmic polarisation on social media contributes to the creation of information bubbles that reinforce users' biases and suppress critical thinking. Thus, in order to develop effective strategies to counter disinformation, it is necessary to consider not only the sources but also the means of dissemination, their adaptability to the digital environment, and the psychological vulnerability of specific population groups.

In response to the new challenges of hybrid warfare, many countries have introduced multi-channel strategies to counter disinformation. Key areas include strengthening the regulatory framework, implementing educational initiatives to foster critical thinking, and introducing independent media monitoring and digital hygiene. The success of these strategies varies depending on the level of inter-institutional cooperation, civil society engagement, and political support (Katsarakis et al., 2024).

To assess the effectiveness of disinformation counterstrategies, the authors conducted a content and quantitative analysis of 16 scientific and analytical publications for 2021–2025 from the international databases Scopus and Springer. The sample was selected based on the keywords: disinformation strategies, media literacy, state policy, information resilience, fact-checking, and education.

Each source was analyzed taking into account the following indicators:

- existence of targeted programs or policies;
- audience coverage;
- level of involvement of civil society/educational/media organizations;
- effects recorded in reports or impact assessments;
- sustainability of results over time.

The analysis identified three key sectors for the implementation of anti-disinformation strategies:

- public policy (regulation, security strategies, national programs);
- education (formal and informal, digital literacy, critical thinking);
- media (fact-checking, journalistic standards, awareness campaigns).

The data was compiled into a table based on a conditional efficiency rating on a 5-point scale. The rating was to be conducted based on predefined criteria to ensure the transparency and reproducibility of the 5-point conditional efficiency rating. One signified little or no systemic action in place; two signified partial or pilot initiatives with little impact; three signified moderate institutionalisation with measuring yet unsteady effects; four was used when policies or programs proved to be consistent in implementation and long-term consequences; and the fifth was comprehensive, multi-actor initiatives with established long-term effects. Both reviewers independently coded each publication, and although no disagreements were reported, they were discussed to reach a consensus, thereby improving the evaluation process by making it less subjective and more reliable. Ratings were assigned by comparing the substantive characteristics of each sector for each year, with a focus on the dynamics of improvement/stagnation. This approach allowed us to build an aggregate model for further visualisation of trends. Before proceeding with the analysis, the authors present a conditional summary table (see Table 2).

Table 2. Level of effectiveness of counter-disinformation strategies (2021–2025)

Area of application	2021	2022	2023	2024	2025	Growth in 2021–2025
State policy	2.5	3.2	3.7	4.1	4.4	+1.9

Education (formal/informal)	1.8	2.4	3.1	3.8	4.2	+2.4
Media and fact-checking	2.9	3.3	3.6	4.0	4.3	+1.4

Source: created by the author based on (Bansal et al., 2025; Fujs et al., 2025; Katsarakes et al., 2024)

As shown in Table 2, all three sectors exhibit positive dynamics in implementing strategies to counter disinformation. The most significant increase is observed in the education sector (+2.4), which indicates the effectiveness of measures to introduce digital literacy and critical thinking into school curricula. Public policy has also made significant progress (+1.9), which is attributed to the implementation of national cybersecurity strategies and strengthened regulatory oversight of the information space. Despite high starting points, the media sector shows the smallest increase (+1.4 %), which may be related to limited resources for independent fact-checking initiatives and challenges in combating viral misinformation (Ng et al., 2024). Figure 1 shows a comparative analysis of the effectiveness of disinformation countermeasures over a five-year period in three key sectors.

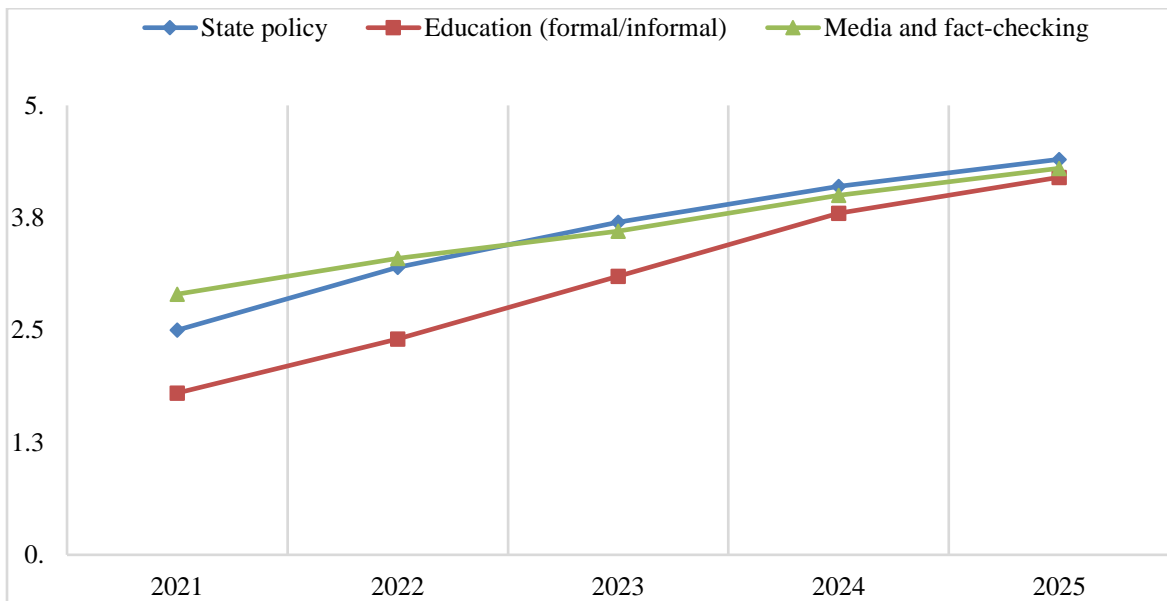


Figure 1. Dynamics of the effectiveness of counter-disinformation strategies in public policy, education, and media (2021–2025)

Source: created by the author based on (Bansal et al., 2025; Fujs et al., 2025; Katsarakes et al., 2024)

The figure shows the dynamics of the effectiveness of counter-disinformation strategies in three main sectors: public policy, education (formal and informal), and media with fact-checking. All three areas show an increase in effectiveness between 2021 and 2025, but with varying intensity and starting points. Public policy started with a score of 2.5 in 2021. The largest increase occurred in 2022 (+0.7), indicating the intensification of regulatory initiatives against the backdrop of the

relevance of information security in the context of the war. The following years show steady but moderate growth, and by 2025, this area reaches 4.4 points. This indicates consistent institutional work and policy adaptation to digital challenges. Education had the lowest initial level – 1.8 points in 2021 – due to the weak integration of information hygiene topics into school curricula. However, this area shows the most dynamic growth. The increase over five years is +2.4 points, with the most noticeable jump occurring in 2023–2024, when education picked up momentum from the digital transformation and mass media literacy courses. Media and fact-checking started from the highest point – 2.9 points in 2021. During the period under review, this sector grew to 4.3 points in 2025, but the increase was the smallest (+1.4 points). Despite the well-developed infrastructure of independent initiatives, growth rates are slow, which is likely due to limited access to funding, a shortage of personnel, and the rapid adaptation of disinformation technologies. Overall, the data indicate positive dynamics in all sectors, with education emerging as a key vector for the future strengthening of the population's information resilience.

To determine the scale of cyberattacks in the context of the information war against Ukraine, the authors conducted content monitoring of incidents recorded in open information sources. Data were collected monthly from 2021 to 2024 and aggregated by type of attack. This approach enables us to develop a dynamic model of conditional changes in the intensity of attacks and types of threats. Table 3 presents statistics on the main types of cyberattacks against Ukrainian organizations over time.

Table 3. Number of recorded cyberattacks on Ukrainian targets by type (2021–2024)

Year	DDoS attacks	Phishing	Viral infection (RAT, botnets)	Account hacking	Information attacks (defacement, fake news)	Total
2021	43	61	28	17	35	184
2022	97	132	81	54	120	484
2023	122	119	101	78	144	564
2024	109	98	84	65	138	494

Source: created by the author based on (State Service of Special Communications and Information Protection of Ukraine, 2022–2024; 2021–2024; Security Service of Ukraine, 2023; Cyberpolice of Ukraine, 2022–2024; InformNapalm, 2022–2023; European Union Agency for Cybersecurity, 2023)

To conduct an empirical analysis of the dynamics of cyberattacks, the authors conducted their own content analysis covering the period from 2021 to 2024. The source base consisted of monthly reports and official statements from Ukrainian cybersecurity agencies, particularly the State Service of Special Communications and Information Protection of Ukraine (SSCIPU, 2022–2024), as well as press releases by the Security Service of Ukraine (SBU) on hacking incidents (2023).

The official sources were supplemented by open monitoring resources, in particular the InformNapalm analytical platform (InformNapalm, 2022–2023). All recorded incidents are classified according to the OWASP recommendations and the ENISA threat classification (European Union Agency for Cybersecurity, 2023). The records were kept taking into account the type of attack, the target, and the presence of signs of an information and psychological component (e.g., accompanying fake narratives).

Figure 2 shows the annual number of cyberattacks recorded in Ukraine by five main types: DDoS attacks, phishing, virus infection (RAT, botnets), account hacking, and information attacks (defacement, fakes).

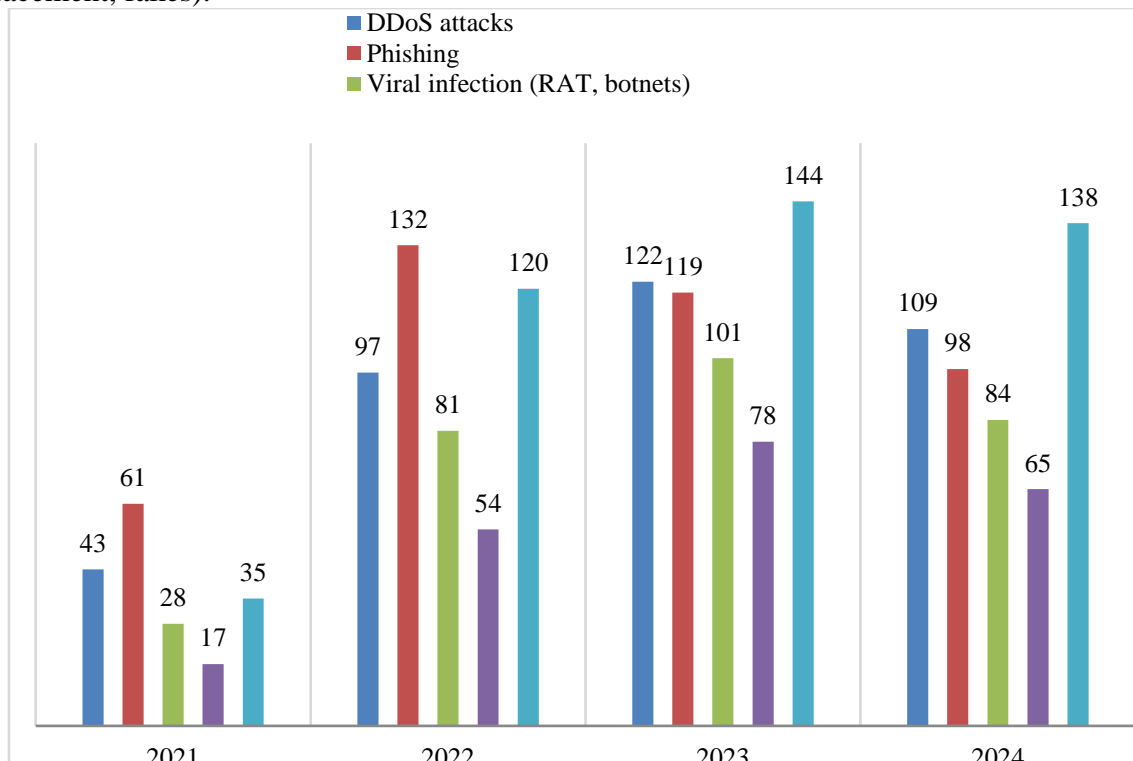


Figure 2. Dynamics of cyber attacks in Ukraine by type (2021–2024)

Source: created by the author based on (State Service of Special Communications and Information Protection of Ukraine, 2022–2024; 2021–2024; Security Service of Ukraine, 2023; InformNapalm, 2022–2023; European Union Agency for Cybersecurity, 2023)

Figure 2 illustrates the dynamics of cyberattacks in Ukraine for the period 2021–2024, categorised into five primary types: DDoS attacks, phishing, virus infections (RAT, botnets), account hacking, and information attacks (defacement, fake content). The most notable increase was recorded in the category of information attacks, from 35 cases in 2021 to 144 in 2023 and 138 in 2024, indicating an increase in both information and psychological pressure. DDoS attacks increased almost threefold, from 43 to 122 in 2023, followed by a slight decline. A similar trend is observed in the categories of phishing and account hacking, where a decline is recorded after the peak figures of 2022–2023. Virus attacks remain the least dynamic, but even here, there is a noticeable steady

increase every year. Overall, the data confirm that cyber aggression peaked in 2022–2023, with 2024 showing only partial stabilisation at a high level, requiring robust response mechanisms.

To ensure a comprehensive analysis of state policy in countering disinformation within the context of hybrid warfare, it is advisable to consider the regulatory framework in three key areas: education, technology, and media. The relevant documents define the principles, objectives, and instruments of state policy in the information and digital environment. Table 4 systematises the most important regulatory acts that provide the legal basis for the formation of information hygiene, digital literacy and resilience to disinformation among the population (see Table 4).

Table 4. Regulatory framework for countering disinformation in the educational, technological, and media contexts

Field	Document title	Content and meaning
Education	Concept for the development of digital competencies among the population of Ukraine (2021)	Defines digital literacy as a national priority, providing for the development of critical thinking skills, media literacy, and information hygiene.
Education	Law of Ukraine “On Education” (2017)	It reinforces a competency-based approach, where information and digital competencies are identified as key to personal and professional development.
Education	On approval of the Concept for the development of civic education (2018)	Supports media education as part of shaping responsible citizens who can stand up to manipulation and fake news.
Technologies	Law of Ukraine “On the Basic Principles of Ensuring Cyber Security of Ukraine” (2017)	Defines the structure of the cybersecurity system, the role of state bodies, and principles for responding to cyber threats, including disinformation as a hybrid threat.
Technologies	National Cybersecurity Strategy of Ukraine (2021)	Formulates national approaches to ensuring information security, including in digital education, data management, and infrastructure.
Media	Ukraine's Information Security Strategy (2021)	Focused on countering disinformation and creating an enabling environment for independent journalism, fact-checking, and awareness campaigns.

Media/EU	EU Code of Practice on Disinformation (2022)	A European ethical standard for online platforms that provides mechanisms for detecting fake news, transparency of algorithms, and cooperation with verified media outlets.
Media / Council of Europe	Recommendation CM/Rec (2018) 1 of the Committee of Ministers to member States	Council of Europe recommendations on protecting democracy from disinformation while safeguarding freedom of expression and promoting ethical journalism.

Source: created by the author based on (Verkhovna Rada of Ukraine, 2017; Cabinet of Ministers of Ukraine, 2021; President of Ukraine, 2021a; President of Ukraine, 2021b; European Commission, 2022; Council of Europe, 2018)

An analysis of the regulatory framework reveals that Ukraine has developed a multi-level strategy for addressing information threats. In the field of education, the focus is on developing digital skills; in the technology sector, on developing a national cyber defence system; and in the media sector, on supporting independent journalism and combating fake news. At the same time, it remains crucial to adopt a cross-sectoral approach and foster cooperation among education, media, and security structures to counter disinformation effectively in the context of hybrid warfare.

In the context of hybrid warfare and the increased presence of disinformation in the digital space, developing information hygiene skills among citizens is becoming a national priority. Information hygiene involves the ability to evaluate information messages critically, recognise manipulation, verify sources, and understand the risks of the digital environment. This is particularly relevant in a context where information attacks are directed not only at individuals but also at the collective consciousness, in particular through social networks, messengers, and automated content distribution algorithms (Tolmach et al., 2024; Katsarakas et al., 2024). In view of this, it is advisable to identify key areas in which information hygiene skills should be developed. Table 5 systematises the main components of recommendations that can be implemented at the individual, community, educational and media institution levels.

Table 5. Recommendations for promoting information hygiene among the population

Direction of formation	Specific action/instrument	Level of implementation	Expected effect
Education	Integration of media literacy into school/university curricula	Formal education	Enhancing critical thinking among young people
Community initiatives	Conducting training sessions, webinars, and information campaigns	Local communities	Accessibility of knowledge outside the educational environment
Digital technologies	Development of interactive applications for fake detection	National/local level	Mass coverage via smartphones
Social networks	Creating educational content and collaborations with bloggers	Social media platforms	Dissemination of reliable information
Journalism	Support for independent fact-checking and ethics training in the media	Professional media	Reducing the number of fake news stories in the public sphere

Source: created by the author based on (Gray & Furnell, 2024; Fujs et al., 2025; Tolmach et al., 2024; Katsarakes et al., 2024)

As can be seen from the table, the formation of information hygiene requires a comprehensive approach. It is essential to combine both institutional actions (reform of educational programs and support for the media) and horizontal initiatives at the community level (training, campaigns, and digital tools). Modern media play a significant role, as they can either amplify information noise or, conversely, be a source of verified knowledge. Thus, resilience to disinformation is only possible through systematic, interdisciplinary, and socially supported efforts.

Discussion

The results of this research show that the education sector is the most active in combating disinformation, followed by policy, and, lastly, media campaigns. Such a trend is aligned with the recent studies that note the transformative role of digital literacy and critical thinking in enhancing the resilience of society (2023; Katsarakes et al., 2024). Relative to these studies, our findings

present a cross-sectoral view of education as a long-term resilience force, and the role of public policy as a stabilising framework in regulation and cybersecurity strategies.

Simultaneously, we find different results from the stance of Bansal et al. (2025), who emphasise the leading role of technological and engineering solutions. Although these are significant, our experience indicates that these actions are short-lived unless structural educational and civic programs support them. This supports the theoretical background of resilience concerning the concept of information security being not only a technical problem, but a socio-cultural phenomenon.

The outcomes of the Ukrainian situation should also be viewed in the framework of hybrid warfare where disinformation is used in parallel with cyberattacks and military aggression (Tolmach et al., 2024). The steep increase in information attacks in 2022-2023 (see Figure 2) shows that the manipulation campaigns were aligned with the wider destabilisation campaign. The results underscore the importance of incorporating resilience frameworks into policy and education to mitigate hybrid threats.

In this way, the debate highlights the need for a balanced model that incorporates technological barriers, regulatory initiatives, educational reforms, and media autonomy. The combined strategy means that resilience to disinformation is sustainable, flexible and compatible with democratic principles. The research findings confirm the hypothesis that the most effective way to counter disinformation in hybrid warfare is to develop digital education and information hygiene among the population. This is in line with Katsarakis et al. (2024), who emphasise the key role of critical thinking and digital inclusion as elements of protection against manipulation. According to our assessment, it was the education sector that showed the most significant increase in efficiency during 2021–2025 (+2.4 points). However, other authors emphasise the predominant role of technological cybersecurity and legal mechanisms. For example, Bansal et al. (2025) believe that effective countering of disinformation requires, first and foremost, improving multi-level control of information flows and applying engineering solutions. In contrast, our position is that technological barriers are only a temporary means of deterring threats and do not form a sustainable information culture if they are not supported by education and awareness.

Another group of researchers (Ng et al., 2024) focuses on the risks posed by the algorithmic polyvariation of content on social media. They emphasise the need for platforms and tech giants to intervene in moderation processes. In this context, our findings partially align with their conclusions; however, the authors believe that platform policies will be effective only under conditions of state control and civic pressure, which are fostered through increased information literacy (Gray & Furnell, 2024; Tolmach et al., 2024). The discussion on the involvement of vulnerable groups in digital security is also interesting. Gray and Furnell (2024) and Gupta and Furnell (2022) propose inclusive approaches through educational technologies and social robots. Our results support the idea of multi-actor interaction, involving both the state and communities, as well as media and educational institutions. Contradictions are observed in assessments of the effectiveness of public policy. The authors believe that public policy should be flexible and

transparent, based on the values of openness, which aligns with the model of democratic digital governance.

Thus, the results of the study are consistent with some previous works, but at the same time emphasise the need for a balanced approach that combines technological tools, education, legal regulation, and civic engagement. The main limitations of our study are the conditional nature of the effectiveness assessment scale and our reliance on secondary sources. Further research should aim to empirically test the relationship between citizens' information hygiene levels and their resilience to disinformation attacks in real-life situations. It is also advisable to examine the impact of cultural context on the perception and dissemination of disinformation.

Conclusion

In this work, the approaches to countering the disinformation in three areas, such as public policy, education, and media, were assessed in three periods, 2021-2025. The results showed that, although every aspect showed improvements, educational programs had the most dynamic ones, and it is possible to note that the main emphasis is set on digital literacy and critical thinking to develop resilience in information. The development of public policy experienced steady growth in regulatory policies and cybersecurity, while the media sector experienced slower growth due to resource and structural constraints.

The research would contribute to knowledge through the creation of an interactive, cross-sectoral outlook and a conditional efficiency rating model, allowing for a systematic comparison of anti-disinformation strategies. The method of analysis can contribute to the theoretical debate about the concept of information resilience by correlating technological, educational, and socio-cultural aspects of hybrid warfare.

The practical consequences of the study are to help policy-makers, educationists and media houses draft coordinated measures to enhance the resistance to manipulation in society. The source of future research ought to be gathering of primary empirical evidence (such as surveys and experimental research) in order to establish the long-term outcomes of the information hygiene programmes, as well as to investigate the culture-specific tendencies in the perception of disinformation.

References

- Bansal, S., Nidhya, M. S., Chheda, K., Rastogi, R., Katariya, J. K., & Garg, P. (2025). An efficient strategy for ensuring multi-cloud information security. *International Journal of System Assurance Engineering and Management*. Advance online publication. <https://doi.org/10.1007/s13198-024-02677-1>
- Cabinet of Ministers of Ukraine (2021). On approval of the Concept for the development of digital competences of the population of Ukraine and approval of the action plan for its implementation: Order No. 167-r, March 3, 2021. <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text>

- Council of Europe (2018). Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e13
- Ead, W. M., & Abbassy, M. M. (2022). A general cyber hygiene approach for financial analytical environment. In: S. Derindere Köseoğlu (Ed.), *Financial data analytics*. (pp. 369–384). Springer. https://doi.org/10.1007/978-3-030-83799-0_13
- European Commission (2022). *The 2022 Code of Practice on Disinformation*. <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformationdigital-strategy.ec.europa.eu>
- European Union Agency for Cybersecurity (ENISA) (2023). *Threat Landscape Report 2023*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- Fujs, D., Vrhovec, S., Hovelja, T., & Vavpotič, D. (2025). SmartICST: A smart information and cyber security training approach for older adults. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-025-13564-y>
- Gray, C., & Furnell, S. (2024). Enhancing cyber hygiene and literacy via interactive mini-games. In: A. Moallem (Ed.), *HCI for cybersecurity, privacy and trust*. (Vol. 14728, pp. 43–52). Springer. https://doi.org/10.1007/978-3-031-61379-1_3
- Gupta, S., & Furnell, S. (2022). From cybersecurity hygiene to cyber well-being. In: A. Moallem (Ed.), *HCI for cybersecurity, privacy and trust*. (Vol. 13333, pp. 124–134). Springer. https://doi.org/10.1007/978-3-031-05563-8_9
- InformNapalm (2022–2023). *Documented cyber operations and hybrid warfare cases*. <https://informnapalm.org/en/>
- Katsarakis, A., Morris, T., & Still, J. D. (2024). Hidden in onboarding: Cyber hygiene training and assessment. In: A. Moallem (Ed.), *HCI for cybersecurity, privacy and trust*. (Vol. 14728, pp. 53–63). Springer. https://doi.org/10.1007/978-3-031-61379-1_4
- Ministry of Education and Science of Ukraine (2018). On approval of the Concept for the development of civic education in Ukraine: Order No. 641, May 30, 2018. <https://mon.gov.ua/ua/npa/pro-zatverdzhennya-koncepciyi-rozvitku-gromadyanskoyi-osviti-v-ukrayini>
- Ng, L. H. X., Kloo, I., Clark, S., & Carley, K. M. (2024). An exploratory analysis of COVID bot vs human disinformation dissemination stemming from the Disinformation Dozen on Telegram. *Journal of Computational Social Science*, 7, 695–720. <https://doi.org/10.1007/s42001-024-00253-y>
- Oliylyk, V. B., Samoylenko, O. M., Batsurovska, I. V., & Dotsenko, N. A. (2021). Information-educational environment in the training of electrical engineering bachelors: Multidisciplinary approach. *Information Technologies and Learning Tools*, 83(3), 259–273. <https://doi.org/10.33407/itlt.v83i3.4373>
- President of Ukraine (2021). On the Information Security Strategy of Ukraine: Decree No. 685/2021, December 28, 2021. <https://zakon.rada.gov.ua/laws/show/685/2021#Text>
- Security Service of Ukraine (2023). *Official press releases on cyber threats and information attacks*. <https://ssu.gov.ua/en/news>
- State Service of Special Communications and Information Protection of Ukraine (2022–2024). *Annual cyber threat reports*. <https://cip.gov.ua/en/reports>

- Tin, D., Barten, D. G., Granholm, F., Kovtonyuk, P., Burkle, F. M., & Ciottone, G. R. (2023). Hybrid warfare and counter-terrorism medicine. *European Journal of Trauma and Emergency Surgery*, 49, 589–593. <https://doi.org/10.1007/s00068-023-02230-y>
- Tolmach, M., Trach, Y., Chaikovska, O., Volynets, V., Khrushch, S., & Kotsiubivska, K. (2024). Artificial intelligence in countering disinformation and enemy propaganda in the context of Russia's armed aggression against Ukraine. In: A. K. Nagar, D. S. Jat, D. K. Mishra, & A. Joshi (Eds.), *Intelligent sustainable systems*. (Vol. 828, pp. 145–152). Springer. https://doi.org/10.1007/978-981-99-8111-3_14
- Verkhovna Rada of Ukraine (2017). Law of Ukraine “On Education” No. 2145-VIII, September 5, 2017. <https://zakon.rada.gov.ua/laws/show/2145-19#Text>