REVIEW ARTICLE

ASIAN JOURNAL OF INTERDISCIPLINARY RESEARCH

Asian Research Association

DOI: 10.54392/ajir26115

Disinformation and Cyber Operations in the Russia–Ukraine War: A Systematic Review of Threats, Mechanisms, and Countermeasures in a Globalized Media Ecosystem

Viktor Melnyk [a, *], Lyudmyla Babenko [b], Olena Dzhahunova [c], Larysa Balycheva [d], Oksana Fedotova [e]

[a] Department of Political Science, Faculty of Philosophy, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[b] Department of History of Ukraine, Faculty of History and Geography, Poltava V. G. Korolenko National Pedagogical University, Poltava, Ukraine
[c] Department of History of Ukraine, Faculty of History, Pavlo Tychyna Uman State Pedagogical University, Uman, Ukraine
[d] Department of Ukrainian Studies and Language Training of Foreign Citizens, Faculty of Training of Foreign Citizens, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
[e] Department of Information Activities, Faculty of Philology and Mass Communications, Mariupol State University, Kyiv, Ukraine
* Corresponding author Email: melnyk1996ethnology@gmail.com
DOI: https://doi.org/10.54392/ajir26115
Received: 14-11-2025; Revised: 26-02-2026; Accepted: 11-03-2026; Published: 28-03-2026

Abstract: The study aims to analyze the impact of globalization on Ukraine's information security from a historical perspective and to identify key challenges and directions for strengthening national resilience in the information domain. The study is based on a structured literature search and qualitative content analysis of scientific sources. Content analysis is conducted to examine academic literature on the evolution of Ukraine's information security under globalization.The findings demonstrate that after the collapse of the USSR, Russian media actively shaped Ukrainian audiences through Moscow-centered narratives. Effective countermeasures emerged only in 2014, while the full blocking of Russian information channels after February 24, 2022, became a crucial step in safeguarding national information security. Key challenges identified include cyber threats, information aggression, unequal access to digital resources, regulatory gaps, and the lack of comprehensive international cooperation. Strengthening Ukraine's information security in the era of globalization requires enhanced cyber defense, the development of media literacy, the adoption of advanced protection technologies, and the implementation of regional security initiatives. Active collaboration with international partners and the integration of modern technologies are essential to ensuring a sustainable and secure information environment.

Keywords: Globalization, Digitalization, International Cooperation, Cyber Defence, Risks.

1. Introduction

Digitalization is undoubtedly an important dimension of this phenomenon (Mansoor *et al.,* 2022). This process has fundamentally changed the previously existing ideas about the storage, transfer and use of information, information resources and personal data. Information (primarily in digital form) has become an important strategic resource, and establishing control over it has become an important aspect of ensuring the stability of public life and the sustainable functioning of national security. However, globalization, as a modern trend, has created many opportunities for the development of digital information systems, data exchange, etc. (Caviglione *et al.,* 2022; Hryshchenko *et al.,* 2025; Seremciuk, 2025), but at the same time has actualized new innovative threats, including for developing countries such as Ukraine. Given the rapid spread of globalization processes, Ukraine's information security has become one of the most important elements of national security. This situation is primarily due to several factors. Among them, the rapid evolution of information and communication technologies, the active use of digital space for various political and military manipulations, the spread of disinformation or even propaganda, which have become integral tools of hybrid confrontations of our time, play a key role (Lysenko *et al.,* 2023; Dykha *et al.,* 2024). Ukraine has experienced the destructive impact of globalization through the deformation of the information field, as it was and still is at the epicenter of the digital threat because of Russia's destructive aggression (Bondarenko *et al.,*

2022; Itzhak & Fer, 2023). Despite many studies, certain issues related to the integration of innovative technologies, particularly artificial intelligence systems, into the field of information security remain insufficiently researched (Hasan, 2024; Willett, 2022). Problematic aspects are also linked to the importance of continuing a comparative analysis of the experiences of different states that have been subjected to information aggression (Mansoor *et al.*, 2022; Zecchinon & Standaert, 2024; Zecchinon & Standaert, 2024). Military operations are accompanied not only by material losses but also by unprecedented threats in the field of information security. Therefore, the main research problem is to identify the main challenges of ensuring information security and determine the main effective mechanisms for ensuring an effective information security space. In such circumstances, the analysis of historical background will allow us to characterize the origins and dynamics of modern information threats, including in the Ukrainian context.

Historical retrospective will allow us to trace the processes of formation and development of Ukraine's information infrastructure, to identify the main challenges faced by Ukrainian national security in different periods of its evolution. An important element of this process will be to highlight the impact of globalization on the strengthening (or weakening) of Ukrainian information security, and the consequences that this has led to. First, the study of the integration of the Soviet legacy into Ukraine's information security, the development of information environments since independence and their current state (in times of integration into the global information space) are relevant research issues for understanding the current state and potential of Ukraine's information security. The scientific novelty of the article will lie in the synthesis of individual facts from historical retrospect alongside an analysis of current manifestations of hybrid warfare, which will allow for a general identification of certain lessons from the past and how they determine the effectiveness of Ukraine's information security in modern conditions of globalization. Ultimately, the Ukrainian experience is unique because it has pointed to vivid examples of the synthesis of classic and new information threats. In the context of hybrid warfare, this has turned the study of Ukrainian practice into a relevant case for further research and a notable retrospective on global security.

The purpose of the proposed article is a comprehensive analysis of the impact of globalization processes on Ukraine's information security through the prism of historical retrospective development.

Research Question (RQ): How and through what mechanisms did globalization transform threats to information security in Ukraine in 1991–2025, and what institutional solutions ensured the growth of the resilience of the information environment?

Sub-questions: (1) What phases of threat evolution can be distinguished in 1991–2013; 2014–2021; 2022–2025? (2) What channels and technological mechanisms of influence dominated in different periods? (3) What countermeasures (regulatory, technological, educational, international) proved to be the most effective?

The analytical framework combines the "vulnerability–capability" approach with the notion of a socio-technical ecosystem (state–platforms–society).

The contribution of the article lies in (1) conceptualizing globalization as a multidimensional driver of information risks, (2) periodizing the evolution of threats and Ukraine's responses, (3) synthesizing the literature on Russian information operations, hybrid warfare, and cyber influence into a single explanatory model.

The practical significance of the proposed article lay in the possibilities of using the obtained results for the further development of individual state strategies in the field of information security, and the gradual integration of modern technologies (including AI systems) into the system of protection against information challenges.

The main scientific hypothesis of the study is that strengthening of Ukraine's information environment in times of globalization is likely to be achieved through a combination of historical lessons learned, active cooperation with international communities, and the use of modern technologies to overcome internal and external threats.

2. Literature Review

2.1. Key Threats to the Functioning of Information Systems

The issue of the impact of globalisation on national security is a relevant part of scientific research. Scholars have addressed this topic, drawing attention to various aspects of this process. Brzozowska *et al.* (2022) pointed to

threats to the operation of information systems that come from both hostile state institutions and private companies and individuals acting independently or according to a pre-agreed plan. The possibility of using hacker groups to carry out digital sabotage has become a serious challenge to the international legal order, requiring action on a national and international legal basis (Bidzilya *et al.,* 2023; Juneja *et al.,* 2024). Moreover, researchers reasonably point out that digital threats in times of globalisation will continue to grow rapidly, due to the rapid development of innovative technologies, some of which are used not only to protect information but also to organise attacks (Hub & Příhodová, 2021). Alongside the traditional analysis of scientific literature, a preliminary bibliometric review was conducted using VOSviewer tools (See Figure 1).

In general, modern authors have identified the main economic, political, legal, technological, medical and cultural dimensions of globalization and shown its relevance for the challenges of information security in Ukraine. Based on the analysis of the Scopus database, 7 clusters were obtained that provide information about the main categories of research on globalization processes through the prism of the humanities.

Cluster 1 - economic, environmental, demographic and psychological aspects of globalization and their impact on the development of society and security.

Cluster 2 - historical, political and ideological factors (USSR, wars, diplomacy) that shape modern challenges to information security.

Cluster 3 - international alliances, arms control, democracy and the "cold war" as factors of global security.

Cluster 4 - geopolitics, international law, annexation, sanctions, sovereignty, the Ukrainian question.

Cluster 5 - new technologies: artificial intelligence, computer science, biochemistry as new challenges and resources for information security.

Cluster 6 – global crises (COVID-19 pandemic), healthcare and communications as areas of information risks.

Cluster 7 – culture, heritage, identity as objects of influence of globalization and information attacks.

This made it possible to identify individual clusters regarding current scientific research in the field of information security. For example, the existence of intensive research in the areas of countering cyber threats, information attacks, and detecting disinformation has been established. However, the issues of integration and the specifics of applying artificial intelligence in digital protection systems, as well as a comparison of research on national information security strategies in different countries, are rather poorly represented.

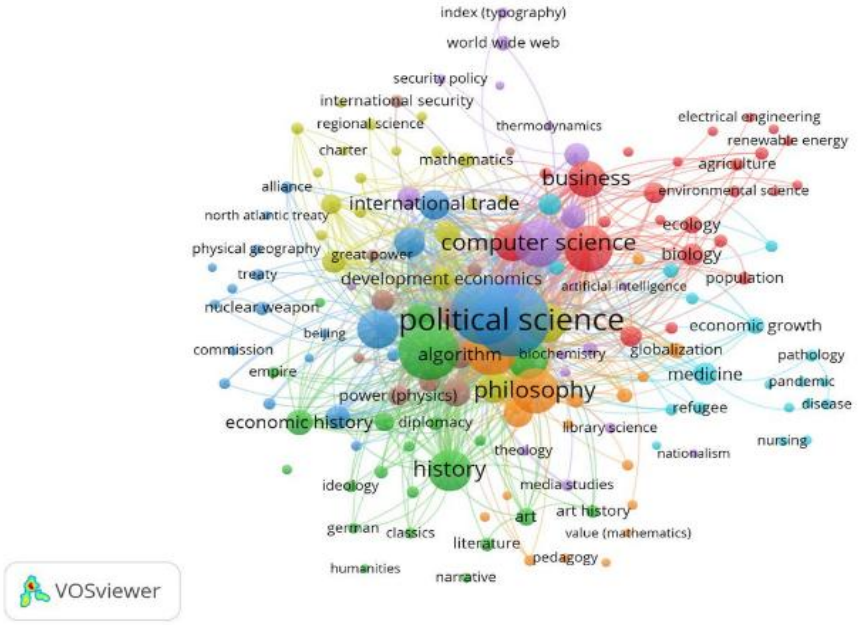

Figure 1. Analysis of scientific literature

Source: Authors' elaboration based on Scopus database export, visualized using VOSviewer

In modern conditions, the economic dimensions of globalization are important. Scientists have determined that transnational corporations and global digital platforms (in particular, Google, Meta, Microsoft, and others) will continue to have a more active influence on the formation of the information space of states, in fact creating parallel instruments for information regulation and control over it (Dubyna et *al.,* 2024; Maliarchuk *et al.,* 2025). The proposed situation has created a double challenge: on the one hand, such private players are well equipped with the infrastructure for the further functioning of information systems, on the other hand, the algorithms and business models they use can contribute to the spread of disinformation and the process of personal data leakage (Borychenko *et al.,* 2024). As a result, researchers have pointed out the importance of creating additional international norms of corporate responsibility in the field of cybersecurity (Seremciuk, 2025; Kaspars, 2022).

At the same time, it is not only about digital threats, but also about the crisis of the overall global security system, as demonstrated by the Russian aggression against Ukraine (Farmkhaus, 2024; Syvak *et al.,* 2023). Russia's military offensive was accompanied by an active propaganda campaign aimed at both Ukraine and democratic countries in general (Rogozińska, 2022). This challenge turned out to be a global one, as it demonstrated the capabilities of military force and accompanying information means of influence in the 21st century. The development of new rules can take a long time, which makes national security systems quite vulnerable to hybrid and post-hybrid attacks. The review of the proposed scientific literature has demonstrated that there is a debate in the professional community about the possibility of further responding to the information security challenge.

2.2. Information Security

Scholars have also developed specific issues in the history and practice of information security protection in Ukraine. Chmyr *et al.* (2023) analysed the development of the post-industrial society through the prism of future security challenges. Their conclusions also include the need to restructure Ukraine's information security as an integral part of Ukraine's national security. Other scholars agree that changes are necessary, at least considering the existing experience of countering Russian aggression (Ślufińska, 2022). However, further ways of such reforms have sparked academic debate. Some researchers emphasise the importance of applying the existing experience of democratic countries.

For example, Izmailov and Yegorova (2023) demonstrated the benefits of using European experience in information security compliance. Such conclusions may be useful in the Ukrainian context, as Ukraine's European integration aspirations will also require appropriate changes (adaptation) of Ukrainian legislation (Izmailov & Yegorova, 2023). The importance of using international experience was demonstrated by researchers who analysed the main aspects of information security in entire regions, including in the context of military confrontation (Marleku & Reka, 2018). At the same time, there are views on the development of information security strategies based exclusively on Ukrainian practices Belkin *et al.* (2022) with a small element of borrowing. This approach is based on the notion that existing practices have proved unprepared to ensure peace in the context of Russian aggression, and therefore the capabilities of other national security systems should be rethought.

Although the practical considerations in this theory are quite clear, advanced national security strategies have not become separate static elements. Governments of other countries are actively using the experience of the Russian-Ukrainian war to adjust existing documents to improve them. Under these circumstances, the arguments of scholars advocating for a synthesis of existing international strategies with Ukrainian experiences Radchenko *et al.* (2023a) appear more promising. This approach would chart a pathway for addressing the negative impacts of globalization on Ukraine's national security. The importance of further development of the national security sphere against the backdrop of the Russian invasion of Ukraine is another important issue that researchers have drawn attention to. Predicting possible ways of developing events, they noted certain aspects of the integration of artificial intelligence technologies into a possible system of countering hybrid challenges and even physical attempts to damage digital information or carry out any other aggressive actions (Andraško *et al.,* 2021; Stewart, 2022). At the same time, the possibilities of countering artificial intelligence itself were also discussed, as its capabilities in criminal hands can also turn into a weapon that can cause significant harm to both individuals and state institutions (Garcia, 2021). The focus on these emerging challenges to national security systems is well-founded, as it highlights the key vectors being explored in expert circles.

The development of civil society institutions has gained additional importance, contributing to the formation of new types of digital culture in society. Researchers have indicated in recent years that aspects such as media literacy, the ability to critically evaluate information and recognize the components of information attacks have significantly reduced the effectiveness of propaganda digital campaigns (Averianova & Voropayeva, 2020; Fyshchuk & Pintsch, 2025). Educational programs on digital literacy and online security have already been developed for Ukrainian realities, which, according to researchers, should be integrated into the broader context of state information policy (Matviienkiv & Vdovychyn, 2024; Vdovichen *et al.,* 2024).

Along with the threat of artificial intelligence, a potential current challenge is the strengthening of global hacker groups that can operate under the cover of government agencies in specific countries. Information about the use of hacker teams by Chinese intelligence agencies to interfere with the functioning of American networks (even the consequences of interference in the US presidential election were discussed) leaked into the information field (Slayton, 2020). Given the activity of Russian hackers, at least such a threat should be expected in the Ukrainian reality (Rohatiuk *et al.,* 2024). Taking this danger into account will require amendments to the legal framework, development of separate mechanisms for responding to and countering such attacks, as even with the likely end of the hot phase of the war, the Kremlin regime's ambitions will continue to pose challenges to Ukraine's national security.

Another important issue is the challenge of regulating artificial intelligence. There is a discussion in the scientific literature about the need to create separate ethical standards that should facilitate the gradual process of integrating AI algorithms into the national security structure (Akimov, 2023; Makovetska *et al.,* 2024). However, imposing excessive restrictions can generally slow down the development of innovative technologies, while the complete absence of regulation will also create certain prerequisites for abuse (Iliev *et al.,* 2020; Nalyvaiko & Lebedieva, 2022). From a research point of view, finding a balance between innovative development and security guarantees has become the basis for the use of innovations.

2.3. Terminological Consistency

To ensure terminological consistency, the following working definitions are used in this study.

Information security is understood as the state of protection of the information space of the state, its institutions and citizens from external and internal threats that may harm national interests, political stability or public trust. In this study, information security covers both the technological and communication dimensions.

Cybersecurity is interpreted as a set of measures and mechanisms to protect digital infrastructure, information systems and networks from unauthorized access, attacks or destruction. Cybersecurity is a component of the broader category of information security, but is not identical to it.

Information warfare means the targeted use of information resources and communication strategies to influence public consciousness, political decisions or the international reputation of the enemy. It can be carried out both in peacetime and in conditions of armed conflict.

Hybrid warfare is considered a complex strategy that combines military, information, economic, cyber and political instruments of influence. In this context, information operations and cyber operations are its constituent elements.

Propaganda is defined as the systematic dissemination of ideas or narratives with the aim of forming a desired perception of events or actors. It can contain both truthful and distorted information.

Disinformation means intentionally created and disseminated false or manipulative information with the aim of misleading the audience.

Misinformation differs from disinformation in that it is disseminated without the intention to mislead, although it can have similar negative consequences.

In the following text, these terms are used consistently in accordance with the above definitions, which allows a clear distinction between the types of threats and the mechanisms for their analysis.

3. Methodology

3.1. Research Design

This study used a structured narrative review (also called a scoping review) as its methodological framework. This design was chosen because the aim of the study was to trace the historical evolution of Ukraine's information security within the context of globalization. This required a systematic coverage of diverse types of sources (empirical studies, policy analysis, content analysis, and technical reports on cybersecurity) over an extended period of time. The structured narrative review ensured breadth of coverage and thematic synthesis.

The review was complemented by an analysis of sociological survey data from the Global Digital Trust Survey 2025 (PwC, 2025) to determine public and institutional perceptions of cybersecurity.

3.2. Materials and Equipment

The study covered the period 1991–2025. This range corresponded to the independence of Ukraine and the trajectory of its information security development in the information space. This range was used in all elements of the study: the formulation of the research question, the parameters of the database search, the inclusion/exclusion criteria and the study selection process.

3.3. Procedures

The search for scientific publications was carried out in the databases Scopus, Web of Science Core Collection and Google Scholar. Scopus was chosen as the main database due to its broad interdisciplinary coverage of peer-reviewed literature in the social sciences, political science, law, and security studies, providing access to influential international publications relevant to the topic. The Web of Science Core collection was included due to its rigorous indexing standards and significant representation of journals at the intersection of international relations, cybersecurity, and political science. Google Scholar was integrated to collect "gray" literature, Ukrainian-language scientific papers, conference proceedings, and analytical reports that are not indexed in Scopus or WoS but are important for adequately representing the national context of the development of information security in Ukraine. The time period of coverage included publications from 1991 to 2025, which corresponds to the period of independence of Ukraine and the evolution of its information security in the context of integration into the global information space. The search involved the use of blocks based on Boolean operators:

Block 1 (Information Security Concept): "information security" OR "cybersecurity" OR "information warfare" OR "information operations" OR "disinformation" OR "propaganda" OR "hybrid warfare".

Block 2 (Geographical focus): "Ukraine" OR "Ukrainian".

Block 3 (Globalization dimension): "globalization" OR "globalization" OR "digitalization" OR "digital platforms" OR "global information space" OR "international cooperation" OR "transnational information".

Full string: (Block 1) AND (Block 2) AND (Block 3).

Search fields: Title, Abstract, Keywords (for Scopus and WoS); All fields (for Google Scholar, with manual relevance filtering at the title/annotation stage). The final search was conducted on 15 March 2025.

3.4. Screening Procedure

The selection of studies was carried out in two stages.

Stage 1 involved title and abstract selection: All retrieved records were checked for compliance with the inclusion/exclusion criteria at the title and abstract levels. At this stage, records that clearly fell outside the scope of the study were excluded.

As a result, a total of 4113 results were obtained. First, all duplicates were rejected (-1276). Then, 2837 results were subjected to a detailed screening. We first analysed the title, abstract, and keywords. Based on this

analysis, 759 items were rejected. Then, another 681 items were excluded as inappropriate because they did not relate to the main mechanisms for ensuring the security of Ukraine's information space.

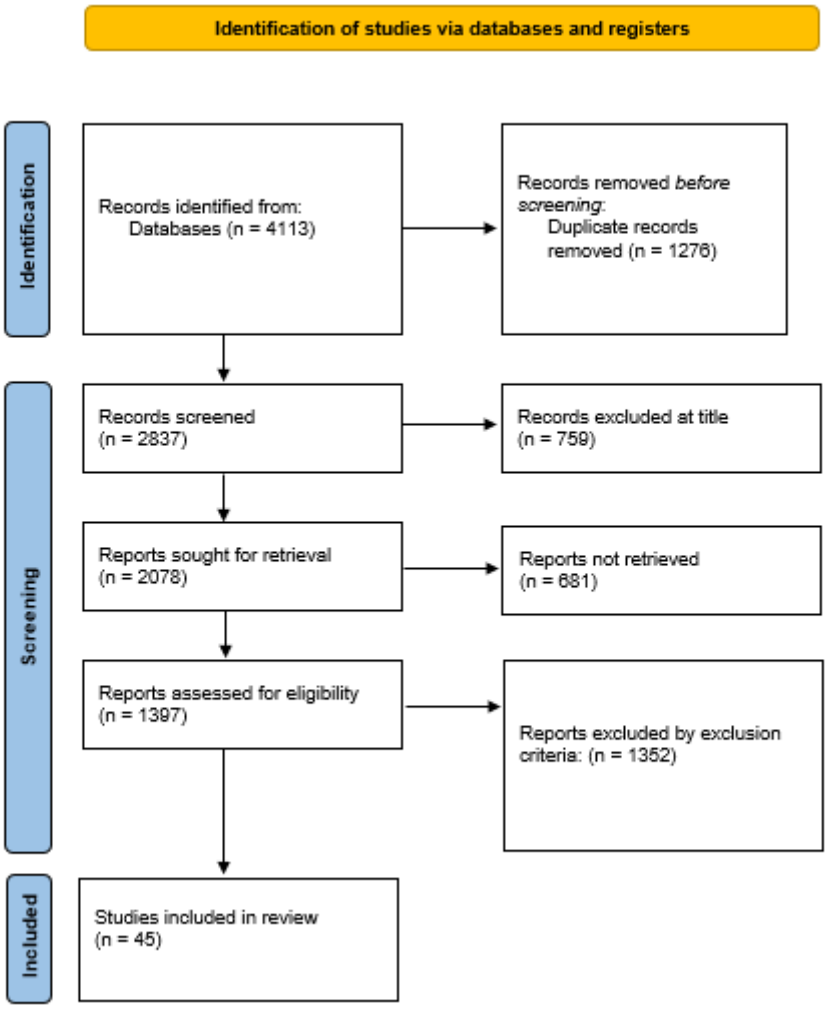

Figure 2. Counts at each selection stage.

Table 1. Inclusion and exclusion criteria

Criterion	Inclusion	Exclusion
Topic	Directly addresses information security, cybersecurity, or information warfare in Ukraine; analyzes globalization-related threats or countermeasures	Exclusively technical studies with no geopolitical or Ukrainian contextual dimension
Timeframe	Published 1991–2025	Published before 1991
Source type	Peer-reviewed articles, book chapters, conference proceedings, official policy documents, validated analytical reports	News articles, journalistic content, blog posts, unverified online sources
Language	English, Ukrainian	All other languages
Availability	Full text accessible	Abstract only (unless full-text request fulfilled)
Duplicates	—	Duplicate records removed prior to screening

Besides, all the remaining studies were evaluated according to the inclusion and exclusion criteria within the framework of global challenges. Stage 2 involved full-text assessment. In particular, potentially relevant records were

retrieved in full text and assessed for final inclusion. The reasons for exclusion at this stage were documented (see Table 1).

To reduce the risk of inconsistency, the following decision rules were applied to borderline cases: (a) when the relevance to the information security context of Ukraine was unclear from the abstract, the full text was retrieved; (b) sources related to cybersecurity in post-Soviet states without specific reference to Ukraine were excluded; (c) sources with dual relevance (e.g., regional comparative studies including Ukraine as a case) were included if findings specific to Ukraine could be identified.

3.5. Data Analysis

The analysis of the selected data was thorough and step-by-step. Data from the included publications were extracted and organized in Microsoft Excel using two structured matrices:

Matrix 1 – Threats: Author(s), year of publication, type of information threat (media manipulation, cyberattacks, disinformation, platform influence), historical period, key findings.

Matrix 2 – State responses: Author(s), year of publication, type of countermeasure (regulatory, technological, educational, international cooperation), identified resilience mechanisms, key findings.

Publications were coded according to four analytical categories aligned with the research questions: 1. Development period (1991–2013; 2014–2021; 2022–2025); 2. Threat type; 3. Countermeasure type; 4. Identified vulnerabilities and resilience factors; 5. After coding, a thematic synthesis and comparative analysis were conducted across different periods.

Given the diverse nature of the included sources, which ranged from empirical studies, qualitative case studies, content analysis, policy analysis, and cybersecurity reports, an assessment approach was applied that took into account the source type (see Table 2).

Table 2. Source type and evaluation criteria

Source type	**Appraisal criteria**
Empirical studies (quantitative/qualitative)	Clarity of research design; sample/data description; analytical transparency; peer-review status
Policy analyses and legal documents	Official provenance; currency; scope of applicability
Technical reports and analytical publications	Institutional credibility; methodology disclosure; recency
Conference proceedings	Peer-review status; specificity of findings

Based on this assessment, the selected materials were assigned a reliability rating for use in the Discussion section:

High reliability - modern empirical research with transparent methodology, published in Scopus/WoS-indexed journals.

Moderate reliability - peer-reviewed theoretical or policy analyses.

Indicative - "gray" literature, sources with limited methodological disclosure

In the Discussion section, conclusions that are supported primarily by high-confidence sources are presented as established conclusions; at the same time, theses based on moderate-confidence sources are presented as new trends or preliminary observations.

3.6. Use of Sociological Data

During the study, the results of sociological surveys conducted by specialists of the Global Digital Trust Insights Survey 2025 were additionally considered (Building cybersecurity through C-suite collaboration. 2025 Global

Digital Trust Insights Survey: insights for Government and Public Services, 2025). The analysis of these materials made it possible to consider public assessments of the level of security of information, to trace the degree of trust in existing state institutions in the field of cyber defense, and the attitude of citizens to international cooperation in countering digital.

4. Results

4.1. Globalization as an Operational Category

Within the framework of this study, globalization is considered not as a general historical background, but as a set of specific cross-border mechanisms that directly shape the information security environment of Ukraine. First, we are talking about ecosystems of global digital platforms, the algorithmic logic of which determines the speed and scale of content distribution, including disinformation. Second, transnational chains of production and distribution of media content allow information narratives to circulate outside national jurisdictions, which complicates regulatory response. Third, global advertising and financial markets in the digital environment create economic incentives for the distribution of polarizing or manipulative content. Diaspora networks also play an important role, which can act as both channels of international support for Ukraine and relays of external information influences. An additional factor is the limited enforcement capacity between jurisdictions and growing international cyber interdependence, which increases both the risks and the need for coordination with partners. Globalisation at the present stage poses an important challenge for the functioning of Ukraine's information security, given the seriousness of the challenges it faces. At the same time, globalisation and Russian aggression have emphasised the importance of developing information security, and the process of such emphasis has been quite long. In 2022, when a new wave of war began with the Russian invasion, all Russian news channels in Ukraine were blocked. This was a fair conclusion to the protection of the Ukrainian information space, which, according to many researchers, should have been cleared of Kremlin influence much earlier (Sopilko *et al.,* 2021). At the same time, threats to the information space have not disappeared (Kopachinska, 2021). The further spread of fake news, distributed through messengers, social networks, online platforms, etc., is observed. The analysis of the corpus of sources generally indicated a consensus that globalization affects Ukraine's information security not as an abstract background process, but through specific cross-border mechanisms. These include: algorithmic ecosystems of global digital platforms that determine the speed and scale of content distribution; transnational chains of media content production and distribution that take information narratives beyond national jurisdictions; global advertising and financial markets that create economic incentives for the distribution of polarizing content; and diaspora networks that can serve as both channels of international support for Ukraine and relays of external information influences (Sopilko *et al.,* 2021; Kopachinska, 2021).

However, researchers disagree in assessing the relative importance of external (global-platform) and internal (regulatory, institutional) factors in shaping the vulnerabilities of the information space. Some authors have drawn attention to the role of algorithmic logic of platforms (Radchenko *et al.,* 2023b; Pomerleau & Lowery, 2020). However, others have pointed to the priority of internal preparedness of the state and civil society (Buriak *et al.,* 2023). However, there is a lack of quantitative studies that would measure the comparative contribution of each of the identified mechanisms to real information incidents in Ukraine. Most sources are limited to qualitative characteristics without operationalized indicators.

4.2. State Information Operations And Strategic Narratives

The process of globalisation creates tangible unique opportunities for further development of the information space, but along with the prospects for further development, it will create significant challenges for Ukraine in the field of information security policy (Radchenko *et al.,* 2023b; Pomerleau & Lowery, 2020). Certain aspects of international threats should be highlighted and considered based on scholars' opinions (see Table 3).

4.3. Evolution of Threats by Phases: From the Post-Soviet Information Vacuum to Hybrid Warfare (1991–2025)

After the collapse of the Soviet Union in 1991, Ukraine's information field was not seriously controlled. Russian-language and less widespread Ukrainian-language resources focused primarily on social life and the difficult

economic situation in the post-Soviet territories. At the same time, using their widespread reach, Russian media began to put pressure on Ukrainian consumers by actively spreading new Moscow narratives. After 2014, the removal of Russian TV channels from the general network and cable TV lists was an extremely important response to the threat to Ukrainian information security. Since 2014, the distribution of Russian films and certain digital resources, including Russian social media, news resources, etc., which actively promoted the Russian vision of the complex events of the military operations, has been blocked (Krawczyk & Wiśnicki, 2022). In 2022, when a new wave of war began with the Russian invasion, all Russian news channels in Ukraine were blocked. This was a fair conclusion to the protection of the Ukrainian information space. However, the spread of fake news continues through messengers, social media, online platforms, and cyberattacks are also active. These findings confirm the conclusions of other scholars who have drawn attention to the gradual growth of the threat to Ukrainian information security (Andraško, 2021; Ryzhuk, 2018; Ryzhuk, 2018). During the 1990s, the Russian authorities did not have sufficient resources to put pressure on Ukraine's information field, but with the accumulation of financial resources, the Kremlin's appetite increased (Karamperidis *et al.,* 2021; Kairat *et al.,* 2023). It is worth agreeing with researchers who argue that after 2014, the Ukrainian authorities revised existing approaches to information security and made the right conclusions (Mazur *et al.,* 2025). As a result, since February 2022, the Ukrainian side has not yielded to Russian digital information influence. At the same time, there are other challenges, such as cyberattacks or the spread of propaganda (De Sousa Correia, 2021). This forces the Ukrainian information security sector to develop further.

Table 3. Challenges to Ukraine's Information Security Related to Globalisation

No	Challenge	Characteristics
1	Increasing number of cyber threats	Globalization has led to the active use of digital technologies in all areas of social life. Practical experience has shown that the most tangible damage is caused by digital attacks that are organized and aimed at the functioning of critical infrastructure, the work of state authorities, websites of state institutions, and various objects of strategic importance.
2	Information aggression	In the face of growing globalisation challenges, information warfare has become one of the most prominent tools for organising hybrid conflicts. According to estimates, about 60% of the fake news actively disseminated by Russian information influence groups in 2024 was aimed at discrediting the Ukrainian army, volunteer initiatives, and Ukraine's partnership with its international partners.
3	Uneven information access	This situation significantly complicates the formation of a single information space with a secure system of operation and established rules of the game. First of all, this unpleasant situation is relevant for rural areas, which have a lower degree of access to Internet information and knowledge about the use of innovative digital technologies is lower than in urban centres.
4	Legal regulation	The study of the current legal framework of Ukraine in the field of information security demonstrates the need for further improvement. First of all, it is necessary to take into account the new challenges associated with the use of artificial intelligence, blockchain technology or some other innovative digital solutions.
5	Need for well-established international cooperation	Certain global challenges can only be overcome by expanding Ukraine's participation in international initiatives, including cybersecurity alliances, programmes for exchanging practical experience with representatives of other countries, legal cooperation in countering cyber challenges, etc. In recent years, Ukraine has approved several agreements with EU member states on the exchange of information on cyber threats and coordination in cyber defence compliance.

Source: compiled by the authors based on (Bobro et al., 2024; Krawczyk & Wiśnicki, 2022)

The analysis shows that the identification of challenges is related to the general growth of cyber threats, targeted information aggression, uneven access to digital resources, legal regulation, and the need for international cooperation to overcome digital challenges. It is proposed to divide the challenges into objective and subjective ones.

The increase in the number of cyber-attacks is a general trend in the modern world, as the digitalisation of life makes it a convenient target for hackers and various fraudsters hunting for information (See Table 4).

Table 4. Matrix of evolution of information threats and responses in Ukraine (1991–2025)

Phase	Time	Actor	Main tactics	Goal	State response	Level of Evidence
I. Post-Soviet Information Vacuum	1991–2013	Russian state media	Gradual narrative through TV channels, newspapers	Formation of pro-Russian public sentiment	No systemic response	Moderate
II. Hybrid Escalation	2014–2021	Kremlin media, cyberattacks, trolls	Blocking of information, disinformation, cyberattacks on infrastructure	Destabilization of public opinion, undermining trust in the state	Blocked Russian TV channels, film production, social networks; development of cyber defense	High
III. Total Information War	2022–2025	Kremlin structures, hacker groups	Massive cyberattacks, disinformation through messengers, attacks on critical infrastructure	Undermining combat capability, spreading panic, discrediting the authorities	Complete blocking of Russian media; international coordination (CERT, EU, NATO)	Very High

4.3. Regulatory responses and institutional transformation in Ukraine and recommendations

After 2014, Ukraine underwent a systemic restructuring of approaches to information security. In particular, Russian TV channels, film production, and social networks were blocked; legislative acts were adopted that regulate cybersecurity and countering disinformation; and coordination mechanisms with international partners were developed. Researchers generally positively evaluated these steps as increasing the information resilience of society (Andraško, 2021; Ryzhuk, 2018; Belkin *et al.,* 2022). These results confirm the conclusions of other scholars that an important step towards improving the state of information security should be comprehensive solutions that would affect both internal Ukrainian affairs and the position of states in the international arena (Belkin *et al.,* 2022; Pidbereznykh *et al.,* 2022). A combination of reforms based on a study of modern hybrid strategies and international cooperation should become the basis for the development of Ukraine's digital information defence system (Suprunenko *et al.,* 2024). This makes it possible to confirm the main scientific hypothesis that strengthening Ukraine's information environment in times of globalisation is likely to be possible because of a combination of historical lessons learned, active cooperation with international environments, and the use of modern technologies to overcome internal and external threats.

However, the effectiveness of regulatory restrictions (including blocking) as an information security tool remains debatable: several authors have pointed to risks to freedom of speech and the limited ability of blocking to stop the spread of disinformation through instant messengers and VPNs (Kopachinska, 2021; Pidbereznykh et al., 2022). In addition, there is a clear lack of independent assessments of the impact of specific regulatory decisions on the level of information security of citizens. Moreover, according to sociological surveys, there are dynamic changes in the evolution of artificial intelligence. As a result of such technological complexity, the need for strengthening digital resilience and cybersecurity has increased. Besides, according to the PwC Global Digital Trust Insights Survey (2025), only 2% of surveyed organizational leaders in Ukraine reported implementing comprehensive cyber resilience measures across all operational levels. CISOs are 13% less confident in the resilience of information systems to the impact of artificial intelligence than CEOs (Building cybersecurity through C-suite collaboration. 2025 Global Digital Trust Insights Survey: insights for Government and Public Services, 2025). The main cyber threats are presented in Figure 3.

As shown in Figure 3, the dominant threats identified by Ukrainian organizational leaders include cloud-related vulnerabilities, data leakage operations, and attacks on connected devices. Notably, these threats are consistent with the cross-border mechanisms identified in the literature. This indicated that platform-dependent infrastructure has created points of influence that cannot be addressed by national regulatory tools alone.

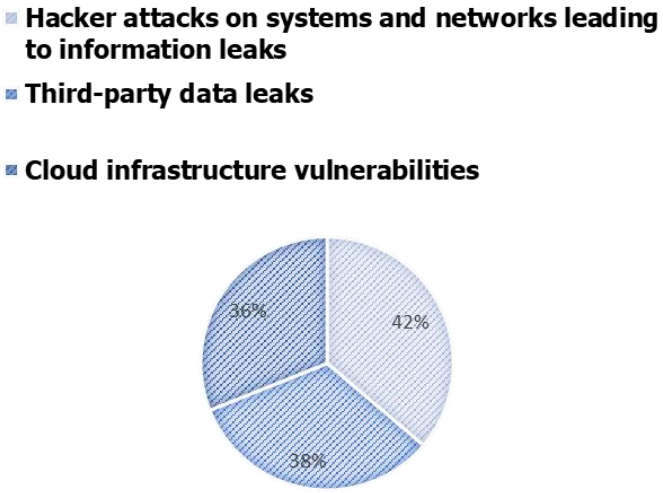

Figure 3. Main cyber threats according to sociological data

Source: Authors' elaboration based on PwC Global Digital Trust Insights Survey (2025)

Table 5. Recommendations for the Development of Ukraine's Information Security against the Background of Global Challenges

No	Recommendation	Description
1	Development of Ukrainian cyber defence capabilities	There is a need to create new centres for responding to cyberattacks and information campaigns that would work with innovative means of technological influence, operational monitoring and countering digital threats. One of the components of such a system is to increase funding for research related to cybersecurity, the use or development of innovative technologies, etc. It is also about forming a national information base on cyber threats, which would allow for a faster response to threats, periodic digital prevention of systems, etc.
2	Raising the level of media literacy	The call for effective national educational campaigns to teach citizens how to recognize disinformation and fake news is a very effective argument. Since state institutions still cannot control all information flows, there is a need for citizens and civil society organizations to counteract possible threats in the information field. The use of media literacy in the curricula of schools and higher education institutions, the development and distribution of relevant mobile applications, or the use of interactive platforms for this purpose will create effective opportunities to raise citizens' awareness of information threats.
3	Latest technologies	The use of modern innovative technologies, including artificial intelligence systems, machine learning, etc. will improve the situation with identifying and neutralising threats to the functioning of the information space. The use of additional technologies (e.g., blockchain) will provide additional opportunities for transparency and security of information transport. On the other hand, the automation of monitoring processes will allow for timely detection of threats and response to them, which can reduce the destructive impact and consequences of hacker attacks.
4	Intensification of regional development of information security	Creating opportunities to provide equal access to innovative digital technologies in all regions of Ukraine. This process can be used to create local cybersecurity centres that could strengthen the protection of local information resources in the regions, conduct trainings or other educational activities for local government officials, interested citizens, NGOs, etc. on the basics of information security.

Source: compiled by the authors based on (Lysetskyi *et al.,* 2024; Prokopowicz *et al.,* 2023; Zolotar *et al.,* 2023)

Thus, the challenges are related to the general increase in cyber threats, targeted information aggression, uneven access to digital resources, legal regulation, and the need for international cooperation to overcome digital challenges. These challenges can be divided into objective and subjective. The increase in the number of cyberattacks is a general trend in the modern world, as the digitalisation of life makes it a convenient target for hackers and various fraudsters hunting for information (Veshapidze *et al.,* 2022; Tarasenko *et al.,* 2022). Similarly, external information and digital attacks do not depend on Ukraine; as of 2025 they can be initiated primarily by the Kremlin regime. Instead, addressing issues related to the legislative framework, digital access, and participation in international partnerships is primarily within the domestic competence of the Ukrainian authorities (Lysetskyi *et al.,* 2024). Accordingly, it is quite possible to solve at least part of the tasks of building a strong information security field, especially given the available recommendations (see Table 5).

Therefore, important areas for improving the state of information security in Ukraine include the development of Ukrainian cyber defence capabilities, raising the level of media literacy of citizens and public officials, the use of the latest protection and monitoring technologies, and the intensification of regional development of information security.

The emphasis on these areas is based on the idea of the importance of technological development of individual information security systems, countering spam attacks, cyberattacks, and other modern challenges of the digital environment (Caviglione *et al.,* 2022; Kavitha & Radha, 2021; Buriak *et al.*, 2023). This makes it possible to deploy a reliable system of protection against potential threats to information security, both on the part of the relevant law enforcement and administrative structures and on the part of civil society's readiness to counteract the spread of fake news.

5. Discussion

The purpose of this article was to provide a comprehensive analysis of the impact of globalization on Ukraine’s information security through the lens of historical retrospective development. This objective involves several key components: examining changes in Ukraine’s information security system, identifying threats and challenges to the information environment, and formulating recommendations for its further development. The central scientific hypothesis is that the strengthening of Ukraine’s information environment in the era of globalization is most likely to result from a combination of lessons learned from history, active cooperation with international communities, and the application of modern technologies to counter internal and external threats. The proposed results show that after the collapse of the Soviet Union in 1991, Ukraine's information field was not seriously controlled. Russian-language and less widespread Ukrainian-language resources focused primarily on social life and the difficult economic situation in the post-Soviet territories. At the same time, using their widespread reach, Russian media began to put pressure on Ukrainian consumers by actively spreading new Moscow narratives. The results indicated that after 2014, the removal of Russian TV channels from the network and cable TV channels became an important response to the threat to Ukraine's information security. In 2022, all Russian news channels in Ukraine were blocked. (Andraško, 2021; Ryzhuk, 2018). This conclusion is supported by high-quality sources—peer-reviewed empirical studies indexed in Scopus/WoS—and is therefore considered the established conclusion of this review.

Researchers consider the occupation and annexation of the Crimean Peninsula to be the peak of Russian propaganda and information pressure, when Ukrainian society was unprepared for the deployment of Russian aggression, and even journalists from democratic European countries did not know how to comment on the events correctly (Karamperidis *et al.,* 2021; Sasko *et al.*, 2025). As a result, since February 2022, the Ukrainian side has not yielded to Russian digital information influence. At the same time, there are other challenges, such as cyberattacks or the spread of propaganda (De Sousa Correia, 2021; Krawczyk et al., 2024). The role of cyberattacks in the hybrid war against Ukraine is a result of high credibility, documented in numerous peer-reviewed empirical studies (Willett, 2022; Fedoniuk *et al.,* 2023; Hryshchenko *et al.,* 2025) and confirmed by institutional reports with moderate credibility. This forces the Ukrainian information security sector to develop further. The analysis shows that the identification of challenges is related to the general growth of cyber threats, targeted information aggression, uneven access to digital resources, legal regulation, and the need for international cooperation to overcome digital challenges. It is proposed to divide the challenges into objective and subjective ones. The increase in the number of

cyber-attacks is a general trend in the modern world, as the digitalisation of life makes it a convenient target for hackers and various fraudsters hunting for information (Prokopowicz *et al.,* 2023; Zolotar *et al.,* 2021).

A combination of reforms based on a study of modern hybrid strategies and international cooperation should become the basis for the development of Ukraine's digital information defence system (Suprunenko *et al.,* 2024). This makes it possible to confirm the main scientific hypothesis that strengthening Ukraine's information environment in times of globalisation is likely to be possible because of a combination of historical lessons learned, active cooperation with international environments, and the use of modern technologies to overcome internal and external threats.

The proposed hypothesis can also be confirmed by analysing the areas for improving the state of information security in Ukraine: development of Ukrainian cyber defence capabilities, raising the level of media literacy of citizens and public officials, use of the latest protection and monitoring technologies, and intensification of regional development of information security. Other scholars have also emphasised the importance of developing several areas at once, which would allow for a comprehensive approach to the formation of information strategies for the future (Akaneme & Metu, 2024; Bobro *et al.,* 2024). It should be noted, however, that evidence on the effectiveness of media literacy programs in active conflict settings remains largely indicative, as most available studies were conducted in pre-war or peacetime settings and lack quantitative measures of outcomes. Globalisation, according to some scholars, could stimulate the search for specific mechanisms for establishing information security, because despite all the challenges, globalisation as a process also contributes to the implementation of foreign experience (Taranenko, 2024; Tsekhmister, 2024). Such an approach should also be supported, as it will facilitate the use of foreign practices in Ukraine but can also demonstrate Ukrainian practices for global use.

Comparison of the proposed results with other international scientific studies also demonstrated that the Ukrainian case is part of broader global trends in the field of cyber threats. Just like in the EU or the USA, the most common challenges are large-scale cyberattacks on state and private resources (Fedoniuk *et al.,* 2023; Hryshchenko *et al.,* 2025). At the same time, the next place clearly belongs to disinformation campaigns (Melnyk *et al.,* 2023; Kuzmenko *et al.,* 2022; Recordati Koen, 2025). The Ukrainian experience has demonstrated a unique combination of all these threats in times of war. At the theoretical level, the results obtained made it possible to determine a model of information resilience during hybrid warfare. In practice, it should combine several interrelated elements: state cyber defense and the presence of an appropriate regulatory framework (Hasan, 2024); the evolution of technological capabilities, including monitoring and early warning systems (Zecchinon & Standaert, 2024); active involvement of civil society through media literacy and critical thinking (Pravdiuk, 2023; Vasconcellos de Carvalho Motta & Succi Junior, 2023). Such a model concentrates the Ukrainian experience and can become a subject for analysis in other countries facing similar challenges (Willett, 2022; Lysetskyi *et al.,* 2024). The value of the Ukrainian case is tangible in the practical plane. The Ukrainian experience could become a guide for NATO and the EU in the field of developing strategies for the operational blocking of information resources (Katerynych, 2022; Savytskyi *et al.,* 2025), integrating state and volunteer structures for better digital protection, and forming educational programs in digital literacy (Hanon, 2025; Pleskach *et al.,* 2024). Such mechanisms can also be useful in other regions where there is a risk of information aggression.

It is shown, that the globalization of the information space became main mechanism shaping Ukraine’s information environment increasingly dependent on the policies of global digital platforms and cross-border enforcement regimes. Platforms defined the rules for content moderation, algorithmic amplification, and information visibility, but these rules were formed outside the national jurisdiction of Ukraine. Therefore, important areas for improving the state of information security in Ukraine include the development of Ukrainian cyber defence capabilities, raising the level of media literacy of citizens and public officials, the use of the latest protection and monitoring technologies, and the intensification of regional development of information security. The emphasis on these areas is based on the idea of the importance of technological development of individual information security systems, countering spam attacks, cyberattacks and other modern challenges of the digital environment (Caviglione *et al.,* 2022; Kavitha & Radha, 2021; Kozak *et al.,* 2024). It is also important to consider that the educational component and a kind of regionalisation of information environment protection are integral parts of modern digital protection strategies that aim to consider not only the capabilities of administrative centres but also the periphery (Buriak *et al.,* 2023; Tarasenko *et al.,* 2022). This makes it possible to deploy a reliable system of protection against

potential threats to information security, both on the part of the relevant law enforcement and administrative structures and on the part of civil society's readiness to counteract the spread of fake news.

Table 6 below demonstrates the causal relationship between the summarized results of the literature synthesis and the proposed recommendations. Each policy proposal is based not on a single example, but on a cluster of consistent findings in scientific research, which increases analytical credibility and transparency in the transition from description to normative implications.

Despite the systematic approach, the study had several limitations. First, the review mainly covered publications indexed in Scopus, Web of Science, and Google Scholar, which may have limited the representation of local or non-specialist sources. Second, language limitations (mainly English-language publications) may have affected the completeness of coverage of Ukrainian and regional studies. Third, the available literature should reflect publication bias, in particular the tendency to analyze the most resonant events. A separate problem is the difficulty of verifying information in conditions of active armed conflict. Some studies relied on operational reports or secondary sources, which made it difficult to independently verify some statements. These limitations did not negate the main conclusions, but they require caution in their interpretation.

Table 6. Results summary

Key findings	Cluster of evidence in the literature	Political consequence
Disinformation spreads through algorithmic amplification of global platforms	Research on platform influence, information operations, digital ecosystems	Deepening cooperation with platforms, developing mechanisms for algorithmic transparency
Cyberattacks are a systemic component of hybrid warfare	Works on cyber operations against critical infrastructure	Strengthening cyber defense of state and energy infrastructure
Regulatory instruments 2014–2022 increased information resilience	Analysis of Ukrainian regulatory decisions after 2014	Institutional stabilization and improvement of the legal mechanism for blocking hostile resources
Level of media literacy affects susceptibility to information attacks	Research on civic resilience and educational programs	Integrating media literacy into educational policy
Transnational nature of threats limits national response tools	Works on jurisdictional constraints and international cyber interdependence	Expanding international coordination (EU, NATO, CERT networks)

6. Conclusion

The structured narrative review conducted allowed us to identify several generalized conclusions with varying degrees of analytical certainty. The most consistent finding in the literature is that information operations have become a systemic element of Russia's strategy of influence on Ukraine, and after 2014, an integral part of hybrid warfare. Studies have also demonstrated a consistent trend towards the growing role of global digital platforms as a medium for disinformation dissemination and, at the same time, as a space for international mobilization of support for Ukraine. It has been established that the combination of regulatory decisions, the development of cyber defense, and the institutionalization of media literacy programs after 2014 contributed to an increase in the level of information resilience of the state. At the same time, globalization against this background had a double effect: it expanded the opportunities for cross-border information attacks and, at the same time, created resources for international coordination.

However, the analysis revealed a number of uncertainties and debatable aspects. There is no clear consensus in the scientific literature on the long-term effectiveness of blocking information resources, the impact of algorithmic amplification on the formation of political beliefs, or measuring the real level of public vulnerability to disinformation under martial law.

The literature synthesis outlined several research gaps that had a high priority. First, an integrated model that would combine platform governance, cyber operations, and state information policy in a single analytical framework will need further development. Second, there is a lack of comparative studies that would allow comparing the Ukrainian experience with the practices of other states that have experienced systemic information operations. Third, empirical measurements of the effectiveness of media literacy programs and international cyber coordination based on quantitative data are needed. Fourth, an analysis of transnational diaspora networks as a factor in information mobilization and countering propaganda has become a promising direction.

Thus, Ukraine's information security in the context of globalization was formed at the intersection of cross-border digital systems, hybrid strategies of influence, and institutional adaptation of the state. Further research should focus not only on describing threats, but also on measuring their impact and comparative analysis of the effectiveness of responses in different national contexts. The value of the work was that it proposed important recommendations for further ensuring information security protection:

1. Development of Ukrainian cyber defense capabilities;
2. Increasing the level of media literacy of citizens and state administrators;
3. Use of the latest protection and monitoring technologies;
4. Activation of regional development of information security.

Therefore, the proposed results made it possible to systematize the historical experience of Ukraine in the field of information security, to form separate models of resilience during the active phase of hybrid information warfare. The novelty of the article lies in the combination of individual elements of retrospective analysis and current topical challenges of globalization. This made it possible to form separate practical recommendations for Ukraine and its international partners (EU, NATO). Ukrainian experience has demonstrated that the effectiveness of responses to hybrid threats is possible through the synthesis of historical lessons, the use of modern technologies and the involvement of a broad international coalition

References

Akaneme, I.N., Metu, C.A. (2024). Predicting mathematics achievement: the role of emotional intelligence and the academic self-concept. *Futurity of Social Sciences*, 2(3), 64-77. https://doi.org/10.57125/fs.2024.09.20.04

Akimov, A.V. (2023). Maritime security of Ukraine: Current status and development prospects under the conditions of martial law. In *Maritime security of the baltic-black sea region: Challenges and threats*. Baltija Publishing. https://doi.org/10.30525/978-9934-26-392-7-2

Andraško, J., Mesarčík, M., Hamuľák, O. (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: Challenges and opportunities for the EU legal framework. *AI & Society,* 36(2), 623–636. https://doi.org/10.1007/s00146-020-01125-5

Averianova, N., Voropayeva, T. (2020). Information Security of Ukraine: Social and Humanitarian Aspects. In *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, IEEE, Kharkiv, Ukraine. https://doi.org/10.1109/picst51311.2020.9467940

Aviv, I., Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. *International Journal of Critical Infrastructure Protection*, 43, 100637. https://doi.org/10.1016/j.ijcip.2023.100637

Belkin, L.M., Iurynets, J.L., Sopilko, I.M., Belkin, M.L. (2022). Culture and the use of information understanding in the field of national security (A case study of Ukraine). *Journal of International Legal Communication,* 5(2), 36–58. https://doi.org/10.32612/uw.27201643.2022.5.pp.36-58

Bidzilya, Y., Snitsarchuk, L., Solomin, Y., Hetsko, H., Rusynko-Bombyk, L. (2023). Ensuring media security in the era of information globalization. *Revista Amazonia Investiga*, 12(69), 249–259. https://doi.org/10.34069/ai/2023.69.09.22

Bobro, N., Bielikov, V., Matveyeva, M., Salamakha, A., Kharchun, V. (2024). Advancing Public Administration: Enforcing Strategic Methods and Utilising Tools. *Archives des Sciences*, 74(3), 201–206. https://doi.org/10.62227/as/74332

Bondarenko, S., Bratko, A., Antonov, V., Kolisnichenko, R., Hubanov, O., Mysyk, A. (2022). Improving the state system of strategic planning of national security in the context of informatization of society. *Journal of Information Technology Management*, 14(1). https://doi.org/10.22059/jitm.2022.88861

Borychenko, O., Cherniavskyi, A., Muliarevych, O., Shelekh, Y., Sabat, M. (2024). Cybersecurity in the energy industry of ukraine: Protection measures and challenges in the context of energy security. *Revista Gestão & Tecnologia*, 24(4), 67–90. https://doi.org/10.20397/2177-6652/2024.v24i4.2876

Brzozowska, A., Bubel, D., Nekrasenko, L. (2022). Determinants related to threats in information and informatics systems. In *Organisation management in the digital economy* CRC Press, 69–122. https://doi.org/10.1201/9781003271345-3

Building cybersecurity through C-suite collaboration. 2025 Global Digital Trust Insights Survey: insights for Government and Public Services. (2025). PwC. https://www.pwc.com/ua/en/survey/2025/cee-findings-from-the-2025-global-digital-trust-insights-survey/government-public-services.html

Buriak, I., Kalynovskyy, A., Pasko, M., Saienko, V., Zavolichna, T. (2023). Actual problems of management and public administration in modern globalization processes. *Pacific Business Review (International),* 16(4), 122-133. https://surl.li/nojvtz

Caviglione, L., Wendzel, S., Vrhovec, S., Mileva, A. (2022). Security and Privacy Issues of Home Globalization. *IEEE Security & Privacy*, 20(1), 10–11. https://doi.org/10.1109/msec.2021.3127372

Chmyr, Y., Nekryach, A., Kochybei, L., Dakal, A., Strelbytska, L. (2023). Postindustrial Society and Global Informational Space as Infrastructure Medium and Factor for Actualization of the State Informational Security. In *National Security Drivers of Ukraine* Springer Nature Switzerland, 61–73. https://doi.org/10.1007/978-3-031-33724-6_4

De Sousa Correia, R. (2021). Information security as digital economy critical success factor. In *Digital Transformation and Challenges to Data Security and Privacy* (p. 209-221). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-7998-4201-9.ch012

Dubyna, M., Panchenko, O., Shpomer, T., Shyshkina, O., Kosach, I., Bazilinska, O. (2024). The Role of Digitalization of the Payment Infrastructure in Ensuring the Economic Security of the State under the Conditions of Social and Political Shocks. *International Journal of Sustainable Development and Planning*, 19(3), 893–908. https://doi.org/10.18280/ijsdp.190308

Dykha, V., Dykha, M., Lukianova, V., Polozova, V., Ivanov, M. (2024). Energy security management in the context of current challenges and international experience. *Polityka Energetyczna – Energy Policy Journal*, 27(4), 133–154. https://doi.org/10.33223/epj/190485

Farmkhaus, P. (2024). Globalisation Challenges in the Development of Ukraine's National Information Policy. *Pakistan Journal of Life and Social Sciences (PJLSS)*, 22(2), 10314. https://doi.org/10.57239/pjlss-2024-22.2.00778

Fedoniuk, S., Karpchuk, N., Yuskiv, B. (2023). Ukraine's Information Security Policy: at the Crossroads between Russia and the West. *Politologický časopis - Czech Journal of Political Science*, (3), 184–205. https://doi.org/10.5817/pc2023-3-184

Fyshchuk, I., Pintsch, A. (2025). Cyber-Attacks in Ukraine: Coping with the Challenges at the Local Level in 2022–2024. *Risk, Hazards & Crisis in Public Policy*, 16(3). https://doi.org/10.1002/rhc3.70025

Garcia, B. (2021). Informação e Segurança no Ciberespaço: A influência da globalização na intensificação de riscos e ameaças na última década. *Ciências e Políticas Públicas / Public Sciences & Policies*, 7(1), 193–212. https://doi.org/10.33167/2184-0644.cpp2021.vviin1/pp.193-212

Hanon, J.P. (2025). Beyond Ukraine Debating the Future of War, edited by Tim Sweijs and Jeffrey H. Michaels. *European Review of International Studies*, 11(3), 475–485. https://doi.org/10.1163/21967415-11030003

Hasan, M. (2024). Russia–Ukraine Propaganda on Social Media: A Bibliometric Analysis. *Journalism and Media*, 5(3), 980–992. https://doi.org/10.3390/journalmedia5030062

Hryshchenko, S., Savchenko, V., Kumeiko, A., Patsuriia, N., Rieznikova, V. (2025). Current State of Information Security in Ukraine. *Danube*, 16(1), 16–29. https://doi.org/10.2478/danb-2025-0002

Hub, M., Příhodová, A.K. (2021). Impact of Globalisation on Data Security – Authentication Issues. *SHS Web of*

Conferences, 92, 05009. https://doi.org/10.1051/shsconf/20219205009

Iliev, A., Ilieva Nikolovska, A., Petrova, E. (2020). Historical retrospective of the integration in NATO and the European Union of the republic of north macedonia. In *Security horizons*. Faculty of Security- Skopje. https://doi.org/10.20544/icp.11.01.20.p30

Izmailov, Y., Yegorova, I. (2023). Possibilities of adapting the EU experience in information security to the conditions of Ukraine. *Economics and technical engineering*, 1(1), 35–43. https://doi.org/10.62911/ete.2023.01.01.03

Juneja, A., Goswami, S.S., Mondal, S. (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. *Journal of Technology Innovations and Energy*, 3(2), 1–22. https://doi.org/10.56556/jtie.v3i2.907

Kairat, K., Karlygash, A., Beglan, T., Saule, B., Talshyn, K., Viktor, T., Abai, K. (2023). Formalization of risk management in the context of digital business transformation. *Indonesian Journal of Electrical Engineering and Computer Science*, 30(3), 1428. https://doi.org/10.11591/ijeecs.v30.i3.pp1428-1439

Karamperidis, S., Kapalidis, C., Watson, T. (2021). Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches. *Journal of Marine Science and Engineering*, 9(12), 1323. https://doi.org/10.3390/jmse9121323

Kaspars, K. (2022). Prerequisites for the formation of a regional security system in the baltic-black sea union. *Three Seas Economic Journal*, 3(2), 29–34. https://doi.org/10.30525/2661-5150/2022-2-4

Katerynych, P. (2022). Comparative analysis of the information security environment in Ukraine and Poland (survey of journalists and editors). *Communication & Society*, 35(4), 37–53. https://doi.org/10.15581/003.35.4.37-53

Kavitha, M.G., Radha, D. (2021). Quality, Security Issues, and Challenges in Multi-cloud Environment: A Comprehensive Review. In *Operationalizing Multi-Cloud Environments*, Springer International Publishing, 269–285. https://doi.org/10.1007/978-3-030-74402-1_15

Kopachinska, G. (2021). Geopolitical View of Ukraine: History of Development and Specifics of its Current Transformation. *Quaestiones Geographicae*, 40(4), 47–62. https://doi.org/10.2478/quageo-2021-0037

Kozak, N.D., Rudynskyi, O.V., Kozak, D.O. (2024). Regulatory and Legal Aspects of Military Doctors and Pharmacists Training in Wartime: Continuous Professional Development at the Faculty of Retraining and Advanced Training of the Ukrainian Military Medical Academy. *Ukrainian Journal of Military Medicine,* 5(3), 30-38. https://doi.org/10.46847/ujmm.2024.3(5)-030

Krawczyk, D., Babenko, V., Yemchuk, L., Lienkov, S., Dzhulii, V., Dzhulii, L., Muliar, I. (2024). Analysis of Information Security under the Conditions of Hybrid War in Ukraine: Social Aspects. *Management Systems in Production Engineering*, 32(2), 235–243. https://doi.org/10.2478/mspe-2024-0023

Kuzmenko, A., Matviienko, L., Kanova, L., Burenko, M., Bukliv, R. (2022). Development of Ukrainian education and science in the context of global challenges and military aggression: results, problems, prospects. *Revista Amazonia Investiga*, 11(58), 177–185. https://doi.org/10.34069/ai/2022.58.10.19

Lysenko, S.M., Veklych, V.O., Kocherov, M.V., Servetskiy, I.V., Arifkhodzhaieva, T.B. (2023). Two dominant security concepts in Europe and its influence on Ukraine. *Prometeica - Revista de Filosofía y Ciencias*, (26), 43–51. https://doi.org/10.34024/prometeica.2023.26.14289

Lysetskyi, Y., Semenyuk, Y., Cirella, G. T., Pavlenko, D., Yuriyovich, G. A., & Demydkin, O. (2024). Conceptual Framework of Ukraine's National Security: Regulatory Examination Using Information and Communication Technologies. *In Contributions to Economics, Springer International Publishing*, 31–46. https://doi.org/10.1007/978-3-031-48735-4_3

Makovetska, N., Dubov, G., Didych, T., Malyshev, B., Varych, O. (2024). Global challenges to state sovereignty in the 21st century. *Salud, Ciencia y Tecnología - Serie de Conferencias*, *3*. https://doi.org/10.56294/sctconf2024.661

Maliarchuk, O., Rylieiev, S., Skrypnyk, M., Matsak, O., Kolomiiets, P. (2025). Reforming the tax system of ukraine in the context of globalization challenges. *Theoretical and Practical Research in Economic Fields*, 16(2), 460. https://doi.org/10.14505/tpref.v16.2(34).15

Mansoor, M.A., Salmanand, E.M., Al-Sartawi, A. (2022). Transformation of Managerial Accounting Trends in the Era of Digitalization. In *From the Internet of Things to the Internet of Ideas: The Role of Artificial Intelligence* Springer International Publishing, 717–723. https://doi.org/10.1007/978-3-031-17746-0_57

Marleku, A., Reka, B. (2018). Non-traditional security challenges as a main security threat to the Western Balkan countries. *Europolity: Continuity and Change in European Governance,* 12(2), 67–86. https://doi.org/10.25019/europolity.2018.12.2.03

Matviienkiv, S.M., Vdovychyn, O.V. (2024). Information threats in a full-scale war: current challenges for Ukraine's national security. *Politicus*, (5), 89–93. https://doi.org/10.24195/2414-9616.2024-5.13

Mazur, H., Bolhov, V., Akhnovska, I., Dluhopolskyi, O., Kozlovskyi, S. (2025). The impact of educational development on the countries' competitiveness in the knowledge economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (1), 140–146. https://doi.org/10.33271/nvngu/2025-1/140

Melnyk, M., Ivaniuk, U., Leshchukh, I., Halkiv, L. (2023). The Sustainable Development and Resilience of Socio-Economic System: Conceptualization and Diagnostics of Problems in Conditions of Global Challenges and Shocks. *International Journal of Sustainable Development and Planning*, 18(4), 1035–1043. https://doi.org/10.18280/ijsdp.180406

Nalyvaiko, L., Lebedieva, Y. (2022). Reproductive human rights: International standards, experience of ukraine and lithuania. *European Political and Law Discourse*, 9(4), 60–73. https://doi.org/10.46340/eppd.2022.9.4.6

Pidbereznykh, I., Koval, O., Solomin, Y., Kryvoshein, V., Plazova, T. (2022). Ukrainian policy in the field of information security. *Revista Amazonia Investiga*, 11(60), 206–213. https://doi.org/10.34069/ai/2022.60.12.22

Pleskach, M., Pleskach, V., Zaitsev, I. (2024). Human Cyber Security: Experience of Ukraine and Lithuania. In *2024 14th International Conference on Advanced Computer Information Technologies (ACIT)*, IEEE, Ceske Budejovice, Czech Republic, 511–516. https://doi.org/10.1109/acit62333.2024.10712592

Pomerleau, P.L., Lowery, D.L. (2020). Research Findings; Contemporary Perceptions of Canadian Security Professionals Regarding the Challenges in Sharing Information with the Public Sector. In *Countering Cyber Threats to Financial Institutions* Springer International Publishing, 123–156. https://doi.org/10.1007/978-3-030-54054-8_6

Pravdiuk, A. (2023). Information security of ukraine: Information influence and information wars. *European Political and Law Discourse*, 10(1), 111–121. https://doi.org/10.46340/eppd.2023.10.1.6

Prokopowicz, D., Gołębiowska, A., Such-Pyrgiel, M. (2023). The role of Big Data and Data Science in the context of information security and cybersecurity. *Journal of Modern Science*, 53(4), 9–42. https://doi.org/10.13166/jms/177036

Radchenko, O., Bielai, S., Kovach, V., Hrabar, N., Yevtushenko, I. (2023b). Formation of Information Security Systems of the State: Status, Trends, and Problems. In *National Security Drivers of Ukraine* Springer Nature Switzerland, 93–112. https://doi.org/10.1007/978-3-031-33724-6_6

Radchenko, O., Stepanko, O., Poroka, S., Piddubnyi, O., Omelchuk, V., Marchenko, S. (2023a). Essence and Content of State-Administrative Duality of "Legitimacy": "Legitimation" and its Place in the Information Security System of the Modern State. In *National Security Drivers of Ukraine*, Springer Nature Switzerland, 185–198. https://doi.org/10.1007/978-3-031-33724-6_11

Recordati Koen, M. (2025). Science of war, strategy in doubt: The ambiguity of military theory in the Age of Reason. *Nuova Antologia Militare,* 6(6), 539–586. https://doi.org/10.36158/979125669253815

Rogozińska, A. (2022). The security of Ukraine in the context of information warfare in cyberspace carried out by the Russian Federation. *Rocznik Instytutu Europy Środkowo-Wschodniej*, 20(2), 107–122. https://doi.org/10.36874/riesw.2022.2.6

Rohatiuk, I., Ivchenko, B.-Y., Kanfui, I., Solovyov, E., Yermenchuk, O., Denysenko, O. (2024). Economic security of Ukraine in wartime: challenges and prospects. *Revista Amazonia Investiga*, 13(81), 78–85. https://doi.org/10.34069/ai/2024.81.09.5

Ryzhuk, O.M. (2018). Providing information security of Ukraine during the hybrid war. *Politicus*, 2, 147–150. https://doi.org/10.24195/2414-9616-2018-2-147-150

Sasko, O., Shvedova, H., Orobets, K., Ovcharenko, R., Ostapenko, O. (2025). Criminal offence during martial law in ukraine: Peculiarities of qualification. *Bangladesh Journal of Multidisciplinary Scientific Research*, 11(1), 13–22. https://doi.org/10.46281/bjmsr.v11i1.2658

Savytskyi, V.L., Kozak, N.D., Verba, A.V., Kozak, D.O., Asaulenko, A.A (2025). The use of chemical warfare agents in the armed aggression of the russian federation against Ukraine: chemical weapons as an unconventional means of warfare. *Ukrainian Journal of Military Medicine*, 6(1), 5–61. https://doi.org/10.46847/ujmm.2025.1(6)-057

Seremciuk, K. (2025). Application of information technologies to ensure the national security of Ukraine under the conditions of martial law. In *Simpozion Ştiinţific al Tinerilor Cercetători. Ediţia a 22-a,* Academy of Economic Studies, 63–65. https://doi.org/10.53486/sstc2024.v2.12

Slayton, R. (2020). Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. *Science, Technology, & Human Values*, 46(1), 81–111. https://doi.org/10.1177/0162243919901159

Ślufińska, M. (2022). The Russia-Ukraine war: Two strategies of communication? In *Information security policy: Conditions, threats and implementation in the international environment*, Ksiegarnia Akademicka Publishing, 67–81. https://doi.org/10.12797/9788381388276.04

Sopilko, I., Svintsytskyi, A., Krasovska, Y., Padalka, A., Lyseiuk, A. (2021). Information wars as a threat to the information security of Ukraine. *Conflict Resolution Quarterly*, 39(3), 333–347. https://doi.org/10.1002/crq.21331

Stewart, H. (2022). Digital Transformation Security Challenges. *Journal of Computer Information Systems*, 63(4), 919–936. https://doi.org/10.1080/08874417.2022.2115953

Suprunenko, S., Pishenina, T., Pitel, N., Voronkova, A., Riabovolyk, T. (2024). Analysis of the Impact of Globalization Trends in the Digital Economy on Business Management and Administration Systems of Enterprises. *Futurity Economics&Law*, 4(2), 131–147. https://doi.org/10.57125/FEL.2024.06.25.08

Syvak, T., Shkliaruk, M., Kopanchuk, V., Postupna, O., Fendo, O. (2023). Structure and function of strategic communications in the system of national and informational state security. In *National security drivers of Ukraine,* Springer Nature Switzerland, 151–166. https://doi.org/10.1007/978-3-031-33724-6_9

Taranenko, A. (2024). Ensuring information security: Countering Russian disinformation in Ukrainian speeches at the United Nations. *Social Sciences & Humanities*, *10*, 100987. https://doi.org/10.1016/j.ssaho.2024.100987

Tarasenko, O., Mirkovets, D., Shevchyshen, A., Nahorniuk-Danyliuk, O., Yermakov, Y. (2022). Cyber security as the basis for the national security of Ukraine. *Cuestiones Políticas*, 40(73), 583–599. https://doi.org/10.46398/cuestpol.4073.33

Tsekhmister, Y. (2024). Medical informatics and biophysics in medical universities of European countries: A systematic review and meta-analysis. *Electronic Journal of General Medicine*, 21(2), em570. https://doi.org/10.29333/ejgm/14197

Vasconcellos de Carvalho Motta, B., Succi Junior, D.P. (2023). Brazilian foreign policy for the war in Ukraine: changing non-alignment, counterfactual, and future perspectives. *Globalizations*, 20(7), 1227–1240. https://doi.org/10.1080/14747731.2023.2224626

Vdovichen, A., Vdovichena, O., Krymska, A. (2024). Digital economy and cybersecurity: Analysis of threats and defense strategies in the context of institutionalization. *Economics. Finances. Law*, 4/2024, 135–140. https://doi.org/10.37634/efp.2024.4.28

Veshapidze, S., Otinashvili, R., Gvarutsidze, A., Abuselidze, G., Zoidze, G. (2022). Modern technologies to overcome the challenges of globalization. *Entrepreneurship,* 10(2), 22–32. https://doi.org/10.37708/ep.swu.v10i2.2

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival*, 64(5), 7–26. https://doi.org/10.1080/00396338.2022.2126193

Zecchinon, P., Standaert, O. (2024). The War in Ukraine through the Prism of Visual Disinformation and the Limits of Specialized Fact-Checking. A Case Study at *Le Monde*. *Digital Journalism*, 13(1), 61–79. https://doi.org/10.1080/21670811.2024.2332609

Zolotar, O.O., Zaitsev, M.M., Topolnitskyi, V.V., Bieliakov, K.I., Koropatnik, I.M. (2021). Prospects and status of defence information security in Ukraine. *Linguistics and Culture Review*, 5(S3), 513–524. https://doi.org/10.21744/lingcure.v5ns3.1545

Author Contribution Statement

Viktor Melnyk: Conceptualization, Methodology, Writing - Original Draft. Lyudmyla Babenko: Data Curation, Investigation, Writing - Review & Editing. Olena Dzhahunova: Formal Analysis, Visualization. Larysa Balycheva: Validation, Resources, Project Administration. Oksana Fedotova: Software, Investigation, Writing - Review & Editing. All the authors have read and agreed to the published version of the manuscript.

Does this article screen for similarity?

Yes

Conflict of Interest

The authors have no conflicts of interest to declare. There is also no financial interest to report. The author certifies that the submission is original work and is not under review at any other publication.

About the License

Cite this Article

Viktor Melnyk, Lyudmyla Babenko, Olena Dzhahunova, Larysa Balycheva, Oksana Fedotova, Disinformation and Cyber Operations in the Russia–Ukraine War: A Systematic Review of Threats, Mechanisms, and Countermeasures in a Globalized Media Ecosystem, Asian Journal of Interdisciplinary Research, 9(1), (2026) 233-253. https://doi.org/10.54392/ajir26115