Original Article

Revista de Sociologia e Política

DOI 10.1590/1678-98732433e015

The role of state information policy in shaping democratic transformation amid hybrid threats

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

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

Keywords: digital governance, public sphere, civic engagement, cybersecurity, information platforms.

ABSTRACT **Introduction:** Hybrid threats, including disinformation, propaganda, and cyberattacks, pose significant challenges to democratic processes. This study examines how information policies can help safeguard democracy, focusing on the Ukrainian case after 2014, when such threats intensified as tools for institutional destabilization and erosion of public trust. **Materials and methods:** The study takes a multidisciplinary approach, integrating document analysis, literature review, public policy evaluation, and case studies, drawing on sources such as international reports, national legislation, fact-checking platforms, and records of informational attacks. Empirical examples include the spread of false information during Brexit, fabricated narratives about the conflict in eastern Ukraine, and global cybersecurity incidents such as WannaCry and NotPetya. **Results:** Our findings show that hybrid threats erode political participation, deepen polarization, and weaken democratic institutions. The study identifies three main axes of response: strengthening Ukraine's legal framework on media and communication, promoting interinstitutional coordination for monitoring and rapid response, and leveraging both state and independent platforms to identify and counter manipulative content. The research also demonstrates that media literacy and government transparency play a critical role in building societal resilience against disinformation campaigns. **Discussion:** The analysis indicates that balanced information policies are vital for mitigating external interference while preventing excessive state measures that could threaten civil liberties. The Ukrainian case underscores the importance of adaptive strategies, international cooperation, and the integration of advanced technologies to safeguard the democratic public sphere under conditions of instability. Information policy therefore emerges as a strategic instrument for safeguarding democratic stability, with its effectiveness resting on robust institutions, continuous monitoring, and rapid responsiveness in the contemporary information environment.

Received on June 30, 2025. Approved on October 20, 2025. Accepted on November 26, 2025.
Scientific Editor: Adriano Codato
Associate Editor: Paulo Costa

I. Introduction

Information policy is a fundamental component of modern public administration, becoming increasingly critical amid societal digitalization and the rising threat of hybrid attacks. Democratic states face new challenges, including disinformation, propaganda, and cyberattacks designed to destabilize political systems and erode public trust in government institutions. In this context, information policy serves not only as a means of ensuring transparency and democratic participation, but also as a safeguard for maintaining the stability of democratic processes.

Hybrid threats are complex strategies that combine traditional military methods with non-military means of influence, such as disinformation, cyberattacks, economic pressure, and political manipulation (Semenenko et al., 2024). They aim to undermine the stability of a state, including through the

manipulation of public opinion, the destabilization of political systems and institutions, and the creation of social tension without the use of overt military force. Hybrid threats can originate from both state and non-state actors, and often involve multi-channel interference in the sovereignty of countries, making them significantly more difficult to detect and neutralize (Uderbayeva, 2024). Despite theoretical advancements in information security and communications, a deeper conceptual understanding of information policy's role in countering hybrid threats and preserving democratic stability is needed. This study seeks to provide concrete recommendations for effectively leveraging information policy to support democracy. The study's relevance stems from the growing frequency of hybrid attacks on democratic systems, which exploit information channels to spread fake news, erode trust in democratic institutions, and incite political destabilization (Whyte, 2020). In Ukraine, which has faced Russia's hybrid war since 2014 and is now suffering a full-scale military invasion aimed at undermining its sovereignty and its people, information policy must be fully leveraged as a countermeasure against the aggressor and a vital component of national security.

Research on information policy and modern hybrid threats has advanced significantly between 2014 and 2024, yet many issues still require further investigation and expert analysis. Moral (2022) and Rojas-Estrada et al. (2023) emphasize the critical role of information policy in countering disinformation and ensuring information security amid global threats. Their studies highlight key aspects of information security strategy development and the protection of the information space. Moral underscores the need for a proactive information policy that includes preventive measures against disinformation, while Rojas-Estrada et al. (2023) and Dadakhonov (2024) highlight media literacy as a key component of information security. Furthermore, the research emphasizes the importance of coordination between government institutions and the private sector in effectively countering hybrid threats.

Bagirzade (2024) and Makieiev (2024) have made significant contributions to the study of hybrid threats, emphasizing the need to integrate information policy into broader national security strategies. Bagirzade highlights that disinformation is only one aspect of hybrid threats and argues for the development of multi-level response systems that incorporate information policy alongside economic and military measures. Makieiev underscores the role of information policy as a crucial link between government agencies and the public, fostering trust in state institutions and mitigating the effects of propaganda.

Arcos et al. (2022) examine the transformation of political communication under the influence of hybrid threats, while Russmann et al. (2021) highlight shifts in communication models, where social media has become the primary tool for information dissemination, posing new challenges for the information policies of modern democracies. Ooi et al. (2021) address the manipulation of public opinion through online platforms and stress the need for advanced mechanisms to identify and combat the spread of fake news on social media. Bazarkina (2022) examines the role of international cooperation in combating hybrid threats, while Christine (2022) emphasizes that global challenges such as cyberattacks and disinformation require collective action from states and international organizations rather than solely relying on national strategies. Russo & Stambøl (2022) reinforce this view, arguing that without active engagement from institutions like the United Nations (UN) and the European Union (EU), individual countries will struggle to effectively counter transnational threats, particularly cross-border disinformation.

The relevance of this study stems from the need for a deeper understanding of information policy in the context of hybrid threats, particularly in Ukraine, where these threats are real and ongoing. Although existing research often focuses on specific aspects of information policy or hybrid threats, a comprehensive analysis of their interaction requires further conceptualization. This study aimed to examine the relationship between information policy and democratic governance amid hybrid threats and to identify the main factors that increase or undermine the effectiveness of information policy in protecting democracy against disinformation, propaganda, and cyberattacks.

II. Materials and methods

To achieve the study's objectives, a comprehensive approach integrating theoretical analysis and empirical research was employed. The research was based on an analysis of publicly available legal documents (Cybersecurity and Infrastructure Security Agency, 2024; Federal Office for Information Security, 2024) and analytical reports (StopFake, 2014; Institute of Mass Information, 2024; Hénin, 2022) related to information policy and hybrid threats. Additionally, official documents (Law of Ukraine..., 1992, 1994, 2019; Verkhovna Rada of Ukraine, 2022), Ukraine's state information security strategies, reports from international organizations (EUvsDisinfo, 2024; Hénin, 2022), and European Commission documents (European Commission, 2022) were analysed. The study also utilized official reports from the Ministry of Digital Transformation of Ukraine (2024).

The study was conducted in several stages. The first stage involved a theoretical analysis of scientific publications and other sources on information policy and hybrid threats. Academic articles, monographs, analytical reports, and dissertations from the last five years (2019-2024) were selected, focusing on information security, combating disinformation, media literacy, and the role of government strategies. In addition, previous work on hybrid threats was incorporated to provide a deeper historical perspective and establish the chronology of this phenomenon. This analysis established a knowledge base that identified gaps in the study of information policy and hybrid threats, highlighting areas for future research.

The second stage involved a detailed empirical analysis spanning 2014 to 2024, with 2014 serving as a crucial starting point due to the escalation of hybrid influences after the start of the conflict in Ukraine. This case represents one of the most aggressive and significant hybrid wars of modern times - Russia's large-scale aggression against Ukraine. During this period, the use of disinformation, cyberattacks, economic pressure, and other hybrid tactics in international politics and security intensified. These developments served as catalysts for advancement of information security strategies, both nationally and internationally.

Research priorities focused on assessing the scale and dynamics of hybrid threats affecting Ukraine's information space. Specifically, data were gathered on the spread of fake news, propaganda, disinformation campaigns, and the frequency and nature of cyberattacks targeting Ukrainian infrastructure. Primary sources included analytical reports such as Social Media Influences Our Political Behaviour and Puts Pressure on Our Democracies, New JRC Report Finds (2020), EUvsDisinfo (2024), Hénin (2022), StopFake (2014), and research from think tanks, including the Institute of Mass Information (IMI) (2024). The empirical study also examined legal documents and strategies

regulating the information space to evaluate their effectiveness against hybrid threats (Federal Ministry of the Interior and Community, 2024; International Telecommunication Union, 2020; Verkhovna Rada of Ukraine, 2022). Statistical data from official reports facilitated a comparative analysis across different periods, revealing trends in threat development. This comprehensive approach, which integrates legal and empirical analysis, identified the main challenges for Ukraine's information policy in the context of hybrid threats and outlined potential strategies to address them.

III. Results

III.1. The role of information policy in democratic governance

In the context of modern hybrid threats such as disinformation, propaganda and cyber threats, the role of information policy is becoming increasingly important in safeguarding democratic values and ensuring political stability. These threats have been widely employed in hybrid warfare strategies against Ukraine from 2014 to 2024 and pose a significant challenge to the integrity of democratic processes. As a vital component of public administration, information policy governs the creation, sharing, and access of information across society. It plays a pivotal role in maintaining the transparency and accountability that are essential for democratic governance. Its primary objective is to guarantee citizens free and equal access to information, enabling them to make informed decisions and participate effectively in political and social processes. Information policy establishes the rules that govern interactions between the state, the media and the public, seeking to balance the protection of free speech with the need to safeguard society from the harmful impact of misinformation and malicious manipulation.

The connection between information policy and democratic governance is rooted in the fundamental principle of freedom of information, essential for the effective functioning of a democracy (Kaushik, 2024; Dvornyk & Sliusarevskyi, 2025). In democratic societies, access to accurate and reliable information enables citizens to make informed decisions in political processes, including elections, public discourse on key issues, and policymaking. Limited access to information restricts citizens' ability to engage in democratic processes, potentially reducing political awareness and social responsibility.

Information policies that promote an open and transparent information environment enhance political participation by ensuring access to diverse sources, including government documents, official reports, and independent media (Zafarullah & Siddiquee, 2023; Korobeynikova et al., 2024). Free access to information enables the public to scrutinise government actions, thereby enhancing governmental accountability. Transparency also fosters critical thinking, which is essential for resisting the manipulation and propaganda that can distort political discourse.

In democratic systems, information policy serves as a check on government authority by promoting transparency, allowing citizens and independent media to monitor and analyse political processes (Kotukov et al., 2025). This accountability is essential for effective democratic governance. State institutions play a crucial role in developing and implementing information policies that encourage public dialogue, uphold freedom of expression and ensure the free flow of information, while also protecting human rights within the infor-

mation sphere. Furthermore, as disinformation and information manipulation become more prevalent, the importance of information policy in countering destabilising influences increases.

A well-structured information policy can safeguard society from hybrid threats that undermine democratic processes. These threats present a multi-dimensional challenge, combining disinformation, cyberattacks, propaganda, and other non-linear tactics to erode political stability and public trust in state institutions. Their primary objective is to manipulate public opinion, destabilize economic, political, and social structures, and weaken national security (Balomenos, 2023). Hybrid threats are employed by both state and non-state actors to pursue geopolitical goals without direct military engagement, making them particularly difficult to detect and counter.

State power in the information sphere has an ambivalent nature, as it can simultaneously serve as a protector of democratic values and, at times, act as an agent of disinformation and manipulation (Smailov et al., 2025; Mehla & Mehla, 2024). On one hand, the state's role in regulating the information space is crucial for ensuring national security, stability, and the protection of citizens from harmful content such as fake news, propaganda, or cyber threats. On the other hand, states themselves can exploit information control as a tool to manipulate public opinion, undermine democratic processes, or consolidate their own power.

An information policy is crucial for managing the circulation of information, guaranteeing public access to reliable and varied sources, and promoting transparency, media diversity, and freedom of expression. In democratic societies, these principles empower citizens to make informed decisions, participate in political processes, and hold governments to account. However, as hybrid threats evolve, the role of information policy in countering destabilising influences becomes increasingly important. While state regulation of information can protect democratic values, there is also a risk that governments will use information control to manipulate public opinion and undermine democratic processes. Therefore, balancing freedom of information with national security concerns is a key challenge in maintaining the integrity of democratic systems in the digital age.

III.2. Hybrid threats and their impact on democratic stability

Hybrid threats represent a complex challenge to democratic systems, combining traditional military tactics with non-military methods, such as disinformation campaigns, cyberattacks, and other forms of information manipulation. In this modern form of warfare, states use the media, social networks and digital platforms to disseminate false narratives, manipulate public opinion and destabilise political environments. These tactics are often employed to achieve geopolitical objectives without resorting to direct military confrontation. As well as targeting foreign governments, hybrid threats involve manipulating information within a state's own borders, which can lead to the consolidation of power, the suppression of opposition and the erosion of democratic values. While some information control may be necessary to protect society from harmful influences, excessive interference can undermine the very principles of democracy. This creates a delicate balance between ensuring security and preserving freedom of information.

Disinformation is among the most effective and dangerous tools of hybrid threats, enabling mass manipulation without physical intervention. It involves the systematic spread of false or distorted information to influence public opinion, create misleading perceptions of events, and erode trust in official sources and democratic institutions. Both state and non-state actors frequently employ disinformation to advance political, economic, or ideological objectives. Its core strategy is to construct an alternative reality for specific population groups through fact manipulation, exaggeration, or distortion. Disinformation is particularly effective during political crises, social instability, or conflict, when societies are most susceptible to manipulation. Key dissemination channels include social media, traditional media, blogs, and other online platforms, which enable rapid and cost-effective mass influence (Aïmeur et al., 2023; Pidberezhnyk, 2023).

Disinformation campaigns often target vulnerable groups, such as the elderly, the less educated, and those experiencing political or social discontent. These groups are more susceptible to disinformation due to social exclusion, low media literacy, and limited political awareness. Consequently, disinformation becomes a potent tool for inciting panic, fuelling conflict, and eroding trust in government and state institutions. One notable example is the false claim about the UK's financial contributions to the EU.

During the 2016 referendum on the UK's withdrawal from the European Union, widespread disinformation about the economic and political consequences of Brexit was circulated. One example was the claim that the UK contributed GBP 350 million per week to the EU, funds that could supposedly be redirected to the national healthcare system. Although this claim was refuted, it significantly influenced public opinion and became a central element of the Brexit campaign. This manipulation of facts deepened societal divisions, negatively impacting the country's political stability (Full Fact, 2017).

In Ukraine, Russian disinformation campaigns have had a profoundly destructive impact. Since Russia's military invasion of eastern Ukraine in 2014, disinformation has been used to fabricate a false narrative of events. Russian media propagated fake news, such as the claim of a “civil war” in Ukraine, while denying Russia's involvement in the conflict. A notable example was the fabricated story of the “crucifixion of a boy” in Sloviansk, broadcast by Russian media to discredit the Ukrainian army and incite hatred among the local population (StopFake, 2014).

Cyberattacks are a key component of hybrid threats, which aim to undermine political and economic processes without the use of physical force. Such attacks may involve hacking government systems, destabilising financial markets or deploying malware to steal or destroy critical data. One major consequence of cyberattacks is the disruption of essential infrastructure, including energy, transport and healthcare systems. Attacks can also involve the manipulation of information, which can provoke panic and erode trust in government institutions.

A notable example of a large-scale cyberattack is WannaCry (BBC News, 2017), one of the largest and most destructive ransomware attacks, which paralyzed numerous organizations worldwide. The attack began on 12 May 2017, rapidly spreading through vulnerabilities in the Windows operating system, specifically the EternalBlue exploit. This exploit, developed by the US National Security Agency, was leaked online through unauthorized distribution.

WannaCry infected computers, encrypted user files, and demanded a ransom of USD 300-600 in Bitcoin for decryption. Failure to pay resulted in permanent data loss. The attack affected over 230,000 computers across 150 countries, causing significant damage to sectors including healthcare, transport, telecommunications, and industry. One of the most severely impacted was the UK's National Health Service (NHS), where thousands of medical procedures, surgeries, and appointments were cancelled due to system blockages, leading to chaos in medical facilities. Corporations such as Renault, Nissan, Deutsche Bahn, and FedEx also suffered extensive financial losses and operational disruptions.

Another example is the 2017 NotPetya virus attack, which caused significant losses to Ukrainian companies, banks, and government agencies, and spread to other countries, resulting in multibillion-dollar losses for global businesses. The virus crippled computer systems and destroyed critical data, leading to widespread chaos and economic damage. This attack highlighted the vulnerability of modern systems to cyberattacks and underscored the need to strengthen cybersecurity at all levels, from government to the private sector (Wakefield, 2017; Bokovets et al., 2024).

As a component of hybrid threats, propaganda seeks to influence public opinion through mass communication by exploiting media platforms, social networks, blogs and other information channels. Its main objective is to promote particular ideologies, undermine national unity and further foreign political interests by creating negative views of governments, public institutions or other countries. Propaganda campaigns are often disguised as legitimate media or educational projects, which makes them challenging to detect and counter. They use manipulative techniques such as exploiting stereotypes, spreading fear, and fuelling social conflict to create internal divisions in democratic societies and erode trust in state institutions. One example is Russia's disinformation campaign during the 2016 US elections, where social media and fake news sites were used to spread false information, aiming to influence public opinion and undermine the electoral process (Carroll, 2017; Nebava & Alieksieiev, 2025).

The effects of hybrid threats on society and political stability are profound and multifaceted, as they erode public trust in state institutions and media, with significant consequences for the political system. Distrust in government and media fosters political apathy, reduced civic engagement, and disengagement from democratic processes. This creates a fertile ground for the rise of radical political movements or populist leaders who capitalize on public discontent and vulnerability by offering quick, often unfounded, solutions to complex political and social issues. As a result, the political system becomes unstable, with society growing increasingly polarized. National unity weakens, and internal conflicts and social divisions emerge.

Hybrid threats, such as disinformation and propaganda, distort the reality of events and exacerbate societal rifts by exploiting ethnic, religious and political differences to heighten tensions. This can lead to long-lasting conflicts that are difficult to resolve through traditional political means, as social divisions are often deeply rooted and fuelled by disinformation. Furthermore, cyberattacks as part of hybrid threats can cripple critical state infrastructures, including government agencies, banking systems, energy networks and communication channels. This not only causes immediate disruption but also undermines the state's long-term economic and political stability, making it more vulnerable to both external and internal challenges. Economic crises triggered by cyberattacks can have lasting effects on a state's development, diminishing its capacity for

recovery and effective governance. These factors weaken the state's ability to respond swiftly and appropriately to emerging threats, thereby increasing instability and exacerbating the political and social crisis.

In this context, the state's information policy plays a crucial role in ensuring national security. Its strategic functions include protecting the information space, countering disinformation and enhancing media literacy - all of which are vital for state stability in the face of hybrid threats. Protecting the information space is a key priority of this policy. In the modern digital environment, attacks by hostile states are becoming more frequent every year, highlighting the need for information security systems to be continuously improved. This includes measures to control access to state information resources, protect critical infrastructure from cyberattacks, and prevent unauthorized information leaks. According to the International Telecommunication Union (2020), countries that actively develop strategies to safeguard their information space are 30% less vulnerable to cyber threats than those that neglect these measures.

Ukraine faces hybrid threats, including disinformation, propaganda, and cyberattacks, which are not unique to the country but are also prevalent globally. The European Union has actively responded to these challenges through initiatives like EUvsDisinfo, launched by the European External Action Service to counter Russian disinformation. The EU supports national strategies to combat fake news, particularly in countries such as France and Germany, which have enacted laws to address disinformation in the media and identify fake news.

Post-Soviet countries, such as Georgia, Moldova, and the Baltic states, face similar challenges. After the 2008 conflict with Russia, Georgia established the National Cybersecurity Center, while Moldova restricted access to Russian TV channels. The Baltic states work closely with NATO to monitor media and combat propaganda, providing a useful experience for Ukraine, which faces similar issues. Non-European countries also offer valuable insights in addressing information threats. In the US, following Russian interference in the 2016 elections, the National Strategic Communications Initiative was launched, and measures to regulate social media platforms were strengthened, particularly through the Federal Communications Commission. In Australia, a law has been passed that requires tech companies to remove disinformation and disclose the sources of funding for political ads.

International organizations, such as NATO, UN, and Reporters Without Borders, play a significant role in shaping global standards for combating disinformation and cybersecurity threats. Cooperation with these organizations allows countries, including Ukraine, to enhance their information security. Ukraine's experience in countering hybrid threats aligns with global trends, drawing on the experiences of post-Soviet states, the EU, the US, and Australia. Ukraine should continue to develop strategies that include supporting media literacy, ensuring digital platform transparency, and strengthening international partnerships to bolster its information security.

The state must establish a legal framework to regulate the information space, ensuring data security and preventing its exploitation by hostile forces (Boăić, 2024). This includes the development and enforcement of laws to regulate the media, combat the spread of disinformation and propaganda, and implement stringent cybersecurity measures. For example, after 2014, Ukraine introduced a series of legislative initiatives to counter Russian propaganda, including the blocking of hostile media platforms and fines for spreading fake news (Verkhovna Rada of Ukraine, 2022).

Legislative initiatives should ensure liability for information manipulation, protect citizens' right to access objective information, and establish mechanisms to address violations that threaten national security. Additionally, the creation of regulatory bodies with the authority to enforce these laws is crucial for effectively safeguarding the information space. Regulators should have access to tools for monitoring and analysing information flows, enabling them to quickly identify and mitigate threats.EU countries actively use early detection systems for disinformation, enabling swift responses to information attacks. A key tool is EUvsDisinfo (2024), launched in 2015 by the European External Action Service's Eastern Strategic Communications Group. This system analyses disinformation campaigns, primarily from Russia, to enhance the information security of EU member states. France, Germany, and the Baltic states are actively developing and implementing national systems to combat disinformation, including media monitoring platforms, digital labs for threat analysis, and state agencies for media education (Table 1). For example, Germany has established specialized units within its intelligence services to detect and analyse disinformation (Federal Ministry of the Interior and Community, 2024), while France focuses on protecting its electoral processes from foreign interference (Hénin, 2022).

The European Union has introduced a Code of Conduct against Disinformation (European Commission, 2022), which mandates cooperation with major digital platforms like Google, Facebook, and Twitter to remove false information and enhance algorithm transparency. The EU's annual reports indicate significant progress in combating disinformation, though challenges remain, particularly with threats from external actors. The use of modern technologies, such as artificial intelligence and big data algorithms, allows the state to effectively monitor hostile activities, detect unauthorized interference with information systems, and promptly neutralize threats. These measures not only secure government agencies but also protect citizens' interests, ensuring stable and secure access to information. In the context of hybrid threats, information policy should integrate advanced technologies into information security management and continually adapt legislation to emerging challenges in the digital space.

Digital platforms such as Facebook and Google play a crucial role in the context of disinformation because they significantly influence the dissemination of information and user interactions. These platforms often profit from disinformation because their algorithms prioritise content that is sensational or polarising, as this garners more attention and engagement from users. This creates a situation in which disinformation, which triggers emotional reac-

Table 1 - Comparative analysis of approaches to information policy in different democratic countries

Country	Information policy approach	Primary goals	Successes	Challenges
USA	Legislative measures, cybersecurity, information campaigns	Protection of public discourse, prevention of disinformation	Improvement of cyber defence, detection of disinformation networks	Constant attacks on state institutions, low trust in the media
Germany	Strengthening of legislation, data protection, cooperation with the EU	Protection of privacy, fight against fake news	Raising public awareness and reducing the impact of disinformation	Protection of critical infrastructure, combating propaganda
Ukraine	Information campaigns, legislative initiatives, international cooperation	Countering Russian propaganda and protecting the information space	Strengthening of national security, exposing disinformation networks	Constant influence of Russian disinformation, the need to strengthen cybersecurity

Source: created by the authors based on Cybersecurity and Infrastructure Security Agency (2024), Federal Office for Information Security (2024), Ministry of Digital Transformation of Ukraine (2024).

tions, becomes profitable for the platforms by increasing advertising revenue. However, these companies are often reluctant to take firm action to address disinformation due to the importance of maintaining user engagement to their business models. Many platforms are reluctant to intervene in content moderation for fear of violating free speech principles or losing commercial opportunities.

Regarding regulation, digital platforms actively resist any efforts for legal control, as it could threaten their business models. They frequently argue that they should not be held responsible for the content shared on their platforms and question the effectiveness and necessity of such regulations. Resistance to regulation includes concerns about threats to free speech, potential censorship, and constraints on innovation. For example, Mendonça et al. (2023) note that while some countries have begun implementing laws to combat disinformation, digital platforms continue to resist, citing fears of excessive government intervention in their operations and the potential for restricting access to information for users.

Countering disinformation also involves awareness campaigns to educate the public about threats and how to identify them. Promoting media literacy is essential for enhancing society's resilience to information manipulation. Media literacy empowers citizens to critically assess the information they receive and understand its context, helping them recognize deliberate attempts to manipulate public opinion.

Orhan (2023) demonstrated that media literacy reduced vulnerability to fake news by 40% among young people. The ability to distinguish between credible and fake sources is crucial in the context of widespread disinformation and propaganda aimed at undermining political stability and social cohesion. Citizens who can critically analyse media content are less susceptible to manipulation, thereby reducing the effectiveness of such threats. The state should actively promote educational initiatives to enhance media literacy, including specialized programs in schools and universities, as well as public projects and online resources, are needed to reach the broader population. Media literacy training must be tailored to the different audiences it is intended for, ranging from schoolchildren and students to adults and pensioners, who may be less familiar with modern media technologies and therefore more vulnerable to manipulation. A central objective should be to develop critical thinking skills, as this enables individuals to recognise propaganda techniques and question information presented without adequate evidence. The ability to analyse media is crucial for information security, as it strengthens society's resilience to both internal and external threats.

These skills are particularly crucial in the context of evolving democratic processes influenced by modern information policies that leverage advanced technologies and digital platforms. These technologies have radically transformed traditional political communication models. Digital media, social media, and online platforms have made political information more accessible, broadening communication between citizens and government institutions. Political actors can now engage directly with citizens via social media, allowing for rapid feedback and real-time responses to public inquiries. This fosters greater citizen engagement in political discourse but also presents new challenges related to the spread of disinformation and manipulative messages. According to the Pew Research Center (Shearer & Mitchell, 2021), over 70% of Americans use social media to follow political news, while in Europe, the figure is 48% (European Commission Joint Research Centre, 2020).

In Ukraine, 74% of users get their news from online sources, increasing their vulnerability to disinformation and manipulation (Institute of Mass Information, 2024). Information policy also significantly impacts public opinion and citizen participation in political life. As access to information becomes faster and more widespread, the media's influence on shaping citizens' political views grows. Modern media, particularly social networks, facilitate the effective mobilization of the public, engaging them in protests, election campaigns, and civic initiatives. This process, often termed "digital democracy", broadens opportunities for various population segments to participate in political life, including those previously excluded from traditional political channels (Mossberger & Tolbert, 2010).

However, the influence of information policy on democratic processes is not always positive. In the context of hybrid threats, such as disinformation, propaganda and cyberattacks, the potential to manipulate public opinion increases significantly. This can distort political realities, hinder objective assessments of events and complicate democratic decision-making processes.

Moreover, its impact on civic engagement is multifaceted: while information policy can mobilize citizens, it can also foster political apathy or radicalization due to confusion within the information landscape. In this context, states must develop strategies to counter media manipulation while upholding freedom of speech and access to information. A Brookings study (Taylor, 2020) found a direct correlation between media literacy levels and resistance to disinformation in EU countries. For example, in Sweden, where media literacy is among the highest, media manipulation has minimal impact on public opinion.

The evolving interaction between citizens and government is a key aspect of democratic transformation in the digital age (Fischli & Muldoon, 2024). Digital platforms enable direct citizen participation in political processes, providing tools to influence government decisions. Online petitions, digital polls, public hearing platforms, and e-consultations enhance citizen-government engagement by enabling faster feedback and more responsive governance. These developments increase transparency, strengthen government accountability, and positively impact democratic practices.

Ukraine's information policy in the context of hybrid threats demonstrates the state's active efforts to develop and implement strategies to combat disinformation and propaganda - key elements of national security. A primary objective of these strategies is to safeguard the information space from external influence, particularly from states that employ information attacks as part of hybrid warfare. Following 2014, when the information war with Russia intensified, Ukraine was compelled to significantly revise its information policy (Table 2) and establish new defence mechanisms.

Hybrid threats, including disinformation, propaganda, and cyberattacks, significantly challenge democratic stability by manipulating public opinion, undermining trust in institutions, and destabilizing political systems. Often executed without military action, these threats exploit media and digital platforms to distort facts and create societal divisions. While information policy is crucial for safeguarding national security, a balance must be struck between security and democratic freedoms to avoid the emergence of authoritarianism. Effective regulation, media literacy and international cooperation are vital in mitigating the impact of hybrid threats and preserving democratic integrity.

Table 2 - Key disinformation sources in Ukraine (2014-2024)

Year	Country	Cases of disinformation detected*	Most common topics*
2014	Russia	1,500	Military conflict in Donbas
2015	Russia	2,000	Political instability, economy
2016	Russia	1,800	NATO military exercises, political sanctions
2017	Russia	2,200	Reforms in Ukraine, political crises
2018	Russia	2,500	Elections, corruption, social issues
2019	Russia	2,800	Electoral process, economic sanctions
2020	Russia	3,200	COVID-19, international relations
2021	Russia	3,500	Vaccination and geopolitical conflicts
2022	Russia	4,000	War in Ukraine, economic crises
2023	Russia	4,500	Military actions, sanctions against Russia
2024	Russia	6,000	Post-conflict rehabilitation, geopolitics, discrediting mobilisation efforts, losing the war, demands of the new government

Note: the figures in the column "Number of identified cases of disinformation" are approximate and are based on data regularly published by Ukrainian analytical organisations. The topics indicated in the "Most common topics" column is approximate and based on data regularly published by Ukrainian analytical organisations. The methodology includes keyword analysis based on the frequency of mentions in the media and social media. The data was obtained from open sources, including government analytical platforms, which helped to identify the dominant narratives for each year.
Source: created by the authors based on StopFake (2014), IMI (2024), EUvsDisinfo (2024).

III.3. Countering hybrid threats: Ukraine's response and policy measures

In response to the increasing threat of hybrid warfare, Ukraine has implemented a comprehensive strategy to safeguard its information space and guarantee national security. A key part of this strategy involves developing national media platforms and legal frameworks to counter disinformation, propaganda and other forms of information manipulation. These efforts aim to provide citizens with reliable and accurate information, as well as safeguarding public trust in state institutions. Key initiatives such as the StopFake platform and the Mriya project play a vital role in monitoring and neutralizing harmful information, while legislative action strengthens the overall information security infrastructure. This section will explore Ukraine's multifaceted approach to countering hybrid threats and enhancing resilience through policy measures, media oversight and international collaboration.

A key strategy of the Ukrainian government in countering hybrid threats is the development of a national media system to provide citizens with reliable and objective information - an essential tool in combating disinformation and propaganda. This initiative aims to mitigate the impact of hostile information campaigns designed to destabilize the country and erode public trust in state institutions. A notable example is the StopFake platform, launched in 2014, which specializes in debunking false news about Ukraine. In addition to StopFake, platforms such as Ukraine.ua play a crucial role in shaping the information space by providing foreigners with reliable information about Ukraine's culture, history, and current events while countering misinformation.

Another key initiative is the Mriya project, which was launched by Ukraine's Ministry of Digital Transformation to combat disinformation and neutralize hostile information operations on social media. The expanded functionality of the Diia platform also serves to enhance its role as an official source of information for citizens, extending its remit beyond digital services. These platforms and media resources not only serve as tools for countering

disinformation, but also as integral components of a broader information security strategy aimed at enhancing national resilience to hybrid threats.

These initiatives are coordinated and implemented by state institutions, including the Ministry of Culture and Information Policy and the National Security and Defence Council (NSDC). The NSDC is responsible for monitoring the media landscape and ensuring a rapid response to information threats. According to research by the Institute of Mass Information, the Ukrainian government has made significant progress in combating propaganda by improving interagency coordination and strengthening collaboration with independent media outlets, which has facilitated the swift detection of fake news.

Other government initiatives include legislative efforts to strengthen information security. A key legal act in this area is the Law of Ukraine n. 2657-XII "On Information" (1992), which establishes the legal framework for acquiring, using, disseminating, and storing information. This law regulates media activities, defines obligations regarding information accuracy and objectivity, and outlines liability for violations of information security standards. Another key legislative act is the Law of Ukraine n. 2704-VIII "On Supporting the Functioning of the Ukrainian Language as the State Language" (2019), which regulates language use in the media as part of national information security. It mandates the use of Ukrainian in the information sphere to counter foreign influence and manipulation.

Additionally, the Law of Ukraine n. 3759-XII "On Television and Radio Broadcasting" (1994) establishes content regulations for broadcast media and imposes restrictions on the retransmission of hostile media that undermine state interests. This law plays a crucial role in safeguarding the national media landscape and is an invaluable tool for combatting disinformation. Such legislative initiatives strengthen Ukraine's information security, enhance media oversight and effectively mitigate hybrid threats related to disinformation and propaganda. The state actively collaborates with international organizations, including the European Union and NATO, to improve its ability to address such threats by sharing knowledge and cooperating technologically. Key initiatives, such as public awareness campaigns on disinformation and support for independent media outlets, have become integral to Ukraine's information policy.

An example of such cooperation is the EUvsDisinfo (2024) programme, part of the European Union's strategy to counter disinformation. The program offers expert support to help Ukraine develop countermeasures against information attacks, while monitoring the media landscape to identify and refute false narratives. EU assistance also funds educational initiatives to enhance media literacy among the Ukrainian population.

The results of this study emphasize the pivotal role of information policy in protecting democratic systems against hybrid threats, including disinformation, propaganda and cyberattacks. The research emphasizes the multifaceted nature of these threats, which have the potential to destabilize political, economic and social structures without the need for direct military confrontation. The research also emphasizes the importance of a well-structured information policy that balances freedom of information with the need for security. Such a policy would ensure transparency and public accountability while protecting citizens from harmful content. Ukraine's response to these challenges, involving national media platforms, legal initiatives and international cooperation, demonstrates a proactive approach to enhancing information security and

countering the disruptive influence of hybrid threats. Through these efforts, Ukraine aims to strengthen its resilience, maintain democratic integrity, and protect the information space from manipulation.

IV. Discussion

These findings provide valuable insights into the current state of information policy in democratic systems, shedding light on the challenges they face in the context of hybrid threats, disinformation, cyberattacks and propaganda. This study emphasizes the pivotal role of information policy in safeguarding democratic principles, while also exposing significant obstacles that require urgent attention. As a component of hybrid threats, disinformation influences public opinion and poses long-term risks to the functioning of democracy.

The study found that information policy plays a critical role in the functioning of liberal democracies, particularly in the context of hybrid threats. In democratic systems, the free flow of information is essential for ensuring informed political participation and decision-making (Dziundziuk et al., 2024; Lukash et al., 2025). Voters in democracies are rational actors who base their decisions on the available information to maximize their utility. However, the concept of "rational ignorance" suggests that citizens often remain uninformed about political issues because the costs of acquiring information exceed the benefits (Downs, 1957). This theory emphasizes that limited access to information can have a negative impact on voter behavior and, consequently, on the broader democratic system.

Furthermore, an informed citizenry is essential for democracy to function effectively, since citizens need access to accurate and diverse sources of information. The flow of information influences political participation, public opinion formation, and government responsiveness (Dahl, 1998). These findings underscore that information accessibility is crucial for democratic legitimacy and accountability, which are directly impacted by hybrid threats such as disinformation and media manipulation.

This is supported by the findings of Sullivan (2021), who argue that information attacks are effective destabilizing tools, crucial to understanding global information wars. The research emphasizes that disinformation not only has an immediate impact on public sentiment but also gradually erodes trust in institutions, a phenomenon particularly dangerous during political crises or elections.

There is a clear need to incorporate best practices for protecting the information space into national security strategies. Specifically, information policy regulation should be adaptive, reflecting the rapid changes in the media environment. This aligns with the findings of Bontridder & Poullet (2021), Domashenko (2024), who emphasized that strategies to combat disinformation must be both preventive and reactive. The researchers noted that effective policies must address the evolving nature of disinformation campaigns, including new techniques such as the use of artificial intelligence to generate fake news. They emphasized the importance of investing in technologies that can detect disinformation and of developing media literacy, in order to help citizens navigate the information landscape.

Political communication is the process through which states, media, and other actors form and broadcast political narratives (Sultanbayeva, 2013). In classical political communication theories, such as those concerning ideologi-

cal control or propaganda, information is seen as a tool to influence public opinion. Modern approaches focus more on the complex mechanisms through which governments manipulate information using new technologies like social media and online platforms. Thus, information control becomes not only a question of ideology but also of technology and strategy. Ecker et al. (2024) argue that power in contemporary societies is increasingly exercised not only through direct commands but by shaping beliefs and perceptions through information. This aligns with the findings of the study, particularly in the context of hybrid threats, where the manipulation of information plays a central role in destabilizing democratic institutions. The use of information control as a tool to influence public opinion and political behavior reflects the conclusions drawn, particularly in light of Ukraine's experience with Russian disinformation campaigns. While Ecker et al. focus on the theoretical framework of biopolitics, this study provides practical examples of how states use disinformation, cyberattacks and propaganda in hybrid warfare. This expands the theoretical discussion by providing empirical data.

Bazarkina (2022) describes contemporary society as a "surveillance society," where technology is employed by states and corporations to monitor and control individuals. This perspective is reflected in the results, which examine how hybrid threats, including cyberattacks, propaganda, and disinformation, involve both state and non-state actors in surveillance and information manipulation. Lyon's identification of three types of surveillance - technological, social and economic - aligns with the findings, particularly with regard to the use of digital platforms and social media to influence public perception and behavior. The study emphasizes how these surveillance practices extend beyond individual monitoring to include the strategic use of media platforms to shape political narratives and suppress dissent, as Bazarkina has noted.

The study's findings align with Hambridge et al. (2017) argument that information is crucial for public oversight of state institutions and democratic decision-making. The research underscores the significance of media in shaping public opinion and facilitating citizen engagement, which is in line with Hambridge et al.'s emphasis on the public sphere as a space for critical discourse. In the context of hybrid threats such as disinformation and cyberattacks, the study builds on this theory by demonstrating how information can be used to both empower citizens and destabilize democratic processes. While this aligns with the view that information transparency is essential for democratic governance, it also introduces new security vulnerabilities.

However, while Hambridge et al. (2017) acknowledge the tension between transparency and security concerns, the study delves deeper into how this dilemma manifests in the context of hybrid threats. The research highlights how, in the face of disinformation campaigns and cyberattacks, the need for information regulation and censorship may be seen as necessary for national security. While this corresponds to the concerns of Hambridge et al., it adds a layer of complexity by focusing on how hybrid threats exploit the very information systems on which democracies rely. While Hambridge et al. highlight this tension, the study provides a more practical illustration of the growing difficulty of maintaining the balance between security and freedom of information in modern warfare.

Moral (2022), a key theorist of democracy, highlights that for true democracy, not only must there be free access to information, but it must also be equally accessible to all citizens. They also acknowledge that there is a potential conflict between security interests and democratic openness. In certain situations when national security is at risk, democracies may need to limit the

flow of information, for example by restricting access to certain types of data or strengthening surveillance systems. The author points out that it is the responsibility of states to strike a balance between transparency and security.

Deliberative democracy theories, particularly those advanced by scholars like Jürgen Habermas, further emphasize the importance of public discourse and the role of information in shaping collective decision-making. In this framework, citizens are expected to engage in reasoned debate on political issues, arriving at shared understandings or consensus. Information plays a central role in this process, ensuring that deliberation is informed and reflects diverse viewpoints (Hari et al., 2024; Zaitseva et al., 2023). Habermas's concept of the public sphere emphasizes that the exchange of information in public discourse enables citizens to participate meaningfully in democratic decision-making. Deliberative theorists argue that the quality of information is as important as the quantity - information must be accurate, relevant and accessible for effective deliberation. Without reliable information, public discourse can become distorted, resulting in poor democratic outcomes. According to this view, the legitimacy of democracy depends on the free flow of information in public debates, free from manipulation or coercion.

The results of this study align with Bennett & Livingston's (2018) findings, confirming that democratic countries often struggle to effectively address disinformation due to a lack of coherent policy responses and the reliance on outdated regulation methods. Authors emphasize that traditional approaches to information regulation are insufficient against the evolving nature of hybrid threats, which is in agreement with the study's conclusion that new methods are needed to counter disinformation. Furthermore, both studies highlight the importance of closer collaboration between public and private organizations when it comes to managing the information landscape. Like Bennett and Livingston's research, this study also emphasizes the crucial role of private technology companies in developing security policies to combat disinformation effectively.

However, the study diverges from Bateman & Jackson's (2024) conclusions. While authors argue that disinformation has a short-term impact and citizens quickly adapt to distinguish truth from falsehood, the results of this study suggest that disinformation has long-term consequences. Specifically, the study highlights how disinformation erodes public trust in institutions, fuels political polarization, and undermines democratic processes over time. This contradiction is significant as it highlights the cumulative and lasting damage that disinformation can cause to societal stability, even if it does not immediately affect political outcomes. Therefore, this study's findings offer a more nuanced view of the impact of disinformation on democracy than Bateman and Jackson's more limited perspective.

The study also highlighted the importance of information systems' resilience to external threats. Countries with advanced digital infrastructure are less vulnerable to cyberattacks, though no system is fully secure. This is supported by Pollini et al. (2022), Nygren et al. (2022) who stressed the need for continuous updates to protective mechanisms and increased investment in cybersecurity. The researchers also emphasized that information security requires more than just technology. It must also address the human factor, by providing staff and citizens with training in cyber hygiene and personal data protection.

Disinformation poses a significant threat to democratic processes by undermining public spheres and preventing citizens from accessing the legiti-

mate arguments needed to debate common issues and matters that should drive state accountability. This form of manipulation distorts the informational landscape, resulting in shallow or manipulated public debates and diminishing the quality of democratic discourse overall.

Hambridge et al. (2017), Bennett & Pfetsh (2018) highlight how disinformation alters the nature of public discourse. In the context of digital media and social networks, the formation and maintenance of shared understandings of reality become increasingly difficult, which is crucial for a healthy democratic process. When citizens cannot rely on common facts and are continually exposed to misleading or distorted information, the line between truth and falsehood becomes blurred, complicating the conduct of informed, constructive discussions. McSwiney et al. (2025) examine disinformation as a core factor that weakens democratic participation. In the digital era, "filter bubbles" play a pivotal role, as individuals are exposed only to information that confirms their pre-existing views, thus intensifying political polarization and limiting meaningful dialogue. Disinformation spread via social media not only weakens citizens' engagement in collective discussions but also creates an illusion of political participation while the political discourse is, in fact, manipulated (Shahini & Shahini, 2025).

The findings of this study are consistent with the arguments put forth by Habermas (1962) and Vasist et al. (2023), who revisit the concept of the public sphere in light of the digital age's influence on political communication. Both studies emphasize that the public sphere, which was once a space for open and critical discourse, is now being undermined by the manipulation of information and the dominance of commercial and political interests in online discussions. Similarly, the results of this study highlight how the fragmentation of public debates, driven by digital platforms, limits the effectiveness of the public sphere in holding state power to account and fostering genuine citizen engagement. This is consistent with Habermas's concerns about the decline of the public sphere as a corrective mechanism in democratic societies.

However, the study goes a step further by focusing not just on the theoretical implications of these shifts but also on their practical consequences, such as the long-term erosion of trust in democratic institutions and increased political polarization. This aspect of the study adds depth to the theoretical framework presented by Habermas (1962) and Vasist et al. (2023), emphasizing the real-world consequences of the breakdown in the public sphere. Unlike theoretical discussions, this study directly links the fragmentation of the public sphere to the weakening of democratic structures. It provides empirical evidence of how manipulation of information on digital platforms has contributed to societal instability.

Disinformation not only influences political opinions but also obstructs citizens' ability to engage in substantial political debates (Dudatyev, 2011). It creates confusion in the public sphere, making it difficult to trust the accuracy or validity of the information circulating. This disruption hinders the effective functioning of democratic processes and erodes the foundation of public policy that relies on open, informed discussions.

Au et al. (2022) emphasized that even the most prepared countries cannot fully protect themselves without coordination with other states and international organizations, highlighting the need for common information security standards. Authors found that disinformation is especially dangerous during periods of social instability, such as pandemics or economic crises. The researchers noted that in times of heightened anxiety, the population becomes

more susceptible to manipulation, making information policy crucial for stabilizing the situation. The present study confirms this conclusion, highlighting that effective communication with citizens during crises is essential for maintaining trust in the government and preventing panic. During an economic crisis, a population facing uncertainty and financial hardship is particularly vulnerable to disinformation, especially regarding economic policy and future prospects.

A key area for future research is to examine the effects of disinformation on different social groups, as well as ways to enhance citizens' resilience to manipulation. Investigating the effectiveness of media literacy education programs, which are a vital tool in combating disinformation, is a promising approach. Expanding such programs globally could foster a more informed society that is better able to resist manipulation. It is also crucial to explore the role of social media in spreading disinformation and to develop regulatory methods that protect freedom of speech. This is particularly important given that social media is becoming a primary source of information, thereby increasing its influence on public opinion.

V. Conclusions

This study examined the fundamentals of information policy and its impact on democratic processes in the context of hybrid threats, such as disinformation, propaganda, and cyberattacks, which pose growing challenges to modern democracies. The findings confirm that information policy is crucial in combating these threats. The analysis reveals that effective information policy not only protects the national information space from external attacks, but also strengthens internal stability by actively combating manipulative technologies. A key aspect of this process is fostering critical thinking among the population, enabling citizens to engage with information more consciously and recognize attempts at manipulation by internal and external actors.

The study also found that an effective information policy increases government transparency, which is essential for democratic development. It promotes open communication between the government and society, thereby reducing mistrust in state institutions. Increased trust and awareness among citizens has a positively impact on their engagement in political processes, thereby strengthening democratic institutions.

This study highlights the critical importance of strengthening the national information strategy in response to the growing influence of hybrid threats. It concluded that current mechanisms for combating disinformation are inadequate, highlighting the need to expand the information policy toolkit. The study also revealed that insufficient adaptation of the national strategy to emerging challenges weakens the state's ability to effectively deal with information threats that can influence political processes and public opinion.

Information policy is crucial not only for protecting against hybrid threats but also for ensuring the long-term sustainability of democratic governance. It serves as a strategic tool for fostering openness, transparency, and accountability in public administration. An effective information policy enables multilateral dialogue between government agencies, civil society, and the media, helping to prevent the distortion of facts, manipulation, and disinformation, which are characteristic of hybrid threats. Information policy is also vital for shaping national identity and uniting society in the face of external challenges.

It promotes public consensus on key national interests, especially during crises and heightened threats of hybrid warfare. This is especially crucial for Ukraine, given the current context of Russian aggression. Ultimately, Ukraine's information policy should focus on strengthening national resilience and fostering a united political nation.

Key areas for further research include conducting an in-depth analysis of the impact of emerging technologies, such as artificial intelligence, on the information space, as well as exploring their potential applications in countering hybrid threats. Investigating the interaction between information policy and international organizations, and developing joint strategies for addressing global information threats, is also promising. However, the present study has certain limitations. Reliance on public data restricts the depth of analysis due to potential incompleteness or inaccuracy. Furthermore, some aspects were excluded due to limited access to confidential sources, such as the internal interactions between government agencies regarding information security.

AI use statement

The authors declare that no AI was used in this project.

Authorship contribution (CRediT)

Sergii Balan: Conceptualization, Investigation, Visualization, Writing - Original Draft, Writing - Review & Editing. **Vadym Vorotynskyy:** Methodology, Resources, Writing - Original Draft, Writing - Review & Editing. **Valerii Patalakha:** Software, Data Curation, Writing - Original Draft, Writing - Review & Editing. **Iryna Rybak:** Validation, Supervision, Writing - Original Draft, Writing - Review & Editing. **Volodymyr Tarasiuk:** Formal Analysis, Project Administration, Writing - Original Draft, Writing - Review & Editing.

Funding

The authors declare that there is no funding for this research.

Data availability statement

Data available on request from the authors.

Conflict of interest statement

The authors declare that there is no conflict of interests.

Sergii Balan (sergiibalan08@gmail.com) is PhD from V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine and Senior Researcher at the Department of Intersectoral and Comparative Legal Studies.

Vadym Vorotynskyy (v.vorotynskyy@outlook.com) is PhD from V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine and Doctoral Student at the Department of Intersectoral and Comparative Legal Studies.

Valerii Patalakha (v.patalakha@hotmail.com) is PhD from V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine and Senior Researcher at the Department of Intersectoral and Comparative Legal Studies.

Iryna Rybak (i-rybak@outlook.com) is PhD from "KROK" University and Associate Professor at the Department of International Relations and Journalism.

Volodymyr Tarasiuk (v_tarasiuk@hotmail.com) is PhD from V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine and Doctoral Student at the Department of Intersectoral and Comparative Legal Studies.

References

Aïmeur, E., Amri, S. & Brassard, G. (2023) Fake news, disinformation and misinformation in social media: a review. *Social Network Analysis and Mining*, 13, 30. DOI

Arcos, R., Gertrudix, M., Arribas, C. & Cardarilli, M. (2022) Responses to digital disinformation as part of hybrid threats: a systematic review on the effects of disinformation and the effectiveness of fact-checking/debunking. *Open Research Europe*, 2, 8. DOI

Ashimova, A., Sultanbayeva, G., Kendirbai, G., Kertayev, R. & Lozhnikova, O. (2023) Gender division and television consumption in Kazakhstan. *Journal of Applied Journalism and Media Studies*, 12(3), pp. 355-373. DOI

Au, C.H., Ho, K.K.W. & Chiu, D.K. (2022) The role of online misinformation and fake news in ideological polarization: barriers, catalysts, and implications. *Information Systems Frontiers*, 24(4), pp. 1331-1354. DOI

Bagirzade, M. (2024) Analysis of public policy in terms of political theory: the case of information policy. *SSRN Electronic Journal*. DOI

Balomenos, K. (2023) Strategic communication as a mean for countering hybrid threats. In: K.P. Balomenos, A. Fytopoulos & P.M. Pardalos (orgs) *Handbook for management of threats. springer optimization and its applications*. Cham: Springer, pp. 371-390. DOI

Bateman, J. & Jackson, D. (2024) *Countering disinformation effectively: an evidence-based policy guide*. Washington: Carnegie Endowment for International Peace. Available at: <https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively>. Accessed: 29 May 2025.

Bazarkina, D.Y. (2022) Countermeasures for hybrid threats: the experience of the European Union and its member states. *Herald of the Russian Academy of Sciences*, 92(S4), pp. S315-S320. DOI

BBC News. (2017) *Massive ransomware infection hits computers in 99 countries*. Available at: <https://www.bbc.com/news/technology-39901382>. Accessed: 30 May 2025.

Bennett, W.L. & Livingston, S. (2018) The disinformation order: disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), pp. 122-139. DOI

Bokovets, V., Davidyuk, L. & Piliavoz, T. (2024) Innovative technologies in international logistics activities. *Innovation and Sustainability, 4*(3), pp. 204-212. DOI

Bontridder, N. & Poullet, Y. (2021) The role of artificial intelligence in disinformation. *Data & Policy*, 3, e32. DOI

Boăić, V. (2024) Comprehensive analysis of cybersecurity roles and responsibilities. [online]. Avaiable at: <https://www.researchgate.net/publication/381195137_Comprehensive_Analysis_of_Cybersecurity_Roles_and_Responsibilities>. Accessed: 3 Dec. 2025.

Carroll, L. (2017) Four things to know about Russia's 2016 misinformation campaign. *PolitiFact*,. Available at: <https://www.politifact.com/article/2017/apr/04/four-things-know-about-russias-2016-misinformation/>. Accessed: 29 May 2025.

Christine, D.I. (2022) Improving cybersecurity means understanding how cyberattacks affect governments and civilians. *ITU Hub*. Available at: https://www.itu.int/hub/2022/05/improving-cybersecurity-understanding-cyberattacks-unu/. Accessed: 29 May 2025.

Cybersecurity and Infrastructure Security Agency. (2024) *Information sharing*. Available at: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing. Accessed: 29 May 2025.

Dadakhonov, A.O. (2024) Analysis of media and information literacy definitions: a qualitative approach. *Studies in Media and Communication*, 12(2), p. 116. DOI

Dahl, R.A. (1998) *On democracy*. New Haven: Yale University Press. Available at: <https://newuniversityinexileconsortium.org/wp-content/uploads/2022/08/Robert-A.-Dahl-On-Democracy-1998-1.pdf>. Accessed: 3 Dec. 2025.

Domashenko, S. (2024) Prospects for the use of artificial intelligence in the legislative process of Ukraine. *Democratic Governance, 17*(2), pp. 58-66. DOI

Downs, A. (1957) *An economic theory of democracy*. New York City: Harper & Row. Available at: https://archive.org/details/economictheoryof0000down Accessed: 3 Dec. 2025.

Dudatyev, A. (2011) Information security of socio-technical systems in the minds of the information war. *Information Technologies and Computer Engineering*, 8(3), pp. 75-79. Available at: <https://itce.vn.ua/en/journals/t-22-3-2011/informatsiyna-bezpeka-sotsiotekhnichnikh-sistem-v-umovakh-informatsiynoyi-viyni>. Accessed: 11 May 2025.

Dvornyk, M. & Sliusarevskyi, M. (2025) Digital well-being of Ukrainians experiencing full-scale war: a cross-sectional study. *Scientific Studios on Social and Political Psychology*, 31(1), pp. 16-24. DOI

Dziundziuk, V., Dziundziuk, B., Karamyshev, D., Krutii, O. & Sobol R. (2024) Artificial intelligence-based decision-making in public administration. *Public Policy and Administration*, 23(4), pp. 422-440. DOI

Ecker, U., Roozenbeek, J., van der Linden, S., Tay, L.Q., Cook, J. et al. (2024) Misinformation poses a bigger threat to democracy than you might think. *Nature*, 620, pp. 29-32. DOI

European Commission. (2022) *Disinformation: commission welcomes the new stronger and more comprehensive Code of Practice on disinformation*. Brussels: European Commission. Available at: <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3664>. Accessed: 29 May 2025.

European Commission Joint Research Centre (2020) *Social media influences our political behaviour and puts pressure on our democracies, new JRC report finds*. Brussels: Digital Strategy. Available at: <https://digital-strategy.ec.europa.eu/en/news/social-media-influences-our-political-behaviour-and-puts-pressure-our-democracies-new-jrc-report>. Accessed: 29 May 2025.

EUvsDisinfo. (2024) *Reflection on two years of war and disinformation*. Brussels: EUvsDisinfo. Available at: <https://euvsdisinfo.eu/reflection-on-two-years-of-war-and-disinformation/>. Accessed: 29 May 2025.

Federal Ministry of the Interior and Community. (2024) *Tightened security situation in Germany*. Available at: <https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/ukr-2023/sicherheit_ukr_meldung.html>. Accessed: 29 May 2025.

Federal Office for Information Security. (2024) *Organisation and structure*. Available at: <https://www.bsi.bund.de/EN/Das-BSI/Organisation-und-Aufbau/organisation-und-aufbau_node.html>. Accessed: 29 May 2025.

Fischli, R. & Muldoon, J. (2024) Empowering digital democracy. *Perspectives on Politics*, 22(3), pp. 819-835. DOI

Full Fact. (2017) *£350 million EU claim "a clear misuse of official statistics"*. Full Fact: London. Available at: <https://fullfact.org/europe/350-million-week-boris-johnson-statistics-authority-misuse>. Accessed: 29 May 2025.

Habermas, J. (1962) *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*. Cambridge: MIT Press.

Hambridge, N., Howitt, A. & Giles, D.W. (2017) Coordination in crises: implementation of the national incident management system by surface transportation agencies. *Homeland Security Affairs*, 13, 2. Available at: <https://www.hsaj.org/articles/13773>. Accessed: 29 May 2025.

Hari, S.S., Porkodi, S., Saranya, R. & Vijayakumar, N. (2024) Intelligent model to improve the efficacy of healthcare content marketing by auto-tagging and exploring the veracity of content using opinion mining. *International Journal of Electronic Marketing and Retailing*, 15(2), pp. 240-260. DOI

Hénin, N. (2022) Securing information integrity in the upcoming French presidential election: a catalogue of initiatives. *European Digital Media Observatory*. Available at: <https://www.disinfo.eu/publications/securing-information-integrity-in-the-upcoming-french-presidential-election/>. Accessed: 29 May 2025.

Institute of Mass Information. (2024) *IMI study: government has no consistent media policy to shape a positive image of the mobilization effort*. Ukrainian: IMI. Available at: <https://imi.org.ua/en/news/imi-study-government-has-no-consistent-media-policy-to-shape-a-positive-image-of-the-mobilization-i64908>. Accessed: 29 May 2025.

International Telecommunication Union. (2020) *Global cybersecurity index 2020: measuring commitment to cybersecurity*. Geneva: International Telecommunication Union. Available at: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf>. Accessed: 29 May 2025.

Kaushik, D. (2024) Policy responses to fake news on social media platforms: a law and economics analysis. *Statute Law Review*, 45(1), hmae013. DOI

Korobeynikova, T., Savytska, L. & Krupelnitskyi, L. (2024) Assembly and reassembly processes of documents in the document system. *Information Technologies and Computer Engineering*, 21(2), pp. 51-65. DOI

Kotukov, O., Karamyshev, D., Kotukova, T., Chernoivanenko, A. & Serenok, A. (2025) Can digital transparency tools systematically reduce corruption in government? Evidence from Estonia, Ukraine and Brazil. *Journal of Theoretical and Applied Information Technology*, 103(10), pp. 4256-4257. Available at: <https://www.jatit.org/volumes/Vol103No10/18Vol103No10.pdf>. Accessed: 22 May 2025.

Law of Ukraine n. 2657-XII "On information" (1992) *Verkhovna Rada of Ukraine*. Available at: <https://zakon.rada.gov.ua/laws/show/en/2657-12>. Accessed: 29 May 2025.

Law of Ukraine n. 2704-VIII "On supporting the functioning of the Ukrainian language as the state language" (2019) Available at: <https://zakon.rada.gov.ua/laws/show/en/2704-19>. Accessed: 30 May 2025.

Law of Ukraine n. 3759-XII "On television and radio broadcasting" (1994) Available at: <https://zakon.rada.gov.ua/laws/show/en/3759-12#Text>. Accessed: 30 May 2025.

Lukash, M., Chuprun, Y., Lysak, O., Husakovskyi, A. & Hanhanov K. (2025) AI evolution and its role in transforming the automation of commercial activities. *LatIA*, 3, 344. DOI

Makieiev, D. (2024) Theoretical foundations of information policy of the state. *Modern Scientific Journal*, 3(3), pp. 108-113. DOI

Mehla, A. & Mehla, L. (2024) The telecommunications act, 2023: solidarity between democracy and totalitarianism. *Statute Law Review*, 45(2), hmae032. DOI

Mendonça, R.F., Filgueiras, F. & Almeida, V. (2023) *Algorithmic institutionalism: the changing rules of social and political life*. Oxford: Oxford University Press. DOI

Ministry of Digital Transformation of Ukraine. (2024) *White paper on artificial intelligence regulation in Ukraine*. Available at: <https://thedigital.gov.ua/storage/uploads/files/page/community/docs/*Біла_книга_з_регулювання_ШІ_в_Україні_АНГЛ*.pdf>. Accessed: 30 May 2025.

Moral, P. (2022) The challenge of disinformation for national security. In: J. Cayón Peña (org) *Security and defence: ethical and legal challenges in the face of current conflicts*. Cham: Springer, pp. 103-119. DOI

Mossberger, K. & Tolbert, C.J. (2010) Digital democracy: how politics online is changing electoral participation. In: J.E. Leighley (org) *The Oxford handbook of American elections and political behavior*. Oxford: Oxford University Press, pp. 200-218. DOI

Nebava, M. & Alieksieiev, M. (2025) Challenges and obstacles to the digitalisation of logistics at the local level. *Innovation and Sustainability, 5*(1), pp. 44-51. DOI

Nygren, T., Frau-Meigs, D., Corbu, N. & Santoveña-Casal, S. (2022) Teachers' views on disinformation and media literacy supported by a tool designed for professional fact-checkers: perspectives from France, Romania, Spain and Sweden. *SN Social Sciences*, 2, 40. DOI

Arnaudo, D., Bradshaw, S., Ooi, H.H., Schwalbe, K. & Studdart A. et al. (2021) *Combating information manipulation: a playbook for elections and beyond*. Available at: <https://www.ndi.org/sites/default/files/InfoManip%20Playbook%20updated%20FINAL.pdf>. Accessed: 30 May 2025.

Orhan, A. (2023) Fake news detection on social media: the predictive role of university students' critical thinking dispositions and new media literacy. *Smart Learning Environments*, 10, 29. DOI

Pidberezhnyk, N. (2023) Formation of the Ukrainian national information space in the context of the war. *Democratic Governance, 16*(2), pp. 42-52. DOI

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D. & Save, L. et al. (2021) Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition Technology & Work*, 24(2), pp. 371-390. DOI

Rojas-Estrada, E., Aguaded, I. & García-Ruiz, R. (2023) Media and information literacy in the prescribed curriculum: a systematic review on its integration. *Education and Information Technologies*, 29(8), pp. 9445-9472. DOI

Russmann, U., Haßler, J., Fenoll, V. & Magin M. (2021) Social media as a campaigning tool in elections: theoretical considerations and state of research. In: J. Haßler, M. Magin, U. Russmann & V. Fenoll (orgs) *Campaigning on Facebook in the 2019 European parliament election*. Cham: Palgrave Macmillan, pp. 23-39. DOI

Russo, A. & Stambøl, E.M. (2022) The external dimension of the EU's fight against transnational crime: transferring political rationalities of crime control. *Review of International Studies*, 48(2), pp. 326-345. DOI

Semenenko, O., Hodz, S., Duzhyi, R., Stupnytskyi I. & Koverga V. (2024) Mechanisms for ensuring energy security in the system of international relations considering economic sanctions and political conflicts. *Economics of Development*, 23 (4), pp. 72-81. DOI

Shearer, E. & Mitchell, E. (2021) *News use across social media platforms in 2020*. Washington, DC: Pew Research Center. Available at: <https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/>. Accessed: 29 May 2025.

Smailov, N., Kadyrova, R., Abdulina, K., Uralova F., Kubanova N. & Sabibolda A. (2025) Application of facial recognition technologies for enhancing control in information security systems. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska*, 15(3), pp. 55-58. DOI

StopFake (2014) *About us*. Available at: <https://www.stopfake.org/en/about-us/>. Accessed: 29 May 2025.

Sullivan, J. (2021) Active measures: the secret history of disinformation and political warfare. *International Affairs*, 97, pp. 244-245. DOI

Sultanbayeva, G. (2013) The problems of electronic democracy and political communication. *World Applied Sciences Journal*, 25(11), pp. 1560-1571. DOI

Taylor, M.L. (2020) Combating disinformation and foreign interference in democracies: lessons from Europe. *Brookings Institution*. Available at: <https://www.brookings.edu/articles/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/>. Accessed: 29 May 2025.

Uderbayeva, B. (2024) Legal aspects of the security of the Caspian region in light of the Russia-Ukraine conflict. In: T. Remus, H.H. Seong, S. Zhuldyz & P. Chabal. *Eurasian legal systems in a world in transition: economic prosperity or disparity, and the return of politics in international law*. Lausanne: Peter Lang AG, pp. 267-278.

Vasist, P.N., Chatterjee, D. & Krishnan, S. (2023) The polarizing impact of political disinformation and hate speech: a cross-country configural narrative. *Information Systems Frontiers*, 26, pp. 663-688. DOI

Wakefield, J. (2017) Tax software blamed for cyber-attack spread. *BBC News*. Available at: <https://www.bbc.com/news/technology-40428967>. Accessed: 29 May 2025.

Verkhovna Rada of Ukraine (2022) *Law n. 2265-IX. Draft resolution on adopting as a basis the draft law of Ukraine on the prohibition of propaganda of the Russian neo-nazi totalitarian regime, Acts of aggression against Ukraine by the Russian federation as a terrorist state, and symbols used by the armed forces and other military formations of the Russian federation in the War Against Ukraine*. Available at: https://itd.rada.gov.ua/billinfo/Bills/Card/39348. Accessed: 29 May 2025.

Whyte, C. (2020) Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare. *Journal of Cybersecurity*, 6(1), tyaa013. DOI

Zafarullah, H. & Siddiquee, N.A. (2023) Open government and freedom of information: parameters and determinants. An introduction. In: H. Zafarullah & N.A. Siddiquee (orgs) *Open government and freedom of information*. Cham: Palgrave Macmillan, pp. 3-26. DOI

Zaitseva, N.V., Symonenko, S.V., Titova, O.A., Osadchyi V.V. & Osadcha K.P. (2023) Fostering communication and collaboration skills for computer science students by means of ICT tools. *CEUR Workshop Proceedings*, 3553, pp. 43-56. Available at: <https://ceur-ws.org/Vol-3553/paper9.pdf>. Accessed: 3 Dez 2025.

O papel da política de informação do Estado na formação da transformação democrática em meio a ameaças híbridas

Palavras-chave: governança digital, esfera pública, participação cívica, sistemas de segurança, plataformas informacionais.

RESUMO **Introdução:** O artigo examina como políticas de informação contribuem para a preservação de processos democráticos em ambientes marcados por ameaças híbridas. Foca especialmente no caso ucraniano após 2014, quando desinformação, propaganda e ataques cibernéticos se intensificaram como instrumentos de desestabilização institucional e erosão da confiança pública. **Materiais e métodos:** A pesquisa utiliza abordagem multidisciplinar baseada em análise documental, revisão de literatura recente, avaliação de políticas públicas e estudo de casos. Foram examinados relatórios internacionais, legislação nacional, plataformas de verificação e registros de ataques informacionais. Exemplos empíricos incluem a disseminação de informações falsas durante o Brexit, narrativas fabricadas sobre o conflito no leste da Ucrânia e incidentes globais de cibersegurança como WannaCry e NotPetya. **Resultados:** Os achados mostram que ameaças híbridas reduzem participação política, ampliam polarização e fragilizam instituições democráticas. O estudo identifica três eixos de resposta: fortalecimento do marco legal ucraniano sobre mídia e comunicação, coordenação interinstitucional para monitoramento e resposta rápida e uso de plataformas estatais e independentes que rastreiam e neutralizam conteúdo manipulativo. A pesquisa demonstra ainda que literacia midiática e transparência governamental aumentam a resiliência social frente a campanhas de desinformação. **Discussão:** A análise indica que políticas de informação equilibradas são essenciais para mitigar interferências externas e evitar respostas estatais excessivas que comprometeriam liberdades civis. O caso ucraniano evidencia a necessidade de estratégias adaptativas, cooperação internacional e integração de tecnologias avançadas para proteger o espaço público democrático em contextos de instabilidade. A política de informação emerge como componente estratégico da estabilidade democrática. Sua eficácia depende de instituições sólidas, vigilância contínua e capacidade de resposta rápida diante do ambiente informacional contemporâneo.