http://dx.doi.org/10.18623/rvd.v23.n4.4678

FIMI VS DISINFORMATION: IMPACT ON DIGITAL SECURITY AND PUBLIC ORDER IN THE EU

FIMI VS DESINFORMAÇÃO: IMPACTO NA SEGURANÇA DIGITAL E NA ORDEM PÚBLICA NA UE

Article received on: 9/2/2025
Article accepted on: 12/1/2025

Antonina Shuliak*
*Lesya Ukrainka Volyn National University, Lutsk, Ukraine
Orcid: https://orcid.org/0000-0002-5234-0758
antoninamytko@vnu.edu.ua

Oleksandr Homaniuk*
*Lesya Ukrainka Volyn National University, Lutsk, Ukraine
Orcid: https://orcid.org/0009-0001-7635-6519
a1ex.ua.man@gmail.com

Yevheniia Vozniuk*
*Lesya Ukrainka Volyn National University, Lutsk, Ukraine
Orcid: https://orcid.org/0009-0009-5045-5269
voznyukyevhenija@vnu.edu

Olena Borysiuk*
*Lesya Ukrainka Volyn National University, Lutsk, Ukraine
Orcid: http://orcid.org/0009-0005-2228-1979
borisjuk.o1ena@vnu.edu.ua

Viktor Kobets*
*Lesya Ukrainka Volyn National University, Lutsk, Ukraine
Orcid: http://orcid.org/0009-0005-3941-6833
kobetsviktor2024@vnu.edu.ua

Hryhorii Zeleniuk*
*Lesya Ukrainka Volyn National University, Lutsk, Ukraine
Orcid: http://orcid.org/0009-0009-9760-9253
ze1eniuk.hryhorii@vnu.edu.ua

The authors declare that there is no conflict of interest

Abstract
The article explores the concept of Foreign Information Manipulation and Interference (FIMI) as a new analytical framework for countering disinformation in the European Union in the context of hybrid threats. It analyzes the evolution of information security as a component of the EU's strategic policy against the backdrop of increasing external interference, in particular, in connection with the Russian-Ukrainian war. The authors argue that FIMI differs from the traditional understanding of disinformation in its scale, systematicity, and institutional reach. The paper examines three main vectors of FIMI's impact on public order: political radicalization, mass distrust of the media and authorities, and social disintegration. It provides an analytical

Resumo
Este artigo explora o conceito de Manipulação e Interferência de Informação Estrangeira (MIIE) como uma nova estrutura analítica para combater a desinformação na União Europeia no contexto de ameaças híbridas. Analisa a evolução da segurança da informação como componente da política estratégica da UE, tendo como pano de fundo a crescente interferência externa, em particular, em ligação com a guerra russo-ucraniana. Os autores defendem que a MIIE difere da compreensão tradicional da desinformação na sua escala, sistematicidade e alcance institucional. O artigo examina três vetores principais do impacto da MIIE na ordem pública: a radicalização política, a desconfiança em massa nos media e nas

Este trabalho está licenciado sob uma licença Creative Commons

assessment of key narratives that erode democratic trust, destabilize governments, and contribute to political division in the EU. Particular attention is paid to the institutional responses of the European Union: from the creation of the East StratCom Task Force and the EUvsDisinfo initiative to the implementation of the Digital Services Act. The need to move from reactive counteraction to the formation of strategic communication and information resilience as a key tool for protecting the democratic system is highlighted. The article emphasizes the role of critical thinking, independent media and education as long-term safeguards against the influence of FIMI. In conclusion, it is proven that FIMI is not only a security challenge, but also a marker of civilizational vulnerability, which requires an interdisciplinary approach to research and a comprehensive response policy.

Keywords: FIMI. Disinformation. Fake. Security. Public Order. Ukraine. EU. Strategy. Media Literacy. Educational Initiatives. Russian-Ukrainian War.

autoridades e a desintegração social. Apresenta uma avaliação analítica das principais narrativas que corroem a confiança democrática, destabilizam os governos e contribuem para a divisão política na UE. É dada especial atenção às respostas institucionais da União Europeia: desde a criação da East StratCom Task Force e da iniciativa EUvsDisinfo até à implementação da Lei dos Serviços Digitais. Destaca-se a necessidade de passar de uma contra-acção reactiva para a formação de uma comunicação estratégica e resiliência da informação como ferramenta fundamental para a protecção do sistema democrático. O artigo enfatiza o papel do pensamento crítico, dos media independentes e da educação como salvaguardas a longo prazo contra a influência da desinformação. Em conclusão, demonstra-se que a desinformação não é apenas um desafio à segurança, mas também um indicador de vulnerabilidade civilizacional, o que exige uma abordagem interdisciplinar à investigação e uma política de resposta abrangente.

Palavras-chave: *Desinformação. Notícias Falsas. Segurança. Ordem Pública. Ucrânia. UE. Estratégia. Literacia Mediática. Iniciativas Educativas. Guerra Russo-Ucraniana.*

1 INTRODUCTION

In the 21st century, the information space has become a key theater of geopolitical confrontation. Increasingly, external state and non-state actors use disinformation, manipulation, and other non-kinetic tools of influence to achieve strategic goals without the overt use of force. Researchers and practitioners have argued for the identification of coordinated disinformation operations as a cybersecurity risk, considering the extensive overlap between the two in terms of tools and attack tactics (Čižik, 2017; Pandit, 2025).

In this context, the European External Action Service (EEAS) has proposed a new conceptual approach to identifying and countering such threats the FIMI (Foreign Information Manipulation and Interference) concept, which represents a structured framework for a systemic response to foreign information interference. The FIMI concept is being formed as a response to the growth of complex and deliberate campaigns aimed

at destabilizing political systems, delegitimizing democratic institutions, undermining public trust and violating information security. The definition of FIMI covers external attempts to distort, suppress, or manipulate information within the target state, including through the use of fake narratives, botnets, controlled media, hybrid accounts or influencing social platform algorithms. Importantly, such influence is not necessarily unlawful – it is often implemented within the framework of legal norms, but at the same time has a clear destructive purpose. FIMI in the EU context is related to activities to combat disinformation and fake news, as well as to counter manipulation and propaganda that undermine democratic processes and European values. This includes the use of various platforms (social networks, messengers, news agencies) and new technologies (such as AI) to spread harmful information.

The aim of the article is to analyze the phenomenon of FIMI as a new analytical framework for countering disinformation in the European Union, as well as to study its impact on digital security and public order. In particular, the authors set the following tasks: to reveal the essence and difference of FIMI from traditional forms of disinformation; to show its role in political radicalization, erosion of trust in the media and authorities, and social disintegration of the EU; to analyze the EU institutional and legal mechanisms (East StratCom Task Force, EUvsDisinfo, Digital Services Act, etc.) aimed at countering these threats; to outline the importance of strategic communication, critical thinking, independent media, and education for the formation of long-term information resilience.

2 MATERIALS AND METHODS

The methodological basis of the article is grounded on an interdisciplinary approach that combines elements of political science, security studies, information sociology, and strategic communications theory. The study uses a set of qualitative analysis methods that allow for a comprehensive understanding of the phenomenon of foreign information manipulation and interference as a systemic threat to digital security and public order in the European Union.

First of all, the content analysis method was used, which provided the systematization and interpretation of destructive narratives distributed in the EU digital

environment. Special attention is paid to the study of the semantic structure of fake messages, mechanisms of emotional framing and patterns of recurrence of key topics in transnational information campaigns.

The use of the case study method elements made it possible to conduct a targeted analysis of specific institutional initiatives of the European Union (in particular, EUvsDisinfo, East StratCom Task Force, Digital Services Act), aimed at neutralizing FIMI operations. The study is accompanied by a review of practical tools for verifying and countering disinformation flows, as well as an analysis of their effectiveness in selected EU member states. To compare different models of responding to the FIMI threat, the comparative analysis method was used, which allowed comparing approaches to information security at the level of individual states and institutions of the European Union. The differences in legal and communication mechanisms for countering disinformation are separately considered.

Thus, the methodology of the article involves a combination of empirical and theoretical approaches, which allows for a comprehensive understanding of FIMI as a multidimensional phenomenon, assessing its impact on public order in the EU, and suggesting directions for institutional response to information threats.

3 RESULTS and DISCUSSION

3.1 Literature review briefly

In recent years, the scientific community has increasingly investigated the relationship between FIMI and the growing threats to digital security and public order in the European Union. The relevance of the topic has increased against the backdrop of Russia's full-scale invasion of Ukraine, which was accompanied by massive disinformation campaigns in the digital environment. One of the key theoretical approaches to understanding the narrative component of disinformation aggression is the concept of "connective strategic narrative" proposed by A. Zakharchenko (2025). The researcher argues that sustainable communication narratives play a crucial role in strengthening the national and international information front, allowing democratic actors to effectively counter FIMI operations through value-oriented mobilization of public

opinion.

Liagusha and Iarovyi (2025) approach the problem from a similar perspective, considering memes as an element of the information culture of resistance in the context of hybrid warfare. Their work emphasizes the role of digital folk art as a factor in strengthening the resilience of democratic societies to manipulative influence. In this context, disinformation is interpreted as a challenge not only to factual truth, but also to the symbolic order of democracy.

The technical aspects of the spread of disinformation in social networks are analyzed by Menaouer et al. (2025), with applying deep learning and graph neural networks methods to a large-scale corpus of tweets. The results obtained by these scholars indicate a high level of emotional polarization of information flows, which creates risks of radicalization and loss of trust in institutions. The studies of Xu et al. (2025) have a similar focus, demonstrating the active interaction of bots and people on Reddit and Twitter platforms in the context of the Russian-Ukrainian war. The authors prove that bots act as catalysts for the spread of fake messages and anti-Western narratives, which directly correlates with challenges to digital security.

From a practical perspective, resistance to disinformation influence is analyzed in the study by Helmus and Holynska (2024), which summarizes the experience of Ukrainian resistance to information attacks. In particular, the emphasis is placed on the role of volunteer initiatives, civil society, and local digital networks in building a horizontal structure of information counteraction.

In the theoretical and modeling dimension, an important contribution is made by the work of Yuskiv et al. (2024), who propose a model of strategic reconstruction of disinformation based on the analysis of communicative intentions. This approach allows not only to respond to the fact of a disinformation attack, but also to predict the logic of its construction, the target audience, and potential escalation. This approach is important for the formation of preventive security strategies. Another significant analytical perspective is provided by Yuskiv and Karpchuk (2025), who examine the impact of Russian information manipulation on public opinion in the run-up to the 2022 invasion. The authors argue that the manipulation was systemic, multi-channel, and strategically woven into perceptions of international legitimacy. This case illustrates how FIMI can not only erode trust but also create the conditions for geopolitical escalation.

Particular attention is paid to the effectiveness of labeling propaganda sources. For example, Aguerri et al. (2024) investigate the impact of the "Russia state-affiliated media" tag on Twitter on user perceptions and trust in content. The researchers record a small but positive effect in increasing the audience's critical thinking. In contrast, Okholm et al. (2024) question the effectiveness of prohibitive mechanisms, such as censorship or blocking of Russian resources, arguing that they can lead to the opposite effect in marginalized digital communities in Europe.

The cybersecurity dimension of the topic is highlighted in the work of Kravchenko et al. (2024), which emphasizes the close intertwining of information and cyber threats in the FIMI format. Researchers consider foreign information interference not only as communicative pressure, but as a form of digital aggression aimed at undermining trust in state institutions and public order as a whole. Homaniuk (2024) considers the role of international cooperation in the context of cybersecurity, emphasizing the importance of joint efforts of governments, the private sector and international organizations such as the UN, NATO, and the EU. Thus, the analysis of available publications demonstrates the complex nature of FIMI as a threat, simultaneously covering the narrative, technical, political, and cultural levels. Strategic counteraction to these influences requires a combination of institutional policy, digital literacy, technological modernization and communicative resilience. Scientific literature indicates the need for an interdisciplinary approach to the study of disinformation in a hybrid environment, where FIMI is not only an informational, but also a security and civilizational threat.

3.2 FIMI scope and dimensions

In the era of digital transformation, information has become a new dimension of power, and its manipulation has become a tool of hybrid influence. Disinformation and other forms of deliberate distortion of the information environment have become a strategic challenge for democratic states. These threats are particularly acute for the European Union, which has found itself at the epicenter of the global confrontation for truth, trust, and control over the minds of citizens. In response to systematic foreign interference in the information space, the EU has developed the FIMI concept, which defines new principles for protecting digital security and public order (What is Foreign

Information Manipulation and Interference (FIMI) and how does it affect democracy, 2025, March 13).

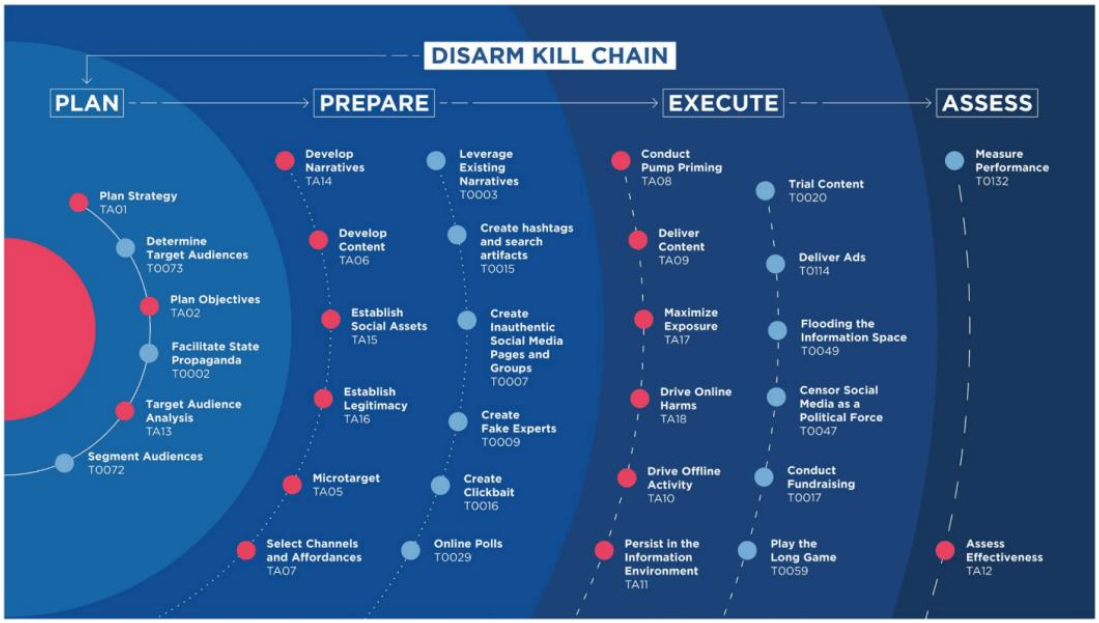
Unlike the traditional understanding of disinformation as individual fake messages, the FIMI concept outlines a holistic phenomenon - the systematic activity of external actors (state or related to them) aimed at distorting the information environment, undermining the legitimacy of institutions, inflaming social tension and destabilizing democratic processes. It is not just about the dissemination of false information, but about a complex campaign that includes context manipulation, the use of botnets, pseudomedia, algorithmic influence, and even artificially created crises of trust (Kochar, 2025; Sługocki, & Sowa, 2021).

The difference between FIMI and disinformation is not only in scale. While disinformation can be a one-time action, FIMI is a planned intervention with a strategic goal. As the European External Action Service (EEAS) points out, within FIMI, attackers adapt their narratives to the socio-cultural characteristics of their audiences, operate through local channels, and their attacks are synchronized with political events (elections, crises, military conflicts). This turns the problem into an infrastructural threat to EU security (Bryjka, 2024).

One of the main consequences of FIMI is the undermining of digital security. In the digital environment, not only infrastructure objects are subject to attacks, but also citizens' trust. Due to manipulative messages, staged attacks and "sensations", the boundaries between truth and lies are blurred, as a result of which society becomes vulnerable to panic, polarization, and loss of orientation (Jackson, 2023). According to the EEAS study, FIMI-type attacks in 2022-2024 covered not only the Eastern Partnership countries, but also the EU internal market - from France and Germany to Slovakia and Italy. Let us consider the key aspects of this phenomenon. The FIMI concept is built on three key pillars: situational awareness, international cooperation, and strategic communication. The first component involves monitoring the information environment, identifying sources, revealing typical patterns of manipulative campaigns, and conducting impact analysis. In this context, the EEAS Disinformation Kill Chain (The Kill Chain Model of Disinformation, 2023) analytical methodology is actively used (see Fig. 1), which allows tracing the stages of an information attack from its source to the distribution channel.

Figure 1

The Kill Chain Model of Disinformation



Source: The Kill Chain Model of Disinformation, 2023

The second element is institutional and interstate cooperation, since information threats are of a cross-border nature and require a coordinated response at the level of international organizations (EU, NATO, G7, OSCE) and regional initiatives. Within the framework of this cooperation, common codes of practice are being developed (for example, the EU Integrity Code), analytical products are being exchanged, and training is being provided for diplomats and security services.

The third — and perhaps most important — component is strategic communication, which involves not only operational counteraction to fake narratives, but also the formation of sustainable narratives aimed at increasing trust in institutions, developing digital literacy, supporting independent media and promoting democratic values (see Fig. 2). Namely strategic communication allows ensuring not only a reaction, but also a proactive information resilience of societies (EEAS, 2023, February 7).

Figure 2

Self-reinforcing workflow for strategically analyzing incidents of Foreign Information Manipulation and Interference (FIMI) (EEAS, 2023, February 7)

3.3 FIMI concept applications

The application of the FIMI concept is particularly relevant in the context of the current challenges facing Ukraine, in particular, in the context of hybrid aggression by the Russian Federation. The war against Ukraine is unfolding not only on the front, but also in the plane of strategic narratives, where FIMI tools are used systematically: from discrediting the Ukrainian authorities and army to influencing the European audience in order to reduce support for Kyiv (Zakharchenko, 2025).

Thus, the FIMI concept is not just an analytical tool, but a holistic strategic framework that combines security, information, diplomatic, and communication components in the fight for truth, trust, and democratic order. Its implementation requires political will, inter-institutional coordination, and constant adaptation to new forms of disinformation activity. In this context, an important task is not only to respond to information threats, but also to form countering narrative based on the values of an open society, facts, and transparency.

The impact on public order is manifested in three main directions.

3.3.1 Political radicalization in the EU through narratives of "betrayal", "external control", and "institutional breakdown".

Political radicalization in the countries of the European Union in the last decade has taken on new forms, often invisible in traditional analytics. It is no longer limited to extremist groups or marginal parties - radical ideas are increasingly penetrating the mainstream, transforming the rhetoric of official politics, disrupting the balance in parliamentary democracies and affecting public trust. One of the most dangerous catalysts of this process has been systemic information manipulation, in particular - the promotion by external actors of toxic narratives such as "national treason", "loss of sovereignty", and "institutional degradation". Within the framework of the FIMI concept, such destructive information patterns are outlined as a component of hybrid warfare (Mirza, et al., 2021; Mudavadi, & Madrid-Morales, 2024). These are not random fakes, but systemic activities from the outside, the goal of which is to undermine political stability, delegitimize governments, and divide democratic societies.

The narrative of "national treason" is actively promoted both in the intra-European and cross-border media space. In Poland, France, Hungary, Slovakia, and Germany, these messages are used or simulated by external actors (in particular, through pro-Russian media) to discredit pro-Western governments, portray them as "agents of external influence" or even as "collaborators". In the Netherlands, for example, in the context of migration policy, statements are being spread that Brussels "dictates" its will to member states, neglecting national interests. In France, especially after the "yellow vest" movement, the thesis of "elite separation" and the loss of "sovereign control" is being actively propagated (Helclová, 2025). The narrative of "management from outside" is even more deeply rooted in the structure of radical discourses. Its function is to create the illusion that national political processes are no longer independent, but subordinate to "global centers of power" – the European Commission, the US, NATO, or even non-existent conspiratorial entities. This discourse fuels Euroscepticism, pushes for withdrawal from unions (as in the case of Brexit) and justifies radical demands for "national re-foundation". It is important to note that such theses are often legitimized even in discussions of leading political parties, lowering the threshold of tolerance for conspiratorialism (Nagasako, 2020).

The narrative of "institutional decay" serves to undermine trust in courts, parliaments, law enforcement agencies, and independent media. This is particularly dangerous in the context of the spread of populist movements that use the rhetoric of "people against the system". In the context of disinformation campaigns, this manifests itself in claims about the corruption of governments, control of the media by global capital, or the undemocratic nature of EU decisions. In some member states, in particular in Hungary and Bulgaria, this has contributed to the delegitimization not only of specific governments, but also of the very idea of European integration (Musolino, 2021).

Political radicalization against the background of FIMI narratives (Zakharchenko, 2025) is not just an electoral phenomenon, but a structural erosion of democratic trust, which provokes a decrease in voter turnout, an increase in political apathy and mobilization in support of authoritarian decisions. It has concrete consequences: a decrease in the stability of governments, the failure of reforms, the deepening of inter-party confrontation and the strengthening of the influence of third countries in the internal politics of the EU (Horizon Europe, 2022).

Therefore, the spread of toxic narratives, such as "betrayal", "management from outside", and "the breakdown of institutions", is not only an information problem, but a fundamental threat to European democracy. Effectively countering them requires not only technological means (monitoring, fact-checking), but also a deeper strategic approach: the formation of transparent, inclusive institutions, the development of civic education and a new ethics of political discourse. This is what can stop radicalization, which today already calls into question the very idea of European unity.

3.3.2 Mass distrust of the media and the state — what causes the EU legitimacy crisis

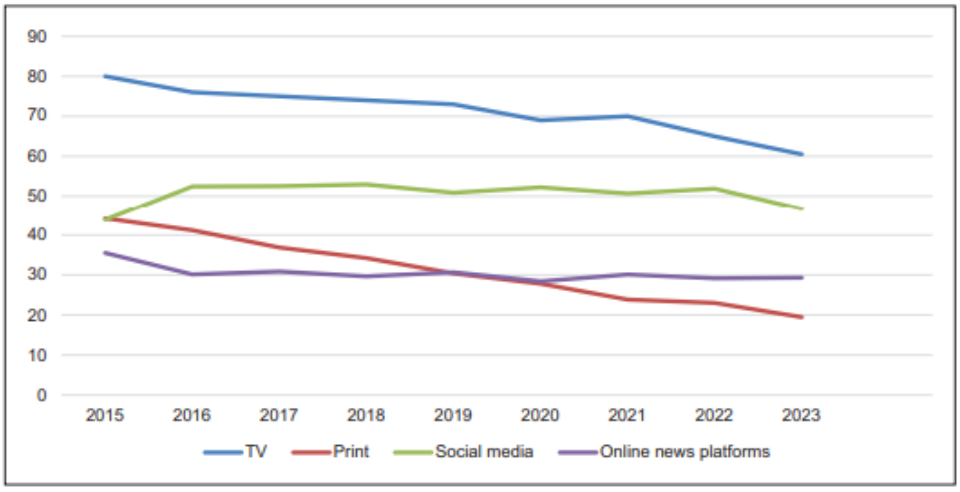
Today, political trust has ceased to be a sustainable asset. Its deficit is increasingly perceived not as an exception, but as a structural feature of a new phase of development of liberal democracy. The European Union, despite its normative potential and system of institutions, is experiencing a deep crisis of legitimacy, which is manifested in the growing distrust of citizens in state institutions and the media. This not only undermines the governability of nation states and the EU as a whole, but also creates a favorable environment for political populism, authoritarian tendencies, and external destabilizing

influences (International IDEA, n.d.)

Systemic fatigue with politics and media. In the early 2000s, trust in EU institutions was relatively high: the European Commission, the European Parliament, and the Court of Justice of the EU were considered the embodiment of legal justice and economic reliability. However, starting with the financial crisis of 2008, and later the migration crisis of 2015, this trust began to decline steadily. The 2023 Eurobarometer study recorded a worrying trend: over 40% of EU citizens do not trust national governments, and over 30% do not trust official European structures (see Fig. 3). This is a direct indicator of a legitimacy deficit (A new Eurobarometer survey reflects opinion and expectations of the EU citizens ahead of the European elections, 2024). The media play a special role in this process. On the one hand, they should act as an intermediary between the authorities and society, and be a platform for public discussion of policies. On the other hand, due to commercialization, political dependence, and the spread of disinformation, the media are increasingly perceived as a tool of manipulation rather than objective information. In many countries of Eastern Europe and the Balkans, the level of trust in the media does not exceed 20–25%. In France, Italy, Greece, and Hungary, this figure fluctuates between 30–35% (see Fig. 4).

Figure 3

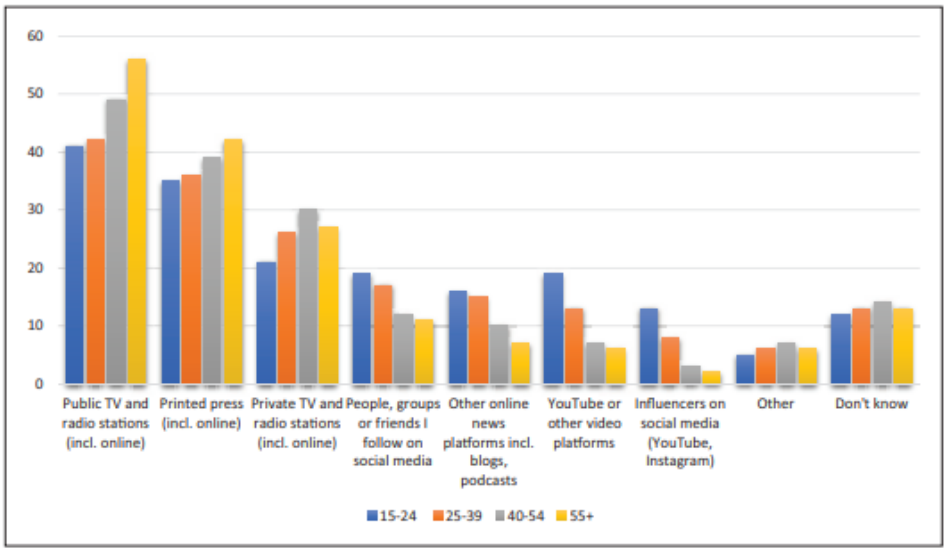
Sources of news in the EU (%)



Source: Fotopoulos, 2023
Note: Data were not available for Cyprus, Estonia, Lithuania, Luxembourg, Latvia, Malta, and Slovenia.

Figure 4

Trust in news source, by age (%) (Fotopoulos, 2023)



Source: Fotopoulos, 2023

Causes of mass distrust. A number of factors contribute to this dynamic. For the average citizen, the European Union often appears as an abstract, "distant" institution that makes decisions without the participation of citizens. The growth of radical movements, populism, FIMI-style information campaigns stimulate the split between "own" and "alien", delegitimizing not only politicians, but also the very structure of political representation. In the digital age, a significant part of the population receives information from uncontrolled sources, where standards of journalistic responsibility are absent. This contributes to the erosion of media trust (Cutajar, 2024, January 22).

Crisis of governance effectiveness. The EU has shown indecision in the fight against COVID-19, migration problems and energy security, which reinforces the perception of the ineffectiveness of the central government.

Impact on the legitimacy of the EU. This complex of factors forms a "crisis triangle": distrust in the media → doubts about the veracity of information → distrust in political decisions → delegitimization of power. The transmission of distrust from national governments to EU institutions is particularly dangerous, since the latter often become responsible for decisions that are made in complex compromise formats. As a result, a paradox arises: despite the growing need for supranational management of global challenges (security, climate, energy), public support for this management is falling. This

threatens to paralyze common policies, destructive fragmentation of the EU, and loss of influence at the global level.

Thus, mass distrust of the media and the state is not only a matter of perception, but a structural threat to the legitimacy of the EU. It requires a comprehensive response: reforming the European communication landscape, institutional openness, strengthening digital media literacy and a new political ethic focused on transparency and engagement. Only in this way can trust be restored both in the media and in the very foundations of the European political project.

3.3.3 Social disintegration of the EU: deepening divisions along linguistic, ethnic, and political lines

The European Union, which historically emerged as a project of integration and overcoming the divisions of the past, is facing a new phenomenon in the 21st century - social disintegration. This is not only a crisis of political solidarity or economic inequality, but above all - the gradual erosion of social unity, which is taking place under the influence of linguistic, ethnic, political, and identity fractures. With each crisis - financial, migration, security, or pandemic - the dividing lines deepen, raising concerns about the EU's ability to maintain internal integrity.

Linguistic and cultural fragmentation. Despite the formal equality of all EU languages, in practice English, French, and German dominate European governance, creating unequal conditions for citizen representation. This creates a linguistic hierarchy, where large member states have the upper hand in decision-making, while countries of Eastern Europe or the Balkans often remain on the periphery of communication. The lack of effective policies for cultural integration and mutual understanding only exacerbates this gap.

Ethnic tension and migration. The 2015 migration crisis catalyzed deep ethno-political polarization in the EU. The governments of Hungary, Poland, the Czech Republic, and later Slovakia and Bulgaria took a hardline anti-migration stance, refusing to accept quotas for migrants. This sparked conflict with EU institutions and the countries of “old Europe,” primarily Germany and France. This geographical-ethnic divide has not disappeared to this day: it affects the distribution of funds, solidarity mechanisms, and

internal security narratives.

Discrimination against ethnic minorities within the EU Roma, Turks, Arabs, Ukrainians creates a shadow zone of exclusion from the civic space. Social integration policies are often declarative in nature and do not change the real situation of marginalized groups.

After Brexit, and against the background of the success of radical movements such as the Rassemblement National in France, the AfD in Germany, or the "Confederation" in Poland, the political landscape of Europe is becoming increasingly fragmented. Political fragmentation is manifested in the conflict between the liberal-globalist and conservative-sovereignist logic of development. The so-called "old" and "new" EU members increasingly come out with incompatible value positions on the rule of law, media freedom, minority rights, and integration depth.

The idea of a common Europe becomes problematic when European institutions have lost the ability to act as an arbiter of political conflict, and instead have become a party to it themselves. Brussels' attempts to punish "unpleasant" states through the mechanism of funding restrictions or sanctions only deepen distrust.

Against the background of the aforementioned divisions, local identities are increasingly strengthened - Catalan, Scottish, Flemish, Corsican. They demand not just cultural autonomy, but political recognition. These trends question the very idea of European citizenship as a supranational unifying mechanism. At the same time, apathy towards identity is spreading among young people: instead of feeling a sense of belonging to the EU, they more often see themselves as citizens of the world or, conversely, only of local communities. This seriously complicates the formation of a European political nation.

The social disintegration of the European Union is therefore not a sudden catastrophe, but a creeping but systemic process. It manifests itself in deepening divisions along linguistic, ethnic, political, and identity lines. If the EU is to remain united and continue the project of democratic integration, it must not only reform its institutions but also create a new social contract that recognizes diversity but upholds common values. Otherwise, instead of a united Europe, we will end up with a politically fragmented mosaic that will lose both internal cohesion and global subjectivity.

In response to these challenges, the European Union is deploying a number of

initiatives within the framework of the FIMI concept:

- the creation of early warning and monitoring mechanisms (EUvsDisinfo, StratCom);
- the adoption of a Code of Practice against Disinformation (2022), which obliges platforms to detect and limit the dissemination of FIMI materials;
- international coordination within the G7, NATO, OSCE;
- strengthening digital literacy and supporting independent media.

At the same time, the scientific and political community recognizes that responding to FIMI cannot be purely defensive. A proactive approach is needed - forming own sustainable narratives, investing in critical thinking, building sustainable institutions that can withstand not only physical but also information attacks. In this context, FIMI is not just a challenge, but a mirror that shows the vulnerabilities of democracies. Resisting FIMI means not only repelling attacks, but also restoring trust, strengthening civil society, and affirming openness and transparency as fundamental values of the European order. The FIMI concept sets a qualitatively new vector for EU security policy. Its implementation allows transforming the fight against disinformation from reactive to systemic, where it is not only about repelling, but also about forming a culture of information resilience as a guarantee of public order and digital security in the European space (Dowse, & Bachmann, 2022).

In this context, the EUvsDisinfo initiative, launched by the European External Action Service, acts as a tool for strategic communications and countering disinformation campaigns aimed at democratic institutions, European unity and security. EUvsDisinfo operates within the East StratCom Task Force (2018), established in 2015 to counter the Kremlin's manipulative influence projects in the information environment. The platform's main mission is to identify, verify, and expose cases of disinformation, as well as to inform the public, journalists, politicians, and educators about the mechanisms and methods of spreading false narratives. Thus, the platform acts not only as an analytical resource, but also as an element of the EU's public diplomacy.

One of the key features of EUvsDisinfo is the creation of a database of disinformation messages, which is systematically updated with examples of fake news detected in the media space in more than 15 European languages. This database allows for the analysis of propaganda strategy patterns, their evolution and target audiences. In

addition, through analytical reports and weekly digests, the platform plays the role of an educational resource that raises awareness of the threats of information terrorism and hybrid aggression.

The institutional support of the initiative by the European Commission and EU Member States demonstrates the recognition of the strategic importance of EUvsDisinfo in shaping a sustainable information environment. At the same time, the platform adheres to the principles of transparency, evidence, and accountability, which allows avoiding accusations of counter-propaganda and strengthens trust in it as a source of objective information.

At the same time, EUvsDisinfo faces a number of challenges, including accusations of restricting freedom of expression and the need to improve the criteria for identifying fake news. Despite this, its activities represent an important example of an institutional response to the global problem of disinformation, demonstrating the potential of democratic mechanisms to protect the truth without violating fundamental freedoms.

In summary, EUvsDisinfo has become more than just a fake news monitoring project, but a systemic truth platform that combines analytics, communication, and education. Its contribution to the formation of digital resilience, media literacy, and public resistance to disinformation attacks is significant both for the European Union and for the global democratic order.

Faced with a wave of external and internal information threats, the European Union has developed a multi-layered strategy to combat disinformation, based on the principles of transparency, human rights, and institutional accountability.

The EU took the first steps towards a systematic counteraction to disinformation in 2015, establishing the East StratCom Task Force to identify, analyze, and expose pro-Kremlin disinformation. In 2018, the Joint Action Plan against Disinformation (European Commission, 2018) and the Code of Good Practice on Disinformation (European Commission, 2022a; European Commission, 2022b)were presented, which envisaged strengthening cooperation between EU institutions, Member States, technology platforms, and civil society. This document identified four main areas: improving the detection of disinformation, strengthening coordination between EU countries, raising awareness among citizens, and putting pressure on online platforms regarding the transparency of algorithms and advertising.

One of the central instruments for implementing the European strategy to counter disinformation was the Code of Practice on Disinformation, adopted in 2018. It was the first regulatory document that laid the foundation for the formation of information security policy in the digital environment. An important feature of the Code is that it was signed by leading technology companies - Meta, Google, Twitter, Mozilla, and others, which demonstrated the willingness of the private sector to join in resolving the problem of the spread of fake content (Proto, Gonzalez, & Garcia, 2025).

The document established the principles of voluntary commitments of online platforms in the field of combating disinformation, in particular: countering the spread of fake news, identifying and restricting the activities of botnets, ensuring transparency of political advertising and facilitating citizens' access to reliable information. Despite its advisory nature, the Code performed several key functions: first, it signaled the willingness of private corporations to cooperate with EU Member States in the field of ensuring information security; secondly, it initiated a new culture of responsibility of digital platforms for the quality and reliability of the content distributed; thirdly, it contributed to the creation of institutional mechanisms for interaction between government structures and civil society.

Thus, the Code of Good Practice has become not only a tool for self-regulation of the digital environment, but also a symbol of the European Union’s transition from fragmented counter-disinformation initiatives to systemic regulation. It marked the beginning of the formation of a multi-layered EU information security architecture, combining institutional, legal, and communication measures with the active participation of the private sector.

The European Digital Media Observatory (EDMO), EUvsDisinfo, the Rapid Alert System network, as well as mechanisms for monitoring online campaigns during elections also play an important role. Such tools provide feedback, analysis of narratives, identification of sources of disinformation and dissemination of analytical products to the public.

The COVID-19 pandemic and the Russian aggression against Ukraine in 2022 demonstrated the evolution of disinformation threats and prompted the need to update approaches. In response, the EU presented the above-mentioned an updated Code of Practice in 2022, which strengthened the obligations of platforms, in particular on bot

labeling, advertising transparency and access to data for researchers. In parallel, digital regulation is actively developing, in particular the Digital Services Act (European Commission, 2022d), which provides for legal liability of platforms for content and allows the European Commission to intervene in the event of the spread of systemic disinformation.

However, the EU strategy is not without its challenges. These include the balance between freedom of expression and information security, jurisdictional issues in the digital space, insufficient resources for independent monitoring, and the risk of politicization of counter-narratives.

In conclusion, the EU strategy to combat disinformation is multifaceted and dynamic, reflecting the recognition of the information space as a critical component of security. By combining legal, institutional, and communication tools, the European Union seeks to ensure the resilience of democracies to manipulation, promote media literacy, and protect citizens' fundamental rights in the digital age. The future of this strategy will depend on its ability to adapt to new technological challenges, enhancing transparency, cooperation, and trust in European society (Liagusha, & Iarovyi, 2025).

The European Union, aware of the hybrid nature of this threat, is implementing a comprehensive legislative policy aimed at creating a sustainable, responsible, and safe digital environment. The EU's legislative initiatives in the field of combating disinformation are based on a combination of legal regulation, self-regulation of digital platforms and support for institutional resilience.

However, the voluntary nature of the Code has proven insufficient in the context of the rapid evolution of threats. In response, an updated version of the Code (Nenadic, Brogi, & Bleyer-Simon, 2023) includes increased platform accountability, algorithm transparency, data access obligations for researchers, combating the financing of disinformation campaigns, and the introduction of indicators to assess the effectiveness of measures. These provisions were legally enshrined for the first time as part of a larger reform of EU digital legislation. The most ambitious step in the field of legislative regulation of disinformation was the adoption of the Digital Services Act (DSA) in 2022 (European Commission, 2022d). This regulatory act establishes the legal liability of large online platforms (VLOPs) (European Commission, 2023a; European Commission, 2023b) for content management, including fakes, manipulation and targeted information

attacks. For the first time in EU history, disinformation has been recognized as a systemic threat, subject to regulation by public authorities and independent oversight.

The DSA obliges digital platforms to assess the risks of disinformation, implement proactive content moderation mechanisms, provide access to data for audits and researchers, and establishes the possibility of imposing fines for non-compliance. Given the influence of external actors – including Russia – on Europe's digital space, the new rules allow the European Commission to respond quickly to threatening information campaigns, including the spread of fake news during elections or crises.

It is also worth noting the adoption of the Digital Markets Act (DMA) (European Commission, 2022c), which, although mainly economic in focus, promotes transparency of algorithms and restrains the monopolization of information influence. Together, these two acts form a new legal architecture of the EU digital space.

The EU's legislative policy on disinformation is closely linked to the concept of the resilience of democracies, as well as the protection of human rights online, in particular freedom of expression. Therefore, the regulation of disinformation is carried out with caution so as not to turn into censorship. All mechanisms should be accompanied by transparent appeal procedures, independent oversight, and the involvement of civil society.

In summary, the EU legislative initiatives demonstrate a balanced approach to countering disinformation, which consists in creating a balanced regulatory system that takes into account both security challenges and the values of freedom. Institutional stability, technological adaptability, and cross-sectoral cooperation remain key prerequisites for the effective implementation of this strategy in the context of hybrid warfare and digital transformation

4 CONCLUSION

To sum up, the EU is implementing a comprehensive approach that combines technological solutions, legislative initiatives, strategic communications, and media literacy to protect public order and security. The EU is actively combating disinformation through the creation of dedicated institutions and strategies. For example, the East StratCom Task Force analyses and exposes fake news, and the Code of Practice on

Disinformation envisages cooperation with technology companies such as Meta, Google, and Twitter to limit the impact of fake news. An important component of the fight is increasing the level of media literacy of citizens and developing independent journalism. Disinformation is a serious threat to the EU, as it destroys public trust, undermines security and contributes to conflicts. To effectively counter it, it is necessary to strengthen information security, develop critical thinking in society, and strengthen international cooperation. Only in this way can the impact of information attacks be minimized and the democratic values of the European Union be protected.

The results of the study demonstrate that the phenomenon of foreign information manipulation and interference (FIMI) poses a complex and systemic threat to the digital security and public order of the European Union. Unlike fragmented disinformation campaigns, FIMI is a targeted, multi-stage form of hybrid aggression that combines manipulative content, cognitive influence and technological means of dissemination, including algorithmic destabilization, botnets and fake news sources. Within the framework of the FIMI concept, key narratives have been identified that provoke political radicalization, mass distrust of the media and authorities, and also increase social fragmentation in the EU. Their spread contributes to the delegitimization of institutions, the erosion of political trust, the growth of support for authoritarian practices and the fragmentation of the European political space.

The European Union, aware of the transnational nature of the threats, has developed a multi-layered strategic response, including institutional, legal, communication, and educational tools. The introduction of initiatives such as EUvsDisinfo, the East StratCom Task Force, the adoption of the Digital Services Act, as well as the development of a Code of Good Practice on Disinformation, demonstrates the transition from a reactive to a proactive security model. The development of strategic communication as the basis of the information resilience of democratic societies is of particular importance. However, the effectiveness of countering FIMI largely depends on the ability to coordinate inter-institutionally, engage civil society, support independent media and promote digital literacy. In this context, the fight against FIMI is not only a security issue, but also a civilizational response to a challenge that threatens the foundations of democratic order, trust, and the rule of law.

Thus, the study allows concluding that FIMI not only changes the nature of threats

in the digital age, but also requires a new approach to shaping EU information security policy, based on the values of an open society, effective regulatory mechanisms, and sustainable narratives that are able to consolidate European societies in conditions of hybrid instability.

AKNOWLEDGEMENT

The research was conducted within the framework of the Jean Monnet Module "EU Counteraction to FIMI" (No. 101172342, ERASMUS-JMO-2024-MODULE).

REFERENCES

[1] *A new Eurobarometer survey reflects opinion and expectations of the EU citizens ahead of the European elections* (2024). PubAffairs Bruxelles. https://www.pubaffairsbruxelles.eu/eu-institution-news/a-new-eurobarometer-survey-reflects-opinion-and-expectations-of-the-eu-citizens-ahead-of-the-european-elections/?utm_source=chatgpt.com

[2] Aguerri, J. C., Santisteban, M., & Miró-Llinares, F. (2024). The fight against disinformation and its consequences: Measuring the impact of "Russia state-affiliated media" on Twitter. *Crime Science, 13*, 17. https://doi.org/10.1186/s40163-024-00215-9

[3] Bryjka, P. (2024). EU Adopts Approach to Countering Foreign Information Manipulation and Interference. The Polish Institute of International Affairs, Policy Paper 3(216).

[4] Cutajar, J. (2024, January 22). From news avoidance to media trust: A European era of doubt. SEC Newgate EU. https://www.secnewgate.eu/from-news-avoidance-to-media-trust-a-european-era-of-doubt/?utm_source=chatgpt.com

[5] Dowse, A., & Bachmann, S. (2022). Information warfare: Methods to counter disinformation. *Defense & Security Analysis, 38*(4), 453-469. https://doi.org/10.1080/14751798.2022.2117285

[6] EEAS (2023, February 7). 1st EEAS report on Foreign Information Manipulation and Interference threats. European External Action Service. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

[7] European Commission (2018). Action plan on disinformation: Commission contribution to the European Council (13–14 December 2018).

https://commission.europa.eu/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en

[8] European Commission (2022a). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

[9] European Commission (2022b). The 2022 Code of Practice on Disinformation. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

[10] European Commission (2022c). The Digital Markets Act. https://digital-markets-act.ec.europa.eu/index_en

[11] European Commission. (2022d). The Digital Services Act. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

[12] European Commission (2023a). A strengthened EU Code of Practice on Disinformation. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_en

[13] European Commission (2023b). DSA: Very large online platforms and search engines. https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops

[14] Fotopoulos, S. (2023). Traditional media versus new media: Between trust and use. *European View*, *22*, 277- 286. https://doi.org/10.1177/17816858231204738

[15] Helclová, A. (2025). How political radicalization speaks: Comparative case study of the Czech SPD party. [MA thesis]. Malmo University, https://www.diva-portal.org/smash/get/diva2:1965296/FULLTEXT01.pdf

[16] Helmus, T. C., & Holynska, K. (2024). *Ukrainian resistance to Russian disinformation: Lessons for future conflict.* RAND Corporation. https://www.rand.org/pubs/research_reports/RRA2771-1.html

[17] Homaniuk, O. (2024). Cybersecurity as a component of international security. *AD ALTA: Journal of Interdisciplinary Research, 14*/02-XLIV, 90–93. https://www.magnanimitas.cz/ADALTA/140244/papers/A_16.pdf

[18] Horizon Europe (2022). Evolution of political extremism and its influence on contemporary social and political dialogue. https://www.horizon-europe.gouv.fr/evolution-political-extremism-and-its-influence-contemporary-social-and-political-dialogue-25511

[19] International IDEA (n.d.). Combating Electoral Foreign Information Manipulation and Interference. https://www.idea.int/project/combating-electoral-foreign-information-manipulation-and-interference

[20] Jackson, N. (2023). The securitisation of foreign disinformation. *Security and Defence Quarterly, 46*(2), 118–138. https://doi.org/10.35467/sdq/190799

[21] Kochar, H. (2025). Examining the threat of digital disinformation to national security in the modern era. *Research Vidyapith International Multidisciplinary Journal, 2*(4). https://doi.org/10.70650/rvimj.2025v2i40011

[22] Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal, 6,* 2024ss0219. https://doi.org/10.31893/multiscience.2024ss0219

[23] Liagusha, A., & Iarovyi, D. (2025). Memes, freedom, and resilience to information disorders: Information warfare between democracies and autocracies. *Social Sciences & Humanities Open, 11*. https://www.sciencedirect.com/science/article/pii/S2590291124004443?via%3Dihub

[24] Menaouer, B., Fairouz, S., & Meriem, M. B. (2025). A sentiment analysis of the Ukraine-Russia War tweets using knowledge graph convolutional networks. *International Journal of Information Technology*. https://doi.org/10.1007/s41870-024-02357-0

[25] Mirza, Sh., Begum, L., Niu, L., Pardo, S., Abouzied, A., Papotti, P., Popper, Ch. (2023). Tactics, Threats & Targets: Modeling Disinformation and its Mitigation. Network and Distributed System Security (NDSS) Symposium 2023, 27 February - 3 March 2023, San Diego, CA, USA. https://dx.doi.org/10.14722/ndss.2023.23657

[26] Mudavadi, K., & Madrid-Morales, D. (2024). Countering political disinformation. In: S. Eldridge, D. Cheruiyot, S. Banjac, J, Swart (eds), *The Routledge Companion to Digital Journalism Studies* (pp. 450-459). Routledge. https://doi.org/10.4324/9781003334774-52

[27] Musolino, S. (2021). *EU policies for preventing violent extremism: A new paradigm for action?*. Barcelona Centre for International Affairs. https://www.cidob.org/en/publications/eu-policies-preventing-violent-extremism-new-paradigm-action

[28] Nagasako, T. (2020). Global disinformation campaigns and legal challenges. *International Cybersecurity Law Review, 1*(1-2), 125-136. https://doi.org/10.1365/s43439-020-00010-7

[29] Nenadic, I., Brogi, E., & Bleyer-Simon, K. (2023). Structural indicators to assess effectiveness of the EU's Code of Practice on Disinformation. European University Institute – Centre for Media Pluralism and Media Freedom (CMPF); European Digital Media Observatory (EDMO). https://cadmus.eui.eu/handle/1814/76101

[30] Okholm, S. C., Fard, A., & Thij, M. (2024). Blocking the information war? Testing the effectiveness of the EU's censorship of Russian state propaganda among

the fringe communities of Western Europe. *Internet Policy Review, 13*(3). https://doi.org/10.14763/2024.3.1788

[31] Pandit, R. (2025). *Information warfare: Battleground of the Digital Age*. Notion Press.

[32] Proto, L., Gonzalez, P., & Garcia, L. (2025). The Great FIMI Pivot: How the EU's Fight Against Disinformation is Being Reframed by the European External Action Service. *Media and Communication, 13,* 9474. https://doi.org/10.17645/mac.9474

[33] Sługocki, W., & Sowa, B. (2021). Disinformation as a threat to national security on the example of the COVID-19 pandemics. *Security and Defence Quarterly, 3*(35), 63-74. http://doi.org/10.35467/sdq/138876

[34] The Kill Chain Model of Disinformation (2023). Fighting Fake News. https://fighting-fake-news.eu/articles/kill-chain-model-disinformation

[35] What is Foreign Information Manipulation and Interference (FIMI) and how does it affect democracy (2025, March 13). CEDEM. https://cedem.org.ua/en/news/fimi/

[36] Xu, W., Sasahara, K., Chu, J., et al. (2025). Social media warfare: Investigating human-bot engagement in English, Japanese and German during the Russo-Ukrainian war on Twitter and Reddit. *EPJ Data Science, 14,* 10. https://doi.org/10.1140/epjds/s13688-025-00528-y

[37] Yuskiv, B., & Karpchuk, N. (2025). External information manipulation and interference: The Russian influence on public opinion on the eve of a full-scale invasion. *Historical and Political Problems of contemporary World, 51*, 59–74. https://doi.org/10.31861/mhpi2025.51.59-74

[38] Yuskiv, B., Karpchuk, N., & Fedoniuk, S. (2024). Model of strategic disinformation reconstruction based on analysis of intentions. *Politologija, 116*(4), 198–237. https://doi.org/10.15388/Polit.2024.116.5

[39] Zakharchenko, A. (2025). Advantages of the connective strategic narrative during the Russian–Ukrainian war. *Frontiers in Political Science, 7*, 1434240. https://doi.org/10.3389/fpos.2025.1434240

[40] Čižik, T. (2017). *Information Warfare - New Security Challenge for Europe.* Centre for European and North Atlantic Affairs (CENAA).

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Shuliak, A., Homaniuk, O., Vozniuk, Y., Borysiuk, O., Kobets, V., & Zeleniuk, H. (2026). FIMI VS DISINFORMATION: IMPACT ON DIGITAL SECURITY AND PUBLIC ORDER IN THE EU. *Veredas Do Direito*, 23(4), e234678. https://doi.org/10.18623/rvd.v23.n4.4678