

Journal Scientific and Applied Research, Vol. 31, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

DISINFORMATION AS A SOCIAL THREAT TO NATIONAL SECURITY (IN THE CONTEXT OF THE RUSSIAN-UKRAINIAN WAR)

Iliana K. Simeonova

Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: i.simeonova@shu.bg

Abstract: *The article examines disinformation as an essential social factor influencing national security in the modern world. In the context of digitalization and rapid dissemination of information, disinformation is becoming a powerful tool for influencing public attitudes, trust in institutions and the stability of the state.*

The article analyzes the main characteristics and mechanisms of disinformation, as well as its social, political and psychological effects. The relationship between disinformation and the processes of public polarization, reducing trust in state institutions and creating a sense of insecurity among citizens is examined.

Special emphasis is placed on the manifestations of disinformation in the context of the Russia-Ukraine war, where information warfare plays a key role alongside traditional military operations. It analyzes how different countries use media and digital platforms to spread propaganda narratives and influence the international and domestic public environment.

Key words: D*isinformation, Information warfare, National security.*

1. Introduction

National security is a complex state of security and resilience of the state, society, institutions and citizens against existing and potential risks and threats. In the traditional understanding of security, the main attention is focused on the military, political and economic dimensions of state protection. However, the development of the information society and digital transformation significantly expand the range of factors capable of influencing national security.

Information has become a strategic resource through which public attitudes, political decisions and patterns of behavior are formed. In the conditions of digital communication, information spreads at an exceptional speed, regardless of national borders and institutional control mechanisms. Social networks provide an opportunity for each user to be both a recipient and a disseminator of information. This transformation has positive effects on freedom of communication, but at the same time creates a favorable environment for the dissemination of false, manipulative and purposefully misleading content.

In this context, disinformation takes on the characteristics of an asymmetric threat. It does not require traditional military resources, but can influence public opinion, trust in institutions, electoral processes and social stability.

The urgency of the problem is reinforced by the use of disinformation in the context of geopolitical confrontation and military conflicts. The Russian aggression against Ukraine demonstrates that information impact can be integrated into a broader system of hybrid tools. The European External Action Service identifies foreign information manipulation and interference (FIMI) as a significant component of the modern security environment, and in its reports it traces systematic campaigns aimed at European societies and supporting Ukraine.

The purpose of this article is to analyze disinformation as a modern threat to national security and to explore the main mechanisms of its impact on society, institutions and democratic processes.

To achieve this goal, the following tasks are set: first, to clarify the essence and specifics of disinformation; secondly, to identify the main sources, methods and techniques of its dissemination; thirdly, to analyze the social, political and economic effects; fourthly, to study disinformation in the context of the Russian-Ukrainian war; and fifthly, to formulate the main directions for countering and increasing public resilience.

2. Nature of disinformation

Disinformation can be defined as the intentional creation, presentation and dissemination of false, misleading or manipulative information with the aim of influencing the perceptions, attitudes or behavior of certain individuals or societal groups.

An essential element of disinformation is the presence of intention. It is this component that distinguishes it from misinformation. In misinformation, false or inaccurate information can be disseminated without the intention to manipulate, while in disinformation, misleading nature is associated with targeted influence. Within the framework of Wardle and Derakhshan, these phenomena are part of a broader "information disorder", which also includes mal-information – the use of real information in a harmful or malicious way.

Propaganda should also be distinguished from disinformation. It is an organised and systematic communication impact aimed at forming certain beliefs and behavioural patterns. Propaganda communication can use both true and false information, while disinformation implies an essential element of misleading.

Therefore, the main characteristics of disinformation can be summarized in several strands: targeting, manipulativeness, use of emotional content, adaptation to specific audiences, rapid dissemination and the ability to reproduce repeatedly in different communication channels.

The main sources of disinformation are diverse, including state and non-state actors, political organizations, media structures, anonymous networks, automated accounts and individual users.

State actors are a particularly significant source when information impact is part of a broader political influence strategy or hybrid activity. In such cases, coordinated networks of information channels, social platforms, media resources and intermediary structures are used.

Social networks such as Facebook, X, and TikTok are changing the traditional model of information intermediation. Algorithmic referral systems can increase the visibility of content that provokes strong emotional reactions, thereby creating conditions for the rapid spread of manipulative messages. The problem is not limited to the existence of social networks alone. The way platforms structure information flows, referral mechanisms, advertising models, automated distribution capabilities, and users' ability to critically evaluate content are essential.

Among the most common techniques are the creation of fake news, the manipulation of context, the use of misleading headlines, the taking of real facts out of context, the manipulation of images and videos, and the creation of fake profiles. The use of bots and trolls is of particular importance. Automated accounts can artificially increase the visibility of a particular message, while coordinated human profiles can create seeming public approval or disapproval.

The development of generative artificial intelligence further complicates the problem. The creation of realistic images, audio and video materials – the so-called. deep fakes – allows the construction of convincing but non-existent events. Thus, the traditional task of "real or fake?" gradually turns into a much more complex process of establishing the origin, context and authenticity of information content.

3. Disinformation as a threat to national security

One of the most significant effects of disinformation is the erosion of public trust. When citizens are systematically confronted with contradictory and manipulative statements, their ability to distinguish between reliable and unreliable information decreases. In the long run, this can lead to distrust not only of individual institutions, but also of the mechanisms of public governance themselves. Research on the so-called. disinformation order highlights the link between the weakening of trust in institutions and the greater vulnerability of society to alternative information sources and manipulative communication strategies. Disinformation can deepen existing societal divisions. Through the use of fear, anger, national, ethnic or political confrontations, it creates conditions for polarization. In crisis situations, this effect can manifest itself in the form of panic, mass anxiety behavior and distrust of official institutions.

The link between disinformation and democratic processes is particularly sensitive. Elections are vulnerable due to the need for citizens to have reliable information in order to form an informed political position. Manipulative information influence can be aimed both at supporting a particular political actor and at demobilising certain groups, discrediting institutions or creating doubts about the legitimacy of the electoral process. The European Commission defines disinformation as a threat to democracy, as it can erode trust in institutions and the media, put elections at risk and make it difficult for citizens to make informed decisions.

The economic impact of disinformation often remains less visible, but can be significant. Manipulative publications can trigger negative expectations, influence investor and consumer behavior, or create doubts about the stability of certain institutions and markets. In times of crisis, the dissemination of false claims about financial institutions, supply, energy or strategic industries can increase economic uncertainty. Economic resilience should therefore be considered as part of a country's overall resilience to information impacts.

4. Disinformation in the context of the Russia-Ukraine war

The Russian-Ukrainian war demonstrates the importance of the information space as an independent dimension of the modern conflict. Hostilities are accompanied by information operations aimed not only at the immediate participants in the conflict, but also at the international community. Information impact aims to influence the interpretation of events, legitimize certain political positions, weaken support for the opposing side and create divisions in societies. The European External Action Service considers FIMI as part of a broader hybrid toolkit and in its 2025 report points to Russia's continued use of information manipulation and interference against Ukraine and its international partners. [ ]

Within the framework of information campaigns, different types of narratives can be observed: questioning the legitimacy of the Ukrainian state and institutions, presenting international support for Ukraine as a threat to other countries, discrediting European and Euro-Atlantic institutions, and using historical, ethnic and cultural themes to polarize public opinion. Particularly characteristic is the adaptation of the same narratives to different national contexts. This shows that modern disinformation does not function solely as one-way propaganda, but as a flexible system of communication impact.

EUvsDisinfo maintains a public database of identified cases of pro-Kremlin disinformation, including content related to the war against Ukraine, NATO and the European Union. The database is updated regularly and is a significant tool for tracking specific information narratives.

The war in Ukraine has shown that disinformation is not limited to the area of immediate military conflict. It can be targeted at the international community in order to change public attitudes about sanctions, military aid, economic relations and political support.

The European Union and NATO are gradually building more systematic mechanisms for identifying, analyzing and countering information manipulation. The European approach includes both monitoring and analysis of campaigns and increasing societal resilience.

5. Social aspects of impact

The effectiveness of disinformation is based not only on the content of the message, but also on its ability to activate emotional reactions. Fear, uncertainty, anger and a sense of threat can reduce the critical assessment of information. A particularly strong impact is observed in crisis situations, when the need for rapid information is high and the possibilities for verification are limited.

The media have a dual role. On the one hand, professional journalism is a major mechanism for verifying and verifying information. On the other hand, the media environment itself can become a conduit for the secondary dissemination of unverified claims. UNESCO emphasizes the importance of media and information literacy, critical thinking, fact-checking and content verification as essential tools to counter information disorder. Therefore, resilience to disinformation cannot be built through technological filters alone. It is necessary to develop the ability of citizens to ask questions about the source, context, evidence and motivation behind an information message.

Vulnerability to disinformation is not the same for all social groups. Older people may experience difficulties in evaluating digital sources and algorithmically generated content. On the other hand, young users are intensive participants in social networks and may be exposed to huge volumes of short and visually oriented content. Therefore, vulnerability should not be associated solely with age. The level of digital and media literacy, political polarisation, trust in institutions and the ability to critically evaluate information are determinative.

6. Measures to counter disinformation

Measures to counter disinformation can be grouped into three groups: in the first group are legislative measures.

Effective counteraction requires a balance between protecting society and guaranteeing freedom of expression. Excessive restriction of information content could create a risk of censorship and restriction of pluralism.

At European level, the Digital Services Act is an important tool, as is the strengthened Code of Practice on Disinformation. In February 2025, the European Commission and the Board for Digital Services support the integration of the Code into the DSA framework as a Code of Practice on Disinformation.

The approach should not be aimed at general content banning, but at transparency, limiting coordinated manipulative behavior, transparency of political advertising, access to data for researchers and increasing the responsibility of platforms.

The second group includes institutional measures. State institutions should build capacity to monitor the information environment, analyze information operations and react quickly to the establishment of coordinated campaigns. When state institutions provide timely, reliable and understandable information, they reduce the information vacuum, which is often filled by unverified content, and inter-institutional interaction between public authorities, security services, academia, media, civil society organizations and technology platforms is also needed.

The third group is educational and societal measures. The long-term countering to disinformation should be based on building societal resilience. Media and information literacy should be developed in the education system. Citizens should have practical skills to verify sources, identify manipulative techniques, recognize false profiles and critically evaluate visual content. In this way, counteraction is transformed from a purely reactive policy into a prevention system based on knowledge, critical thinking and institutional trust.

7. Challenges and future trends in information security

The development of artificial intelligence represents one of the most significant challenges to the future of information security. Generative models allow the creation of highly realistic text, visual and audio content with minimal technical resources.

Deepfake technologies can be used to create false statements of political leaders, manipulated video recordings, or fictitious events. As a result, not only the amount of false information increases, but also the difficulty in establishing authenticity. At the same time, an increase in the automation of information operations is expected. Artificial intelligence can be used to generate multiple variations of a single message, to adapt content to different audiences, and to automate the management of information networks.

This implies the need to develop technological means for detecting synthetic content, systems for tracing the origin of information and mechanisms for rapid verification.

Future countermeasures should be based on the concept of public information resilience. It implies the ability of the state and society to identify information threats, assess their impact, react in a timely manner and restore trust after an information incident occurs.

8. Conclusion

Disinformation is becoming a structural factor of the modern security environment. Its impact goes beyond the boundaries of media communication and affects the resilience of institutions, democratic processes, social trust and economic stability. The main feature of modern disinformation is its ability to use the digital environment for rapid, large-scale and targeted impact. Social networks, automated accounts and generative artificial intelligence further increase the potential for manipulating public opinion. In this context, national security should include not only the protection of physical and digital infrastructure, but also the protection of the **information resilience of society**. Countering disinformation cannot be entrusted to a single institution or implemented solely through legislative restrictions. In the end, the most sustainable defense against disinformation is not absolute control over the information environment, but the **ability of society to recognize manipulation, verify information and make informed** decisions. It is an informed and critically thinking society that represents one of the key elements of national security in the digital information environment.

References

[1] European Parliament and Council. Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).

[2] European Commission. The 2022 Strengthened Code of Practice on Disinformation. Brussels, 2022. The Code is integrated into the DSA framework as a Code of Practice on Disinformation in 2025.

[3] European External Action Service (EEAS). Report on FIMI Threats – March 2026. Brussels, 2026.

[4] European External Action Service (EEAS). 2025 Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI). Brussels, 2026.

[5] European Union. EUvsDisinfo Database. Brussels: European External Action Service.

[6] UNESCO. Journalism, Fake News & Disinformation: Handbook for Journalism Education and Training. Paris: UNESCO, 2018.

[7] Wardle, C., & Derakhshan, H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe, DGI(2017)09. Strasbourg, 2017.

[8] Bennett, W. L., & Livingston, S. (2018). The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions. European Journal of Communication, 33(2), 122–139. DOI: 10.1177/0267323118760317.

[9] Tandoc, E. C., Lim, Z. W., & Ling, R. (2018). Defining “Fake News”: A Typology of Scholarly Definitions. Digital Journalism, 6(2), 137–153.

[10] Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The Science of Fake News. Science, 359(6380), 1094–1096.

[11] Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), 211–236.

[12] Bennett, W. L., & Pfetsch, B. (2018). Rethinking Political Communication in a Time of Disrupted Public Spheres. Journal of Communication, 68(2), 243–253.

[13] Vosoughi, S., Roy, D., & Aral, S. (2018). The Spread of True and False News Online. Science, 359(6380), 1146–1151.

[14] Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and Its Correction: Continued Influence and Successful Debiasing. Psychological Science in the Public Interest, 13(3), 106–131.

[15] EUROPEAN COMMISSION. A Strengthened EU Code of Practice on Disinformation. Brussels: European Commission.