ROMANIA'S SUSCEPTIBILITY TO HYBRID THREATS RELATED TO DISINFORMATION – THE NECESSITY OF DEVELOPING A NATIONAL STRATEGY TO COUNTER FAKE NEWS, ALONG WITH THE REQUISITE FRAMEWORK FOR ITS EFFECTIVE IMPLEMENTATION –

Colonel Constantin-Dorin BĂLAN, PhD
Headquarters Multinational Corps South-East
DOI: 10.55535/RMT.2025.1.04

This paper provides an analysis of the current efforts at both national and international levels to prevent and combat disinformation, with the goal of highlighting Romania's vulnerability to this phenomenon and proposing institutional, coordinated, and unified measures for its effective management.

Following a brief introduction to the contemporary security context, along with a concise overview of the recent evolution of disinformation, the paper proceeds to define and explain the key concepts within this field.

The analysis then examines the international landscape, focusing on the efforts of global organizations to address disinformation, as well as showcasing examples of countries that have successfully implemented institutional measures to tackle this issue.

At national level, the paper evaluates the responses from government institutions, academia, civil society, international organizations, the media, and private sector initiatives dedicated to combating disinformation.

The paper concludes with a set of key findings and recommendations, emphasizing the need for unified action in managing disinformation through the establishment of a national strategy. It further proposes the creation or expansion of dedicated structures to implement this strategy, along with the development of the necessary mechanisms to prevent and counter the analysed phenomenon.

Keywords: fake news; disinformation; hybrid threats; narrative; Russia;

Motto:
"Falsehood flies, while truth comes limping after it".
Jonathan Swift

INTRODUCTION

The Russian Federation's invasion of Ukraine marks a pivotal moment in the early 21st century from both a security and defence perspective, profoundly impacting the geopolitical landscape of the Black Sea region and extending its reverberations globally. Universally recognized as a key event that will shape the geopolitical future for decades, the war in Ukraine continues to captivate international attention due to its polarizing nature and the combination of traditional conflict methods with recent forms of aggression, including non-kinetic operations that can be classified as hybrid warfare.

The Russian Federation's invasion of Ukraine marks a pivotal moment in the early 21st century from both a security and defence perspective, profoundly impacting the geopolitical landscape of the Black Sea region and extending its reverberations globally.

According to various analyses compiled in a 2020 report by the US Department of State, the groundwork for hybrid threats was laid by Russian Federation entities, such as the Main Intelligence Directorate of the Russian Armed Forces (GRU) and the Internet Research Agency (IRA) – a private entity with strong ties to the Russian government – beginning with the invasion of Crimea in 2014. The invasion, preceded by the so-called *"little green men"*[1] operation, was marked by an element of surprise, facilitated by a pre-existing environment heavily influenced by coordinated disinformation campaigns, making it easy to manipulate public perception and gain strategic advantage.

While battlefield disinformation, in various forms, has been employed throughout history, particularly during the global conflicts of the early 20th century and the post-Second World War period, the hybrid operations in Crimea and their continuation during the 2022

[1] The term was initially used by the locals in Crimea to describe Russian soldiers who appeared around Ukrainian military bases prior to the effective annexation of the peninsula. The term was later adopted by the international press and became widely used within NATO after being employed by the NATO Supreme Allied Commander (SACEUR) at the time to describe the ambiguous and subversive nature of these troops in the forceful takeover, with minimal resistance, of Crimea from the moment these troops appeared in February 2014. (A.N.).

invasion of Ukraine represent a significant escalation, heavily heavily supported by advanced technologies. The mentioned development has caught the North Atlantic Alliance off guard, both at the institutional level and within individual member states, which have largely struggled to address the scale of the phenomenon. Many NATO structures dedicated to countering disinformation were, at that moment, either outdated or, in some cases, non-existent.

CONCEPTUAL BOUNDARIES

In the context of hybrid threats, which are considered forms of aggression by nations striving to become global power centres without possessing the necessary economic, social, or military capabilities, the phenomenon of spreading fake news and, by extension, disinformation, is increasingly gaining importance among structures responsible for national security and defence.

In the context of hybrid threats, which are considered forms of aggression by nations striving to become global power centres without possessing the necessary economic, social, or military capabilities (Hybrid CoE, 2023), the phenomenon of spreading fake news and, by extension, disinformation, is increasingly gaining importance among structures responsible for national security and defence. The reasons for this growing focus are varied, but the most significant include the societal risks posed by this phenomenon, such as the erosion of citizens' trust in the state's ability to effectively respond to external aggression, or the detrimental impact that disinformation, in its various forms, has on the management of military operations at the tactical level. An example in this regard is the *"Lisa"* case in Germany, which was replicated in Lithuania during the deployment of a German Battle Group, where German soldiers were falsely accused, through social media posts, of committing sexual assaults during military activities (Schultz, 2017).

From the outset, we aim to address the definition of *fake news*, given the complexity of this term and the various nuances under which it can manifest. This type of content, which is *"neither fully false, nor fully true"* (Bârgăoanu, 2019), is often distorted to such an extent that the technological filters developed to prevent it are rendered ineffective. Thus, to cover the broad spectrum given by the use of both completely false and partially false (or partially true) news, we will continue to use the notion of *fake news* (Bălan, 2023, p. 18), understanding by it that type of news that erroneously describes (intentionally or unintentionally) a fact or phenomenon from everyday reality.

One of the most widely recognized classifications of disinformation identifies three primary categories, with the English language offering greater flexibility in capturing the linguistic nuances associated with this concept. According to Corbu et al. (2021), these categories include *disinformation*, which refers to the intentional dissemination of false information with the intent to mislead. It is followed by *misinformation*, which involves the transmission of incorrect information without a clear intent to deceive. Finally, *malinformation* refers to the presentation of true information that is irrelevant to the public interest, used solely to cause harm or moral damage. An example in this regard is the use of personal information, such as an individual's sexual orientation (Wardle, Derakhshan, 2018), in discussions related to the professional qualifications.

One of the most widely recognized classifications of disinformation identifies three primary categories, with the English language offering greater flexibility in capturing the linguistic nuances associated with this concept: disinformation, misinformation, malinformation.

In the context of combating disinformation, two primary categories of countermeasure efforts can be distinguished. The first is represented by the concept of *prebunking* (Nolan, Kimball, 2021), which involves exposing false narratives before they gain traction (prevention). The second category is *debunking* (Kvetanova et al., 2020), which refers to efforts aimed at countering disinformation after it has spread (response). For both approaches – interventions conducted before or after the dissemination of *fake news* – the key challenge lies in appropriately calibrating the response. An overzealous or premature reaction may inadvertently amplify the spread of false information, counteracting efforts to mitigate the phenomenon.

The latest approaches in the field of Strategic Communication (StratCom) currently focus on identifying comprehensive formulas for analysing and evaluating the information environment (Information Environment Assessment/IEA) seen as an effort that combines highly qualified human resources (*data analysts* – data scientists) and modern technological tools (software for monitoring and automatic analysis of large volumes of data – *data mining, machine learning*).

Additionally, within the StratCom departments of the commands under the NATO Command Structure, a new line of effort is progressively taking shape, specifically focused on securing unanimous agreement among the member states for coining the *cognitive domain* as the sixth operational domain of NATO, alongside *land*, *air*, *maritime*, *cyber* and *space*. The sustained lobbying of Allied StratCom

specialists towards the military and political leadership of the Alliance to obtain the unanimous agreement necessary for this endeavour is also facilitated by the recent completion of the newest concept in the sphere of strategic communication – the *cognitive warfare (CogWar)*, the related document being currently on approval process at the level of the command structures of the North Atlantic Alliance (NATO ACT, 2022).

Currently, within the StratCom community in NATO, there is an ongoing debate about the opportunity to introduce a sixth operational domain – the cognitive domain – alongside the land, air, maritime, cyber, and space domains. To implement this initiative, it is essential to clearly define the concept of *cognitive warfare* (CogWar), with the NATO Allied Command Transformation (NATO ACT) being the structure responsible for overseeing this process (NATO ACT, 2022).

These countermeasures, developed in response to major social crises widely recognized for their significant disinformation component, have evolved in a heterogeneous manner. Each country or international organization has adapted its procedures to suit local specifics and obligations to international organizations.

THE CURRENT INTERNATIONAL SITUATION

An analysis of how states and international organizations address the phenomenon of disinformation must consider the significant impact it has had on national security in various countries, with the illegal annexation of Crimea and the subsequent outbreak of the war in Ukraine serving as the most prominent example. It is also crucial to examine the effects of disinformation on public health, as demonstrated during the COVID-19 pandemic, as well as its influence on political decisions through subversive methods, as seen in the election of Donald Trump as President of the United States of America for his first mandate and the process of the United Kingdom's exit from the European Union (BREXIT).

Currently, following a period of reflection during which government institutions, civil society, the academic community, and the private sector have analysed the phenomenon of disinformation in all its forms, we are at a point where countermeasures are gaining increasing attention. These countermeasures, developed in response to major social crises widely recognized for their significant disinformation component, have evolved in a heterogeneous manner. Each country or international organization has adapted its procedures to suit local specifics and obligations to international organizations. As a result,

coherent approaches have emerged, both legislatively and procedurally, in countries such as the United States of America, France, the United Kingdom, Germany, and the Baltic States. Authorities in these countries have launched extensive projects focused on detecting disinformation and implementing necessary measures – some of which are coercive – to limit its spread.

Regarding *International Organizations*, whether political-military, economic, or those dedicated to maintaining peace and security, they have rapidly developed procedures, norms, rules, and doctrines to facilitate the monitoring of the information landscape and ensure a prompt response, both directly via their own communication channels and through media and social networks. For instance, the United Nations (UN) has initiated a series of activities, including awareness campaigns, collaborations with national authorities, and the development of media education programs. Similarly, the European Union (EU) has not only developed analogous platforms but also issued normative acts designed to serve as a foundation for similar legislative initiatives in member states.

Similarly, disinformation is recognized in NATO's new Strategic Concept as *a tool employed by both state and non-state actors to undermine democracy, institutions, and social cohesion within member countries* (2022, p. 5). In response, the Alliance has proposed the development of capabilities to counter these threats. Consequently, the issue of combating disinformation is addressed at multiple levels within the organization, including the maintenance of an online platform designed to dismantle hostile narratives[2] – *Setting the Record Straight* (NATO, 2024). This initiative is complemented by the dissemination of NATO's own messages across all available channels, including in English, French, and more recently, Russian (with the Russian diaspora as the target audience). These efforts are supported by a series of measures aimed at managing large social networks, with the goal of identifying the most effective *fact-checking* solutions. The objective of these actions is to limit the spread of *fake news* on these platforms as soon as it emerges.

Disinformation is recognized in NATO's new Strategic Concept as a tool employed by both state and non-state actors to undermine democracy, institutions, and social cohesion within member countries. In response, the Alliance has proposed the development of capabilities to counter these threats.

[2] A specific narrative developed to discredit or defame a particular target (NATO's approach to countering disinformation, 2023).

In this context, Ukraine's experience in the information war waged by the Russian Federation since 2014, both directly and through *proxies*[3], is particularly instructive. A study by the RAND Corporation (Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict, 2024) discusses, in the first phase, the measures implemented by Ukrainian authorities prior to the outbreak of war in February 2022. They included the establishment of government and civil society institutions dedicated to combating disinformation and the implementation of preventive actions with the support of the national intelligence community. The same study also highlights a series of actions taken following the Russian invasion, focused on countering hostile narratives disseminated across three distinct areas: within Ukraine, within Russia, and towards the international community. Among the most important lessons learned from Ukraine's experience in the fight against disinformation, the study identifies the need to recognize the new operational theatre created by information warfare, strengthen institutions tasked with combating disinformation, establish common working procedures with civil society, and increase investments in the capabilities offered by such partnerships.

A study by the RAND Corporation discusses, in the first phase, the measures implemented by Ukrainian authorities prior to the outbreak of war in February 2022. They included the establishment of government and civil society institutions dedicated to combating disinformation and the implementation of preventive actions with the support of the national intelligence community.

NATIONAL CONTEXT

At the governmental level, initial steps toward the procedural foundation for combating disinformation began after the adoption of NATO's Strategic Communication Policy (StratCom) in May 2016, followed by the Romanian Armed Forces StratCom concept in October 2017. This effort, led by the Ministry of Foreign Affairs and the Ministry of National Defence, sought to establish a national strategic communication framework to integrate concrete measures for countering disinformation. The discussions were rooted in similar doctrines already implemented within NATO and the Romanian Armed Forces, and were further informed by the expertise of communication specialists from ministries and government agencies responsible for security and defence.

[3] External (third-party) actors or groups used by countries or organizations to achieve their goals without direct involvement (Hybrid CoE, 2023).

The White Paper on Defence (2021) recognizes disinformation as one of the hybrid threats facing Romania, alongside cyberattacks and other forms of non-military aggression. Anticipating the growing scale of this threat, the Ministry of National Defence, through the Information and Public Relations Directorate, launched the *Inforadar* platform in the fall of 2018 to combat *fake news*. This platform is considered a best practice example at both governmental level and within NATO member countries.

Additionally, the Ministry of Foreign Affairs has spearheaded a national initiative to develop a *National Strategic Communication Strategy*, online behaviour guides, and a public reporting mechanism for *fake news* cases, under the aegis of the National Cyber Security Directorate (NCSD). Expert analyses have also been conducted within the Euro-Atlantic Resilience Centre (e-ARC).

In the *academic sector*, several universities and research centres have demonstrated considerable efforts in identifying and addressing disinformation. Communication departments have shown particular interest in this field, carrying out various initiatives aimed at raising awareness of the phenomenon both within the academic community and beyond. These initiatives play a crucial role in theoretically understanding how disinformation spreads in both physical and virtual spaces. They also contribute to disseminating this knowledge among undergraduate, master's, and doctoral students, ensuring that the awareness of disinformation reaches a broader public through its educational and societal roles.

Civil society and non-governmental organizations have also been highly active in combating disinformation and *fake news*, showcasing a high level of expertise and a strong commitment to forming partnerships with governmental institutions. In this context, we can mention *Global Focus*, a non-governmental organisation that focuses on using automated tools to detect *fake news* based on digital footprints in the online environment. Moreover, the *Anti-fake platform*, developed by the *"Eurocomunicare" Organisation,* offers a range of projects centred on media education for both students and journalists.

Last but not least, it is relevant to mention the *New Strategy Centre* think tank, which, through its experts, promotes the importance of disinformation awareness at conferences and high-level meetings.

ROMANIAN MILITARY THINKING

The White Paper on Defence (2021) recognizes disinformation as one of the hybrid threats facing Romania, alongside cyberattacks and other forms of non-military aggression. Anticipating the growing scale of this threat, the Ministry of National Defence, through the Information and Public Relations Directorate, launched the Inforadar platform in the fall of 2018 to combat fake news. This platform is considered a best practice example at both governmental level and within NATO member countries.

This group emphasizes the crucial aspects to consider when devising strategies to combat disinformation.

The Romanian media's approach to combating disinformation and *fake news* is somewhat ambivalent. Some media organizations show genuine concern for countering the phenomenon through partnerships with IT companies to verify information in real-time as well as through the direct collaboration of journalists and the news sources (to verify the accuracy of the information from the source).

On the other hand, some segments of the media prioritize attracting large audiences, often at the expense of rigorous news verification. The focus on sensationalism, event dynamics and strategy to target a large audience are sometimes used to justify bypassing the critical stage of verifying information from multiple sources before releasing it to the public.

The focus on sensationalism, event dynamics and strategy to target a large audience are sometimes used to justify bypassing the critical stage of verifying information from multiple sources before releasing it to the public.

In the *private sector*, companies are increasingly aware of the significant impact disinformation can have, especially regarding reputation management and associated operational and financial risks. Their strategies focus on technical solutions such as early detection of bots and trolls, as well as monitoring online brand reputations to avoid associating with sources generating false information. Public-private partnerships are also promoted, such as multinational brands' affiliation with the European Union Code of Practice against Disinformation (European Union, 2021) and collaboration with the National Directorate for Cybersecurity. Additionally, telecommunications companies are involved in developing media education programs in schools.

IT businesses play a distinct role in tackling the challenges of combating *fake news*, primarily through collaborations with other stakeholders. They include partnerships with the media to implement fact-checking tools, developing cybersecurity solutions to detect troll networks and disinformation propagated through automated processes (e.g., Bitdefender), creating AI-based content verification solutions (e.g., ThinkOut), and preventing cyberattacks aimed at facilitating disinformation spread (e.g., CrowdStrike). These initiatives help shape a diverse landscape of actions dedicated to preventing and combating disinformation in the business sector, contributing added value to national efforts. The emphasis on innovative technologies strengthens these efforts and maximizes the potential advantages they provide.

In conclusion, it is clear that, at the national level, Romania's expertise in combating disinformation and its practical initiatives are comparable, in terms of technological and academic capabilities, to those of countries such as the United States of America, the United Kingdom, France, Germany, and the Baltic States. Media education programs are considered essential for dismantling disinformation from the early stages of education, with several initiatives already working towards integrating critical thinking into school curricula.

Furthermore, numerous *fact-checking initiatives* have been launched in collaboration with public and private institutions that have already implemented and utilized such solutions. At the level of public discourse, there is a clear interest in developing the necessary tools to combat disinformation, recognizing its destructive impact on society and its various segments, as continuously highlighted by the media and online communication channels.

ROMANIAN MILITARY THINKING

Romania's expertise in combating disinformation and its practical initiatives are comparable, in terms of technological and academic capabilities, to those of countries such as the United States of America, the United Kingdom, France, Germany, and the Baltic States.

CONCLUSIONS AND PROPOSALS

Following the emergence of disinformation as it is recognized today, characterized by technological amplification and a strong ideological charge, a period of awareness-raising efforts at all levels of society began. However, resistance to these efforts, managed and funded by both state and non-state actors, was fuelled by the commercial nature of social media algorithms. The mentioned dynamics led to the unnecessary prolongation of the awareness phase, allowing the proliferation of disinformation to be further entrenched and refined, thereby enabling its unchecked spread.

As noted in the previous chapter, international initiatives to combat disinformation have become increasingly numerous and are beginning to yield visible results. Many media institutions and press agencies now verify information before dissemination. At the national level, a diversity of initiatives has emerged. However, a key gap remains – there is a lack of national coordination, both conceptually and materially. These initiatives continue to operate in a fragmented, uncoordinated manner, and could be described as *academic silos* (Donovan, 2020). The concept of *isolated research* is not new; a study conducted under the aegis of the European Union, as early as 2018, recommended the abandonment of isolated research (Independent

High-Level Expert Group on Fake News and Online Disinformation, 2018, p. 27), advocating for the unification of media education programs to integrate all available expertise in civil society, academia, and professional institutions within the EU.

The current geostrategic context and security climate necessitate swift adaptation to ongoing changes, whether they are economic, social, political, or, particularly, security-related. The dynamics observed over the last decade have highlighted the anachronism of structures and concepts based on outdated *status quos*, such as the paradigms that arose from the Cold War and collapsed in the early 1990s.

The recent technological revolution, combined with the exponential expansion of social networks that have become central to interpersonal interactions, has created a highly complex and unpredictable information environment. The sheer abundance of information, facilitated by an increase in information sources, complicates the identification of relevant information, both in the physical and virtual realms.

Moreover, the recent technological revolution, combined with the exponential expansion of social networks that have become central to interpersonal interactions, has created a highly complex and unpredictable *information environment*. The *sheer abundance of information* (Toffler, 1970, p. 350), facilitated by an increase in information sources, complicates the identification of relevant information, both in the physical and virtual realms. In this context, technology, coupled with human expertise in managing large volumes of data, offers a viable solution.

Given the challenges outlined above and the imperative to implement concrete measures to counter disinformation through a unified *national effort*, we propose that the government make a decisive step toward developing a *comprehensive national strategy to combat disinformation*. This *strategy* should integrate the expertise from various sectors of society, aiming to create a holistic understanding of the information environment in Romania, as well as external information that may affect the country through hybrid threats.

To ensure the legal consistency and scope of the proposed s*trategy*, it is essential for it to be adopted as a standalone law or be integrated into a defence-related law through an appropriate legislative amendment. This approach will allow the *strategy* to extend beyond administrative regulations and establish rights and obligations for citizens, such as the right to correct[4] information provided by any content-generating entities, including individuals who transmit

[4] The right to be informed – a fundamental right guaranteed by the Constitution of Romania (2003) through Articles 30 and 31 – refers to the obligation of mass media and public and private institutions to provide accurate information (A.N.).

information to others such as *influencers*, who currently operate in a minimally regulated environment (Khamis, Ang, Welling, 2017). The *strategy* should also define key social relationships, addressing aspects related to civil liability, social protection, criminal law, property law, and commercial relations.

The *strategy* should aim to establish cooperative relationships with public and private institutions, non-governmental organizations, academia, and independent experts, all of whom should be co-opted into a national project dedicated to combating disinformation and other information-related threats. To avoid the duplication of efforts, it is crucial that the *strategy* should efficiently manage available resources and align the objectives of all participating institutions within the project.

Once the unifying concept is consolidated and the necessary human and material resources are assessed, a further essential step would be the creation of a dedicated *structure* to operationalize these concepts, transforming them into concrete norms and procedures for application. This *structure* could be modelled after a directorate and operate under the direct subordination of the Government, ensuring its independence and equidistance from other public activities (ministries or government agencies). Depending on the assessment of specialists and available resources, this *structure* could be integrated into existing bodies managing hybrid threats in Romania and the Euro-Atlantic space, such as the National Cybersecurity Directorate or the Euro-Atlantic Resilience Centre, expanding their responsibilities accordingly.

Ongoing research into the spread of fake news must become a permanent feature of future efforts, given that the technological evolution we are experiencing is still in its early stages. In this regard, it is vital for the academic sector to remain a key partner in this national effort, ensuring continuity in research and staying abreast of new developments in the field.

Ongoing research into the spread of *fake news* must become a permanent feature of future efforts, given that the technological evolution we are experiencing is still in its early stages. In this regard, it is vital for the academic sector to remain a key partner in this *national effort*, ensuring continuity in research and staying abreast of new developments in the field.

While the issue of disinformation is not new, awareness of the phenomenon is now widespread across all levels of society. We observe numerous public speeches, calls for action, and requests from civil society to authorities to address this issue, whose persistence undermines the credibility of government institutions. The long-term

consequences of this erosion of trust are difficult to predict. Therefore, it is critical that authorities should take prompt action to mitigate the phenomenon before it reaches a scale that renders any subsequent prevention or countermeasure efforts ineffective.

BIBLIOGRAPHY:

1. Bălan, C. (2023). *Identificarea, catalogarea și analizarea emoțiilor induse de știrile false în rândul audiențelor, prin utilizarea unor soluții de tip sentiment analysis și data mining* (Doctoral Thesis). București: Școala Națională de Studii Politice și Administrative.
2. Bârgăoanu, A. (2018). *Fake news – Noua cursă a înarmării*. București: Evrika Publishing House.
3. *Carta Albă a Apărării/White Paper on Defence* (2021). Bucureşti: Ministerul Apărării Naționale.
4. *NATO Strategic Concept* (2022). Madrid.
5. *Constituţia României/Constitution of Romania* (2003). Bucureşti: Parlamentul României.
6. Corbu, N., Bârgăoanu A., Durach, F., Udrea G. (2021). *Fake News Going Viral: The Mediating Effect of Negative Emotions*. Media Literacy and Academic Research, vol. 4 (2), p. 61.
7. Donovan, J. (2020). *The breakdown: Joan Donovan on domestic misinformation*. Berkman Klein Center for Internet & Society, https://cyber.harvard.edu/story/2020-12/breakdown-joan-donovan-domestic-misinformation, retrieved on 25 September 2024.
8. European Commission (2018). *Directorate-General for Communications Networks, Content and Technology, A multi-dimensional approach to disinformation* – Report of the Independent High-Level Group on fake news and online disinformation. Publications Office, https://data.europa.eu/doi/10.2759/739290, retrieved on 28 September 2024.
9. Helmus, T.C., Holynska, K. (2024). *Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict*. RAND Corporation, https://www.rand.org/%20pubs/research_reports/RRA2771-1.html, retrieved on 22 November 2024.
10. Hybrid CoE (2023). *COI Hybrid Influence*, https://www.hybridcoe.fi/coi-hybrid-influencing/, retrieved on 28 September 2024.
11. Khamis, S., Ang, L., Welling, R. (2017). *Self-branding, 'micro-celebrity' and the rise of Social Media Influencers*. Celebrity Studies, 8(2), pp. 191-208, https://doi.org/10.1080/19392397.2016.1218292, retrieved on 22 November 2024.
12. Kvetanová, Z., Kačincová, A., Švecová, P., Švecová, M. (2021). *Debunking as a Method of Uncovering Disinformation and Fake News.* In: Višňovský, J., Radošinská, J. (Eds.) (2021). *Fake News Is Bad News – Hoaxes, Half-truths and the Nature of Today's Journalism*, IntechOpen. DOI: 10.5772/intechopen.93738.

13. NATO ACT. *Cognitive Warfare. Protecting the Alliance Against the Threats of Cognitive Warfare* (2023), https://www.act.nato.int/activities/cognitive-warfare/, retrieved on 6 January 2025.
14. NATO (2023). *NATO's approach to countering disinformation*, NATO.int., https://www.nato.int/cps/en/natohq/topics_219728.htm, retrieved on 30 January 2025.
15. NATO (2024). *Setting the Record Straight*. NATO.int., https://www.nato.int/cps/en/natohq/setting-the-record-straight.htm, retrieved on 26 September 2024.
16. Nolan, S.A., Kimball, M. (2021). *What Is Prebunking?* In *Psychology Today*, https://www.psychologytoday.com/us/blog/misinformation-desk/202108/what-is-prebunking, retrieved on 30 January 2025.
17. Schultz, T. (2017). *Lithuania pushes back on fake news*. DW, https://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870, retrieved on 30 January 2025.
18. Toffler, A. (1970). *Future Shock*. New York: Bantam Books.
19. U.S. Department of State (2020). *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*, https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/, retrieved on 30 September 2024.
20. European Union (2021). *Code of Practice on Disinformation*, https://ec.europa.eu/info/publications/code-practices-disinformation_en, retrieved on 25 September 2024.
21. Wardle, C., Derakhshan, H. (2017). *Thinking about 'information disorder': formats of misinformation, disinformation, and mal-information*. Journalism, 'Fake News' & Disinformation, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c, retrieved on 23 September 2024.