ISSN: 2450-6869

eISSN: 2719-6763

No. 20, 2024

DEFENCE SCIENCE REVIEW

http://www.journalssystem.com/pno/

DOI: 10.37055/pno/205780

Original article

Received: 2025-02-13

Revised: 2025-03-16

Accepted: 2025-06-01

Final review: 2025-03-12

Peer review: 2025-02-10

Keywords:

state security, hybrid warfare, information warfare, disinformation, artificial intelligence

Disinformation as a Threat to State Security

Krzysztof Kaczmarek [1,2], A-F

ORCID 0000-0001-8519-1667

Koszalin University of Technology, Poland

Mirosław Karpiuk [3], A-F

ORCID 0000-0001-7012-8999

University of Warmia and Mazury in Olsztyn

Claudio Melchior [4], A-F

ORCID 0000-0002-6124-4717

Università degli Studi di Udine, Włochy

A - Research concept and design B - Collection and/or assembly of data C - Data analysis and interpretation D - Writing the article E - Critical revision of the article F - Final approval of the article

Abstract

Objectives: This article examines the impact of disinformation on state security and explores effective countermeasures within democratic societies. The study analyses the mechanisms of information warfare, the role of artificial intelligence in both the spread and detection of disinformation, and the legal challenges in regulating this phenomenon. The key objective is to determine how to mitigate threats to disinformation while upholding democratic principles of free speech and access to information.

Methods: Research adopts an interdisciplinary approach, integrating political science, legal, sociological, and technological perspectives. It includes a literature review, case studies, and a comparative analysis of disinformation strategies used by state and nonstate actors. Special attention is paid to AI-based tools and cybersecurity frameworks in the countering of disinformation.

Results: Disinformation is a crucial component of modern hybrid warfare, aimed at destabilising democracies and influencing political and security decisions. Traditional fact-checking methods prove to be ineffective, as false narratives often appear more credible than factual information. AI-driven solutions remain experimental, facing challenges in transparency and adaptability. Additionally, legal efforts to combat disinformation often clash with democratic norms, complicating regulatory responses.

Conclusions: State security in the digital age demands evolving countermeasures that integrate technological, legal, and educational initiatives. Raising public awareness and improving media literacy are essential, but balancing security policies with civil liberties remains a challenge. Future research should refine AIdriven detection methods and develop adaptable legal frameworks to address emerging threatstake place independently.

Corresponding author: Krzysztof Kaczmarek Koszalin University of Technology, Faculty of Humanities,Poland, email: puola1972@gmail.com

Introduction

The starting point for the analyses and considerations carried out in this article is the assumption that there is currently an information war that threatens the security of Western states and societies. Therefore, it is important to develop and implement effective methods and tools to counter information attacks. However, to develop effective tools for fighting in information warfare, it is necessary to be widely aware that during war, not only kinetic tools and weapons are used to fight. Psychological warfare and the influence of the opponent without the need to use weapons are also important. One of its tools is disinformation (Derlatka, 2023, p. 226). Currently, the most commonly used, and often the only, way to combat disinformation is to verify facts, identify false information, and authoritatively correct them. However, in the face of ubiquitous disinformation, these actions are not effective and false information is often perceived as more credible than true information. (Rubinelli and Diviani, 2025), because its contents seem rational to some recipients (Dobrowolska, 2024, p. 124).

When developing ways to combat disinformation, it is also important to remember that not all false information is disinformation and can often be misinformation. Misinformation is information that is incomplete, false, or presented in a false context, which misleads the public opinion, which can be created and spread unconsciously by people who do not have the appropriate knowledge on a given topic or those who do not verify the information before further sharing. Disinformation, on the other hand , is the deliberate creation and spread of such information (Kuznetsova *et al*., 2025, p. 5). Therefore, the difference between misinformation and disinformation lies in intentionality. However, from the user's point of view, distinguishing these phenomena is difficult and often impossible, and both can cause threats. Although disinformation is much more dangerous to the security of the state , because it is most often prepared by the state apparatus and teams consisting of specialists in various fields such as psychology, history, mathematics, linguistics, and cultural studies. Therefore, experts should also develop methods and procedures to combat disinformation. It should be taken into account that in a democratic state, citizens should be guaranteed access to information (Włodyka, 2022, p. 352).

Therefore, the main goal of this article is to find an answer to the question of how to effectively counteract disinformation. The effectiveness of the methods used so far to combat this phenomenon will also be examined. The research hypothesis assumes that, in order to ensure the security of the state and its citizens, protection measures against disinformation must evolve continuously, adapt to the dynamically changing information environment, and be effective at the same time. To verify it, the authors decided to use an analysis of the literature on the subject supplemented by an interdisciplinary approach combining political, legal, sociological and technological-IT analysis. Due to the broad scope of the issue, the authors focused on the threats posed by disinformation to Western societies, with particular attention paid to Poland and the European Union in the context of the hybrid activities of the Russian Federation.

1. Disinformation as a Weapon of War: Tools, Targets, and Threats

Disinformation has always been a weapon of war. Its goal is to mislead the enemy, weaken them by creating and deepening social divisions, and present them in a negative light in the eyes of international opinion. The main goals of disinformation activities remain unchanged, and the current development of modern technologies and the universality of access to information and almost unlimited possibilities of its dissemination only mean that new tools appear that can be and are used during disinformation activities. These are often bots and other digital tools based on artificial intelligence (AI) algorithms and big data analysis (Kaczmarek, Karpiuk, Melchior, 2024, p. 104). Due to their specificity, the so-called social networks are most often used as disinformation distribution channels (Marigliano, Ng, Carley, 2024, p. 3).

The current international situation and security environment mean that societies of democratic western countries are most vulnerable to disinformation. This is because disinformation, manipulation, and propaganda cannot be effectively combated in accordance with the law without violating the standards of a democratic state, including freedom of communication (Bayer, 2024, p. 590). Therefore, fighting disinformation is a challenge for the security of the state and its citizens. At the same time, it should be emphasised that currently, in the context of security, the areas of combating disinformation and ensuring cybersecurity largely overlap, and regulations regarding digitisation are increasingly being viewed in terms of state security (Farrand, Carrapico, Turobov, 2024, p. 2382).

Currently, from the perspective of European countries, the greatest threat of disinformation comes from Russia. This applies to former Soviet republics such as Moldova (Nistor, Stretea, 2025, pp. 177-178) or the Baltic states (Morknas, 2022), the countries of the former eastern Bloc (Markowitz, 2023, pp. 294-313), as well as all those on which Russia wants to exert influence. Therefore, preparation for the fight against disinformation requires understanding the importance of information itself for the functioning of modern societies and states.

Information plays a very important role today, and technological and civilisational development increases its importance. The technological revolution has completely changed the methods of social communication, enabling access to increasingly effective communication tools. Along with this development, new forms of threat and new ways of intercepting information appear that are important from the point of view of the functioning of the state and society. This forces public bodies and institutions to search for new solutions in the area of information protection and ways of responding to threats, in order to ensure a high level of security and continuity of the state's functioning (Skwarski, Szkudlarek, 2020, p. 14).

Disinformation has a direct impact on the security of the state and poses a major threat to it. It can affect the state's policy in the field of defence and security, including its strategic goals related to ensuring the independence of the state. Disinformation can interfere with democratic mechanisms, which can undermine state stability and irregularities in the functioning of public authorities. This is an undesirable phenomenon from the point of view of the public interest.

Disinformation is not an end in itself, but a means of achieving a specific, usually long-term, political, or military goal. State security is not Only its duration, but also, if not primarily, its security in the future and in this respect disinformation activities may have particularly harmful effects, which will manifest themselves in the occurrence of crises (Kacaa, 2015, p. 64).

Security, as an institution that is supposed to counteract disinformation, is a state in which states, organisations, social groups, and citizens are properly protected against threats that may harm integrity, prosperity, or survival (Kaczmarek, 2024, p. 412).). Due to the essence of security, its importance for the state and society, a broad interpretation of the threat should be adopted (Karpiuk, 2019, p. 191). Such an approach to the threat allows its elimination even before it causes undesirable effects. One of the threats that destabilise the state may be disinformation, which causes negative effects in the security environment that is supposed to protect systemic institutions.

Disinformation is spread to a large extent in cyberspace. Cyberspace – art. 2 sec. 1b of the Act of 29 August 2002 on martial law and on the competences of the Supreme Commander of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland (i.e., Journal of Laws of 2022, item 2091, as amended) is understood as the space for processing and exchanging information created by ICT systems, together with the connections between them and relations with users. The activity that takes place in cyberspace should be safe. It is important that there are no threats that are significant for users of ICT systems, as well as threats that affect the normal functioning of the state and its institutions (Karpiuk, Melchior, Soler, 2023, p. 8).

The Internet is currently used not only for quick communication, but also for obtaining information or providing services, which is why the protection of its users is very important. The Internet brings with it not only the possibility of quick, easy, and cheap contact, but also threats, including those related to criminal activity (Czuryk, 2022, p. 40). In the era of digital information, the Internet is the main source of access to information for most people around the world. In addition to true and reliable sources, disinformation is also spreading on the Internet, which poses a significant threat to society. It can lead to disorientation, mislead, contribute to the spread of false beliefs, and undermine the democratic electoral process. In response to this challenge, AI has become a promising tool in the fight against disinformation on the Internet (Serwis Rzeczypospolitej Polskiej, 2023) .

Content creation tools based on AI algorithms allow you to significantly accelerate the process of creating false news, graphics, or videos. Additionally, the development of such technology allows for the creation of materials of very high quality (deep fakes), which significantly complicates the distinction between false and true materials (Sobek, 2024, p. 77). This technology is already so advanced and widely available that this type of fake material can only be detected by algorithms that detect errors in digital materials that are imperceptible to humans (Sharma *et al*., 2024, p. 2). At the same time, the development of technology means that digital tools for detecting deep fakes must constantly improve their performance.

Due to the development of disinformation and its presence in strategic areas, it is necessary to act decisively and as quickly as possible in the field of its detection, which will allow one to increase the level of security in all its aspects. For this purpose, it would be necessary to use the development of technology, mainly technology based on AI algorithms and machine learning, to detect disinformation content (Wróblewski, 2024, p. 158).

Many government and nongovernmental, national, and international institutions are attempting to determine the positive and negative impact of AI on societies and to characterise its advantages and disadvantages and its development in specific cybernetic and social directions (Gergelewicz, 2024, p. 83). Public institutions must also focus on using AI to combat disinformation, as well as protecting against its generation of false information, including detecting such information and educating society about such threats. It should be emphasised that AI algorithms can be a significant support in the fight against disinformation, due to the potential they have.

Disinformation activities are also subject to criminal sanctions. Polish lawmakers clearly provide that anyone who, while participating in the activities of a foreign intelligence service or acting on its behalf, conducts disinformation, consisting in the dissemination of false or misleading information, with the aim of causing serious disruptions in the political system or economy of Poland, an allied state or an international organisation of which Poland is a member, or inducing a Polish public authority, an allied state or an international organisation of which Poland is a member, to undertake or refrain from taking specific actions, shall be subject to a penalty of imprisonment for a period of not less than 8 years. Such a sanction is provided for in Article 130 § 9 of the Act of 6 June 1997, the Penal Code (Journal of Laws of 2024, item 17, as amended - hereinafter referred to as the Penal Code).

Intelligence disinformation is also punishable under Article 132 of the Penal Code. According to this provision, anyone who, while providing intelligence services to Poland, misleads a Polish state authority by providing forged or altered documents or other items or by concealing true or providing false information of significant importance to Poland shall be subject to a penalty of imprisonment from one to 10 years. The perpetrator's conduct consists in misleading a Polish state authority by providing forged or altered documents or other items or by concealing true or providing false information of significant importance to the Republic of Poland (Zgoliński, 2023).

The subject of protection provided for in Article 132 of the Penal Code is the security of Poland. To outline a more complete picture of intelligence disinformation, attention should be paid to the concepts used in this provision. Thus, intelligence services are the undertaking of all activities consisting in obtaining, analysing, processing, and transferring information for the benefit of Polish bodies dealing with intelligence. These activities may be paid or unpaid. In turn, misleading means creating a false belief in the actual state of affairs. A Polish state body is any state body that deals with the protection of internal or external security of the Republic of Poland. The transfer (in any form) to a Polish state body of documents with the content indicated in Article 132 of the Penal Code. Other objects are all movable items of significance for the activities of intelligence institutions of the Republic of Poland. Hiding true information should be understood as concealing, making unknown information about the actual state of affairs. Giving false information is the transfer of information inconsistent with reality. A forged document is a document that has been created in order to be recognised as authentic by giving it the appearance of such a document. A forged document is an authentic document in which its content has been changed in an unauthorised manner (Bachnio, 2024) . According to art. 115 § 14 of the Penal Code, a document is any object or other recorded information carrier to which a specific right is associated, or which, due to the content contained therein, constitutes evidence of a right, legal relationship or circumstance of legal significance.

Effectively combating disinformation also requires implementation of solutions at the international level. In the case of the European Union, one of the first concrete actions to combat disinformation was the establishment in 2015, within the structures of the European External Action Service, of a Task Force of East StratCom , whose main task is to build social resilience through the possibility of fact checking information. As part of the implementation of the EUvsDisinfo project , the group also provides a database of information on pro-Kremlin propaganda (EUvsDisinfo, 2023). The European Community also funds projects aimed at developing digital tools to combat disinformation and creating platforms for fact-checking content (European Commission, n.d.).

Current European Union legislation, on the other hand, requires large Internet service providers to introduce procedures to limit the spread of false information. In this context, EU legal acts emphasise limiting content that may be harmful to minors, public health, and public safety (European Union, 2022). Another document is the Code of Practice on Disinformation , which is to be an essential element of the European Commission's set of tools to combat disinformation (Serwis Rzeczypospolitej Polskiej, 2023).

The North Atlantic Treaty Organization (NATO) is also involved in the fight against this phenomenon (Kennedy Trudeau, 2023). However, due to the nature of these activities, detailed information about them is not available, and those that are available only concern social campaigns and the creation of fact-checking platforms.

The fact that disinformation spread via social media can be a complement to kinetic military actions is evidenced by statistics on false and manipulated information that began to appear in the Polish information space several dozen hours before Russia's attack on Ukraine on February 24, 2022. According to the Institute for Internet and Social Media Research, there was excessive publishing activity in the form of phrases interactions: 'Banderites' in a negative context understood as 'they are not people"; "dogs"; "murderers", "child killers"; "UPA" in the context of 'murderers of Poles"; "Ukrainians" in the context of the words 'to murder Poles"; "Ukrainians" in the negative context of "labour market"; "unemployment"of vulgarities in various variations, negatively referring to citizens of Ukraine; 'genocide' in the context of negative historical references regarding Ukraine; contextually expressed support for the actions of the President of Russia; dynamically increasing growth of phrases negating the cohesion of the NATO alliance, humiliating and ridiculing the most important European leaders compared to).

2. Artificial intelligence in the detection of disinformation

The field of artificial intelligence represents a revolutionary force in the realm of information, with a potentially significant impact on both the creation and counteraction of disinformation (Germani, Spitale, Biller- Andorno, 2024). However, the direction of this impact remains uncertain, leaving open the possibility of AI becoming either a devastating instrument of manipulation or a crucial resource for security and truth (Božić, Gregić, 2024, p. 126). Its ability to generate sophisticated content, in conjunction with the increasing accessibility of AI tools, raises questions regarding its potential as both a means of provocation and a means of defence. On the one hand, AI has been shown to amplify the capabilities of those who intend to spread disinformation by creating more credible, personalised, and persuasive false content. On the other hand, it offers innovative tools to combat these same contents, although often with limitations and relevant ethical implications.

When analysing the possibilities of using AI, it should always be taken into account that it is only a tool prone to malfunction, either due to errors made during design and creation or as a result of training on poorly selected databases. Another limitation is that deep learning algorithms are not yet perfect and can only analyse data from a limited area (Zhao, 2025). Currently, work is underway to develop ways to use AI to combat disinformation, but the problem resulting from the lack of transparency in decision making by algorithms has not yet been solved (La Gatta, Sperl, De Cegli, Moscato, 2025). Another problem is that AI algorithms learning on existing data sets are not yet able to quickly and accurately detect constantly emerging new false information that may be an element of disinformation activities (Kuznetsova *et al.*, 2025, p. 15). However, AI is also used as a tool to create disinformation (Cantón-Correa, Montoro-Montarroso, Gómez-Romero, and Molina-Solana, 2025, p. 467). Therefore, it is reasonable to say that there is currently a kind of arms race between those who will carry out disinformation actions and those who want to counteract such actions. The result of this race is the rapid development of digital tools, including the growth of AI capabilities.

The development of digital tools has an impact on all spheres of social, professional, and private activity. Algorithms continuously analyse user activity on the network, and the concept of anonymity is becoming an oxymoron. As a result, societies are exposed to disinformation on an unprecedented scale. The use of deep-fake technology, which involves generating images, sounds, and videos that never actually existed, is already at such a high level that humans are unable to recognise forgery (Zhang, Ni, Nie, 2025). The synergy of prepared audiovisual content and personalised messages increases the risk of negative social phenomena caused by disinformation.

Analysing the literature on the subject, one can conclude that the use of AI to combat disinformation is only at an experimental stage, and the still existing limitations of this digital tool do not allow it to detect disinformation in real time. Another problem is determining the basis to determine what misinformation, disinformation, false news, or truth is. To sum up the analyses of the use of AI in detecting and combating disinformation, it should be noted that it is only a tool that, even with the ability to act autonomously, should be under constant supervision, and its decisions should not be trusted uncritically. At the same time, like any digital tool, artificial intelligence is susceptible to cyberattacks, the greatest threat being those that appear at the design or training stage and are difficult to detect.

However, even though AI algorithms are getting better at analysing text, there are still difficulties in interpreting sarcasm, irony, or controversial discussions, which can lead to false alarms or missing disinformation. As such, the effective use of this tool to combat disinformation is a matter for the future. Especially since the development of technology means that the same tools used to detect disinformation are also used to create it.

Conclusions

The omnipresent information noise makes it very difficult, and sometimes almost impossible, to distinguish false information from true information. Especially in the case of disinformation activities, false information is prepared in such a way that it looks true and credible. At the same time, prepared messages usually present events that are not impossible. It seems that the only way to effectively combat disinformation is to completely block the spread of false information. However, such actions are contrary to the principles of a democratic state of law. Therefore, the greatest challenges related to the fight against disinformation face democratic states in which access to information and freedom of communication are among the basic civil rights (Fatimah, Wiwoho, Isharyanto, 2024, p. 482). In addition, to block false information, it is necessary to determine which is false and which is true, and to determine who and on what basis should do it.

However, the most important conclusion is that disinformation activities threaten the security of the state by changing the perception of reality by societies and their decision-making based on false information and data. This may concern not only voting behaviour, but also support for security and defence policy or international cooperation. When developing strategies to combat disinformation, it is also worth remembering that such activities are often unnoticeable at first, and the achievement of goals is planned only in the distant future.

Referring to the research hypothesis included in the introduction to this article, it can be stated that it has been verified positively because, in an era of rapid technological progress, ensuring the security of the state and its citizens requires, among other things, continuous improvement of methods of combating disinformation. However, effective methods to combat disinformation are currently only theoretical. In practice, complete elimination of the spread of false information can only be achieved by restricting civil rights. Social awareness of the existence of disinformation and the threats resulting from it is also very important. This can be achieved by educating citizens, which, although not always effective, can significantly reduce the level of threat. At the same time, attention should be paid to monitoring the recipients of content who may be radicalised as a result of external influence. Such a control may also seem controversial. However, ensuring the security of the state requires partial restrictions on some freedoms. It should be considered whether freedom of speech or increasing the level of security is more important.

As conclusions and recommendations for future research, it should be assumed that there is currently a war in which the battlefield is, among others, the Internet, and the weapon is disinformation, the tools of which evolve with technological progress. Therefore, when preparing strategies and tools to combat this phenomenon, a polemological approach is advisable.

References

Bachnio, A. (2024). LEX/el., art. 132., in Majewski, J. (ed.) *Kodeks karny. Komentarz* Warszawa: Wolters Kluwer.

Bayer, J. (2024). The European response to Russian disinformation in the context of the war in Ukraine. *Hungarian Journal of Legal Studies*, 64(4), pp. 589-599. https://doi.org/10.1556/2052.2024.00004.

Božić, J., Gregi, M. (2024). Artificial intelligence as a tool in war and a weapon for peace, the power of disinformation. *National Security and the Future*, 25(2), pp. 105-130.

Cantón-Correa, J., Montoro-Montarroso, A., Gómez-Romero, J., Molina-Solana, M. (2025). Perfiles y necesidades formativas de los fact-checkers de la Península Ibérica: impacto de la IA. *Doxa Comunicación*, 40, pp. 465-491. https://doi.org/10.31921/doxacom.n40a2725.

Czuryk, M. (2022). Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues. *Studia Iuridica Lublinensia*, 31(3), pp. 31-43. https://doi.org/10.17951/sil.2022.31.3.31-43.

Derlatka, K. E. (2023). Wielowymiarowość dezinformacji w wojnie – wybrane przykłady stosowania dezinformacji jako narzędzia wojny. *Acta Universitatis Lodziensis. Folia Historica*, 114, pp. 225-240. https://doi.org/10.18778/0208-6050.114.13.

Dobrowolska, J. (2024). Disinformation challenges facing the Three Seas Initiative – frame analysis of the key narratives. *Lithuanian Annual Strategic Review*, 22(1), pp. 123-140. https://doi.org/10.47459/lasr.2024.22.5.

Farrand, B., Carrapico, H., Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs*, 100(6), pp. 2379–2397. https://doi.org/10.1093/ia/iiae231.

Fatimah, S., Wiwoho, J., Isharyanto. (2024). Global perspectives on freedom of expression in environmental governance: Legal implications and challenges. *Jambe Law Journal*, 7(2), pp. 481-507. https://doi.org/10.22437/jlj.7.2.481-507.

Gergelewicz, T. (2024). Bipolarity of Artificial Intelligence – Chances and Threats. *Ius et Securitas*, 2(2), pp. 71-94.

Germani, F., Spitale, G., Biller-Andorno, N. (2024). The dual nature of AI in information dissemination: ethical considerations. *JMIR AI*, 3(1). https://doi.org/10.2196/53505.

Kacała, T. (2015). Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa. *Przegląd Prawa Konstytucyjnego*, 2(24), pp. 49-65. https://doi.org/10.15804/ppk.2015.02.03.

Kaczmarek, K. (2024). Wpływ zmian klimatycznych na bezpieczeństwo. *Journal of Modern Science*, 58(4), pp. 410-430. https://doi.org/10.13166/jms/192195.

Kaczmarek, K., Karpiuk, M., Melchior, C. (2024). A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data. *Prawo i Więź*, 50(3), pp. 103-121. https://doi.org/10.36128/PRIW.VI50.907.

Karpiuk, M. (2019). Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17). *Studia Iuridica Lublinensia*, 28(1), pp. 185-194. https://doi.org/10.17951/sil.2019.28.1.185-194.

Karpiuk, M., Melchior, C., Soler, U. (2023). Cybersecurity Management in the Public Service Sector. *Prawo i Więź*, 4(47), pp. 7-27. https://doi.org/10.36128/PRIW.VI47.751.

Kennedy Trudeau, E. (2023). *Kompleksowe i skoordynowane podejście do strategicznej komunikacji*. NATO Review. Available at: https://www.nato.int/docu/review/pl/articles/2023/03/16/kompleksowe-i-skoordynowane-podejscie-do-strategicznej-komunikacji/index.html.

Kuznetsova, E., Makhortykh, M., Vziatysheva, V., Stolze, M., Baghumyan, A., Urman, A. (2025). In generative AI we trust: Can chatbots effectively verify political information? *Journal of Computational Social Science*, 8(15). https://doi.org/10.1007/s42001-024-00338-8.

La Gatta, V., Sperlì, G., De Cegli, L., Moscato, V. (2025). From single-task to multi-task: Unveiling the dynamics of knowledge transfers in disinformation detection. *Information Sciences*, 696, 121735. https://doi.org/10.1016/j.ins.2024.121735.

Marigliano, R., Ng, L.H.X., Carley, K.M. (2024). Analyzing digital propaganda and conflict rhetoric: a study on Russia's bot-driven campaigns and counter-narratives during the Ukraine crisis. *Social Network Analysis and Mining*, 14(1), 170. https://doi.org/10.1007/s13278-024-01322-w.

Markowitz, S. (2023). Crowddoing and crowdfunding democracy: Innovative strategies for countering foreign disinformation in Central and Eastern Europe. *New Perspectives. Interdisciplinary Journal of Central & East European Politics and International Relations*, 31(4), pp. 294-313. https://doi.org/10.1177/2336825X231206718.

Morkūnas, M. (2022). Russian Disinformation in the Baltics: Does it Really Work?. *Public Integrity*, 25(6), pp. 599-613. https://doi.org/10.1080/10999922.2022.2092976.

Nistor, R. M., Stretea, A. I. (2025). Dismiss, distort, distract, dismay: The civil society in Moldova in the face of disinformation. *Civil Szemle*, 22(1), pp. 177-194. https://doi.org/10.62560/csz.2025.01.11.

Rubinelli, S., Diviani, N. (2025). An argumentation theory-based assessment tool for evaluating disinformation in health-related claims. *Patient Education and Counseling*, 133, 108622. https://doi.org/10.1016/j.pec.2024.108622.

Sharma, S. K., AlEnizi, A., Kumar, M., Alfarraj, O., Alowaidi, M. (2024). Detection of real-time deep fakes and face forgery in video conferencing employing generative adversarial networks. *Heliyon*, 10(17), e37163. https://doi.org/10.1016/j.heliyon.2024.e37163.

Skwarski, A., Szkudlarek, P. (2020). Rola informacji i zagrożenia dezinformacją w systemie bezpieczeństwa państwa. *Studia Administracji i Bezpieczeństwa*, 9, pp. 11-28.

Sobek, J.P. (2024). Treści generowane przez sztuczną inteligencję w kontekście ochrony przed dezinformacją, *Studia Bezpieczeństwa Narodowego*, 33(3), pp. 69-90. http://dx.doi.org/10.37055/sbn/188916.

Włodyka, E. M. (2022). Dostępność cyfrowa w Unii Europejskiej–praktyka i założenia teoretyczne. *Rocznik Integracji Europejskiej*, (16), pp. 349-358. https://doi.org/10.14746/rie.2022.16.21.

Wróblewski, T, (2024). Sztuczna inteligencja jako narzędzie do walki z dezinformacją. *International Journal of Legal Studies*, 17(1), pp. 149-166. https://doi.org/10.5604/01.3001.0054.6967.

Zgoliński, I. (2023). LEX/el., art. 132, in Konarska-Wrzosek, V. (ed.) *Kodeks karny. Komentarz*. Warszawa: Wolters Kluwer.

Zhang, J., Ni, J., Nie, F. (2025). DSM: Domain Shift Modeling for general deepfake detection. *Signal Processing*, 230, 109822. https://doi.org/10.1016/j.sigpro.2024.109822.

Zhao, D. (2025). Cognitive process and information processing model based on deep learning algorithms. *Neural Networks*, 183, 106999. https://doi.org/10.1016/j.neunet.2024.106999.

Other sources

European Commission. (n.d.). *Funded projects in the fight against disinformation*. Available at: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/funded-projects-fight-against-disinformation_en.

European Union (2022). *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). (Text with EEA relevance)*.Available at: https://eurlex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32022R2065#rct_40.

EUvsDisinfo. (2023, 5 lipca). *To challenge Russia's ongoing disinformation campaigns: Eight years of EUvsDisinfo*. Available at: https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-eight-years-of-euvsdisinfo/.

IBIMS (2022). *Komunikat ws. dezinformacji ws. sytuacji na Ukrainie w internecie*. Available at: https://ibims.pl/komunikat-ws-szerzenia-dezinformacji-ws-sytuacji-na-ukrainie-w-polskiej-przestrzeni-internetowej/?fbclid=IwAR0FkgWPHKHxZG2UdKtYN2DTeAsYTbwDZLOwaQ78_ZwZPUC1vBUng4tIl5o.

Serwis Rzeczypospolitej Polskiej (2023). *Kodeks postępowania w zakresie zwalczania dezinformacji otrzymał nowe brzmienie*. Available at: https://www.gov.pl/web/krrit/kodeks-postepowania-w-zakresie-zwalczania-dezinformacji-otrzymal-nowe-brzmienie.

Serwis Rzeczypospolitej Polskiej (2023). *Wykorzystanie sztucznej inteligencji w wykrywaniu dezinformacji w Internecie*. Available at: https://www.gov.pl/web/5g/wykorzystanie-sztucznej-inteligencji-w-wykrywaniu-dezinformacji-w-internecie.