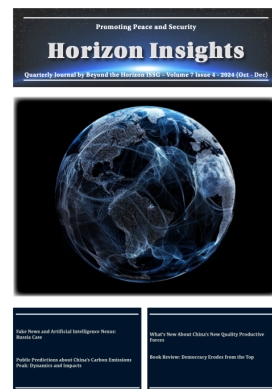




Fake News and Artificial Intelligence Nexus: Russia Case

Georgia Vasileiou



To cite this article:

Vasileiou, G. (2024). Fake news and artificial intelligence nexus: Russia case. Horizon Insights, 7(4), 1–8.
<https://doi.org/10.31175/hi.2024.04.01>

Link to this issue of the journal: <https://doi.org/10.31175/hi.2024.04>

Horizon Insights Journal Homepage: <https://behorizon.org/horizon-insights/>

ISSN: 2593-3582 (printed), 2593-3590 (online)

Submit your article



Fake News and Artificial Intelligence Nexus: Russia Case

by Georgia Vasileiou *

Abstract:

In the era of the digital world and the rapid spread of misinformation, newly implemented technologies have become a critical tool for digital sovereignty. The use of Generative AI and Fake News implications bring new challenges to information dissemination. This paper examines the relationship between Artificial Intelligence (AI) and Foreign Information Manipulation and Interference (FIMI) focusing on their combined impact on information disorder. Furthermore, the article explores a case study about Russian FIMI to illustrate the geopolitical impact of information manipulation, particularly through the use of generative AI, and its potential to reshape modern society.

Introduction:

In the digital era, technologies such as Artificial Intelligence – particularly Generative AI – are transforming how societies share and consume information. While these tools offer great potential, they also enable destructive practices like the large-scale spread of fake news and disinformation. Misinformation campaigns have evolved into coordinated efforts involving both state and non-state actors. Within this context, Foreign Information Manipulation and Interference (FIMI) has emerged, combining disinformation strategies with Artificial Technology (AI) to influence public opinion and undermine democracy.

This paper explores the intersection between Generative AI, Fake news, and FIMI, beginning with a conceptual definition of the terms. It then examines how AI technologies are used to create and disseminate disinformation. A case study on Russian FIMI during the war in Ukraine illustrates these dynamics in practice. The paper concludes by reflecting on AI's broader implications for democratic information ecosystems.

By addressing those aspects, the paper aims to highlight the challenges of AI-based disinformation.

1. Generative AI and Fake News

This chapter introduces key concepts related to AI-driven disinformation, including definitions of Generative AI, Fake News, and Foreign Information Manipulation and Interference (FIMI). It further explores the implications of generative technologies for information dissemination, laying the theoretical foundation for understanding how AI can both enhance and undermine the integrity of public information.

1.1 Generative AI

In today's fast-evolving technological environment, it is crucial to define *Generative Artificial Intelligence* (AI). Generative AI has emerged as one of the most transformative digital technologies of recent years, radically altering how information is created, circulated, and perceived. Its growing influence is not only felt in creative industries and everyday communication, but increasingly in the political and informational domains. In an era where public trust in information is fragile, understanding the mechanisms behind AI-generated content is crucial.

Unlike other forms of AI, which has primarily focused on classification or prediction, generative AI systems are designed to actively create content that resembles human-produced material (Ivanova & European Commission, 2021). These systems are often built on deep learning techniques, particularly transformer-based architectures, and are trained on large-scale datasets. As a result, generative AI can produce coherent text (e.g., through Large Language Models like ChatGPT), generate images from textual input (for example using diffusion models such as DALLÉ), and create synthetic audio, including voice and music. The ease with which believable yet entirely fabricated content can be produced undermines the distinction between real and synthetic, thereby facilitating the spread of disinformation, manipulated media and contributing to the erosion of public trust in digital information environments.

While generative AI provides new means of producing content, its societal impact is shaped by how these tools are employed in the construction and circulation of false or misleading narratives. In the next section, the concepts of Fake News and Foreign Information Manipulation and Interference (FIMI) are explored in order to understand how technological capabilities are transformed into instruments of influence and manipulation.

1.2 Fake News and Foreign Information Manipulation and Interference (FIMI)

Although spreading messages and fake news is not an innovation of the 21st century, the term became more popular during the 2016 US presidential election when a lot of websites published falsified or heavily biased stories (Soetekouw & Angelopoulos, 2022), leading people to question science, true news, and societal norms. Fake news can be defined in a variety of ways, but the simplest definition is the most accurate; it is any news story that contains false information on purpose. Fake news can take many forms and can have many different goals, some harmless, some less so (Young-Brown, 2019). Fake news as a genre is defined by three pillars: low facticity,

* Research Assistant at Beyond the Horizon ISSG

intention to deceive, and presentation in a journalistic format. While the motivation for creating or spreading fake news vary — ranging from humorous, political, economic or ideological — the common denominator is the deliberate attempt to mislead audiences. The rise of fake news can be attributed to several factors, such as the increasing use of disinformation in political discourse, the challenges posed by the Internet and social media to modern democracies, and the rise in popularity of “clickbait” news. Also, digital advertising drives fake news by making it lucrative for publishers to pursue views or clicks in place of correct information. The proliferation of fake news and disinformation online has sown widespread doubt, leaving credible news outlets and legitimate journalism under siege. A recent VRT study found that 1 of 2 now harbors deep scepticism toward real news outlets — transforming healthy doubt into outright distrust (VRT International, 2023), showing how the persistent spread of fake news erodes public confidence in legitimate journalism and undermines the credibility of democratic information systems.

While fake news refers to specific pieces of deliberately fabricated or misleading content, it is only one element, and one tool, within a broader and more systemic phenomenon known as *information manipulation*. Information manipulation extends beyond isolated news stories to encompass coordinated strategies aimed at influencing public opinion, distorting facts, or undermining trust in democratic institutions. It often involves the strategic use of digital technologies, algorithms, and social media platforms not merely to misinform, but to manipulate the very structure of the information environment. According to the European Parliamentary Research Service (2024), information manipulation can be defined as “*using digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations*” — a definition that highlights the methods and tools regimes employ.

Building on this, information manipulation functions as a key tool within Foreign Information Manipulation and Interference (FIMI). While the former refers to the tactical distortion of information, FIMI represents a broader strategic pattern whereby foreign actors coordinate such manipulative practices to undermine societal trust and disrupt democratic processes — often operating in legally ambiguous grey zones below the level of armed conflict. What distinguishes FIMI from more general forms of information manipulation is its foreign origin, strategic intent, and coordination. According to European External Actions Service (EEAS) (2024): “*Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory*”. FIMI is often in combination with cybersecurity and hybrid threats (Yuskiv & Karpchuk, 2024).

The growing sophistication of information manipulation has been accelerated by advances in generative AI. These technologies have transformed the production and spread of information, raising new challenges for trust, authenticity, and democratic resilience. Understanding how Generative AI specifically impact information dissemination is essential and is explored in the next section.

1.3 Implications of Generative AI for Information Dissemination

Generative AI presents significant challenges for information dissemination by enabling the rapid production and spread of fake news. These technologies undermine not only the accuracy of information but also public order. Generative AI as become a common tool in FIMI operations, with the aim to disseminate false or altered content across borders, aiming to manipulate public opinion and destabilize societies. This growing threat has prompted recent European legislative initiatives to safeguard truth in the digital era.

The emergence of large language models (LLMs), such as ChatGPT, has opened new avenues for disinformation by enabling the automated production of realistic and persuasive content (Barman et al., 2024). These capabilities make LLMs appealing tools for malicious actors seeking to manipulate public discourse through synthetic text. As Barman et al. (2024) note, this raises serious ethical concerns about the amplification of disinformation through AI. A particularly advanced application of generative AI is the creation of *deepfakes*—synthetic videos or audio recordings that are often indistinguishable from authentic material. These can be used to impersonate individuals, fabricate events, and disseminate deceptive narratives (Gil et al., 2023; Tahraoui et al., 2023). By compromising identity security and distorting reality, deepfakes pose significant risks to democratic processes and further blur the line between truth and deception.

State-sponsored actors increasingly use AI-driven disinformation campaigns on social media to influence public perceptions regarding elections, legislation, and armed conflicts (Barman et al., 2024). These campaigns can distort public understanding, erode trust in media, and even implant false memories of fabricated events.

The phenomenon of rapid and far-reaching spread of false information has been described as an “infodemic” — a term first used by Rothkopf (2003) during the SARS outbreak and later popularized during the Covid-19 pandemic. According to Yuan et al. (2023), the term refers to the harmful overabundance of false or misleading information, especially in digital environments. The integration of networked, mass, and AI-enhanced communication systems makes combating such falsehoods increasingly urgent.

In the information pandemic era where fake news or deepfakes becoming viral, the boundaries between truth and deception are blurred. This leads us to the next chapter which delves into how AI actively contributes to the creation and spread of information manipulation, exploring the tools and techniques that make these manipulations possible.

2. The Architecture of AI-Driven Information Manipulation

This chapter examines how artificial intelligence is used to create, shape, and disseminate information manipulation in digital environments. After understanding that, we are delving into the tools and techniques used for information manipulation.

2.1. Creation of Information Manipulation through AI

The creation of information manipulation through AI is a multidimensional phenomenon. Manipulation is a concern in many domains, such as social media, advertising, and chatbots (Carroll et al., 2023). In the case of AI systems, they have documented problems with truthfulness. However, manipulation can also be based on truth telling, such as making a true statement that has false implicatures (Carroll et al., 2023).

The information manipulation through AI is not limited only to the creation of Fake News. A typical example is the use of generative AI in the context of FIMI, which is an umbrella term for misinformation, disinformation, malinformation, and other distortions (Bjurling et al., 2024). Digital FIMI can consist of many different data types, either alone or in combination, and while at present generative AI models perform best concerning text output, the steady increase in performance that is observed for other data types makes it highly likely that generative AI will eventually dominate or completely replace conventional methods for FIMI distortions (Bjurling et al., 2024).

To better understand how AI functions in this space, Bergh (n.d.) introduces the concept of the “three C’s”: content, cognition, and competition. Content refers to the digitized information itself — often AI-generated — and forms the visible layer of manipulation. Cognition involves the way individuals process, interpret, and respond to this information, with AI systems designed to exploit cognitive biases and shape perception. Finally, competition reflects the strategic dimension of information manipulation, especially in the geopolitical context where information has become a tool of influence and contestation (Bergh, n.d.).

Together, these dimensions show how AI transforms information manipulation from isolated incidents to systemic interference. Understanding this evolution is crucial for analyzing the specific techniques and technologies used in AI-driven disinformation, as explored in the next section.

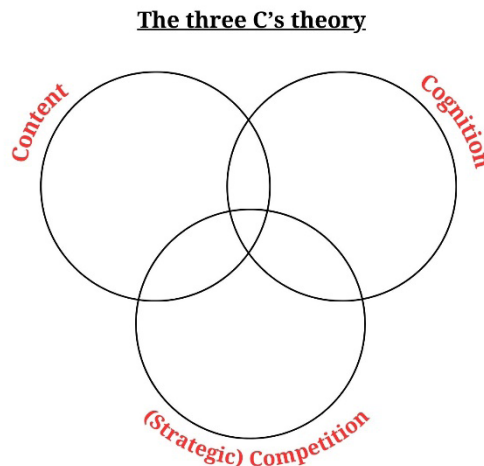


Figure 1: The three C's theory (Bergh)

Understanding how AI shapes the creation of manipulated content lays the groundwork for a closer look at the concrete tools and techniques that operationalize these strategies in practice.

2.2. Tools and Techniques of Information Manipulation

As mentioned before, information creation through Artificial Intelligence is multidimensional, particularly regarding the tools and techniques used to manipulate it. In general, disinformation is often employed as a political weapon by governments or organizations to advance agendas or discredit adversaries (Kachelmann et al., 2023), especially in digital spaces. While generative AI holds potential for societal benefit, it can also be exploited for harmful purposes (Bjurling et al., 2024).

The digital world consists of hardware, software, networks, infrastructures, and most importantly data (Rodilos-

so, 2024), which means free access to personal information. That can lead to privacy issues, filter bubbles, and the spread of misinformation. Several social media platforms have been accused of using algorithms to manipulate what content users see in their feeds, to promote certain political or commercial interests (Ienca, 2023). Particular techniques can lead to biased opinions or misinformation to manipulate the public.

Filter bubbles emerge from algorithm-driven curation processes that tailor content to user-specific profiles, driven by Recommender Systems (RSs) and Machine Learning Algorithms (MLAs), which predict preferences based on behavioural data (Rodilloso, 2024; Ienca, 2023). Such algorithmic filtering fosters personalized echo chambers. Machine-generated content has long been tied to threats such as phishing and disinformation, largely due to the ability of Large Language Models (LLMs) to generate human-like, easily accessible, and personalized content (Yang et al., 2023).

AI-powered bots and fake accounts have significantly influenced Online Social Networks (OSNs), particularly during high-impact events like elections, healthcare crises, and market disruptions (Akhtar et al., 2024). These accounts coordinate manipulation efforts and disinformation campaigns. Trolls – often non-professionals – contribute by spreading provocative, emotionally charged content such as manipulated racist or sexist material, further fuelling division (Masood et al., 2021). Hyper-partisan media, including fake news sites and blogs, serve as major sources of disinformation (Masood et al., 2021). Generative AI enables these actors to rapidly produce false content aimed at increasing reach and engagement. Political parties, leveraging their online influence, also participate in spreading misinformation to large audiences (Masood et al., 2021).

Beyond individuals and organizations, foreign governments use these techniques to shape international opinion and undermine other nations. Countries such as China, Israel, Türkiye, Russia, the UK, Ukraine, India, and North Korea are believed to run state-sponsored accounts, websites, and apps that employ “digital footsoldiers” to smear opponents and disseminate false narratives (Masood et al., 2021). With digital monitoring and manipulation now widely available, private actors may also engage in cross-border information attacks (Masood et al., 2021).

The internet has become a “global village” where technological tools are deployed as political weapons in the struggle for digital sovereignty. This section has outlined the main mechanisms of information manipulation. The last third and last chapter explores a case study of Russian FIMI with a focus on its role in the war in Ukraine.

3. Case Study of Russian FIMI

3.1 Introduction:

Russia offers a particularly illustrative case of Foreign Information Manipulation and Interference (FIMI), where information operations are not peripheral but central to the state's geopolitical strategy. In the context of the war in Ukraine, FIMI has been institutionalized as a tool to justify aggression and destabilize opposition, increasingly enhanced by the use of generative AI.

Closely linked to cyber operations and hybrid threats, FIMI has become a central tactic in the geopolitical strategies of authoritarian regimes (Yuskiv & Karpchuk, 2024). The integration of AI technologies further augments these efforts by increasing the speed, reach, and precision of disinformation campaigns. Public statements by Russian authorities, including President Putin, suggest that one of the lessons Russia has been learning is that AI-enabled weapons systems and infrastructure provide clear battlefield advantages (Zysk, 2024).

This chapter examines how Russia combines FIMI and AI to pursue strategic objectives, with a focus on the war in Ukraine.

3.2 Definition of the Case Study

To define and contextualize the case, it is important to note that Russian armed aggression against Ukraine began in 2014 and was multidimensional from the outset (State Service of Special Communications and Information Protection of Ukraine, 2023). Russia has since employed hybrid tactics such as economic warfare and propaganda to advance its objectives. The full-scale invasion of Ukraine commenced on 24 February 2022.

Russia's interest in artificial intelligence dates back to the early 2010s. In 2018, President Vladimir Putin, acknowledged the importance of AI, claiming that “whoever becomes the leader in this field will rule the world” (Hunter, et al., 2023). AI has also been instrumental in Russia's information manipulation efforts. For decades, Ukraine's information sphere has been vulnerable to Russian propaganda (Yuskiv & Karpchuk, 2024). In the lead-up to the 2022 invasion, the Kremlin disseminated narratives portraying Ukraine and its allies in hostile terms, including false claims of genocide against Russian-speaking Ukrainians and accusations of Nazi ideology among Ukraine's leadership (Virtosu & Goian, 2023).

Information warfare has become increasingly sophisticated, merging traditional military strategy with digital influence operations (Savaryn, 2023; Tsozniashvili, 2024). Russia's approach aims to sow societal divisions, erode democratic institutions, and garner support for its imperial agenda (Virtosu & Goian, 2023).

The pillars of Russia's disinformation strategy include strategic distortion of facts for political purposes, emotional manipulation of public sentiment, distraction from domestic or geopolitical actions, and the deployment of media control, cyber-attacks, and coordinated bot and troll activity (Virtosu & Goian, 2023).

Since the escalation in 2022, Ukraine has implemented various countermeasures, such as establishing fact-check-

ing networks, expanding media literacy initiatives, and developing a national policy against disinformation (Savaryn, 2023).

3.3 Key Examples and Analysis

After the Russian full-scale invasion of Ukraine, more attention has been drawn to how FIMI has been used as a strategic and coordinated policy and tool in the preparation and execution of the military aggression against Ukraine (EEAS, 2024). In disinformation campaigns, AI is already used to disseminate false content (Islas-Carmona et al., 2024), because AI provides possibilities on automated creating and distribution of manipulation campaigns with better personalization and targeting (Chyzhova, 2024).

Combining fake information and AI, especially through social media is a common strategy for Russia. Telegram played a vital role in the Russian-Ukrainian war. It is well-known that Telegram channels use AI to disinform users. There are also cases of using deepfakes in Russian manipulative campaigns since the start of the full-scale war, portraying for example President V. Zelenskyy or the Commander-in-Chief of the Armed Forces General V. Zaluzhnyy, calling the Ukrainians to give in (Chyzhova, 2024). Although there are no borders in the case of misinformation. For example, in 2023, the analysts of the Center for Countering Disinformation unveiled a network of YouTube channels in Africa with completely AI-generated content, promoting Russian narratives by fake journalists (Chyzhova, 2024).

Another example of Russian FIMI is the campaign named “DoppelGänger”, operated by the Russian Social Design Agency and Structura National Technologies. “DoppelGänger” promotes pro-Russian narratives and infiltrates Europe’s media landscape by disseminating disinformation through a network of cloned websites, fake articles, and social media manipulation (U.S. Cyber Command, 2024). This campaign was denounced by the French government and employed generative AI to create disinformation content and purchased domain names similar to legitimate media to mimic news outlets, governments, and think tanks, luring unsuspecting readers into a maze of falsehoods (U.S. Cyber Command, 2024; Islas-Carmona et al., 2024). That campaign uses social media bots to spread its pro-Russian narratives with a multi-stage website obfuscation to mask links between the bots and in-authentic sources (U.S. Cyber Command, 2024). Those narratives include portrays of Ukraine as a failed, corrupt, and Nazi state. Also, it denies the Bucha massacre and spreads Kremlin-approved narratives on the Ukraine war (U.S. Cyber Command, 2024).

Those examples have highlighted that the harm of FIMI activities goes beyond the impact on democracy and society — it can also be used as an instrument of war. In that case, Russia is not using FIMI as a sporadic opportunity to interfere but as a strategic instrument of its foreign policy, with the help of AI. In general, the invasion is the culmination of Russia’s years-long propaganda campaign and involvement aimed at undermining Ukraine’s sovereignty and territorial integrity.

Conclusion:

This article aimed to emphasize how AI-driven FIMI has a significant impact on modern societies. The rise of identity-based disinformation within the broader context of information manipulation and interference by foreign actors who exploit deep societal fractures should be highlighted as a serious threat. Through the Case Study of Russian FIMI, it is clear that the disinformation campaigns have increased the scope and scale of manipulation, posing serious problems for information integrity and international stability. The disinformation campaigns have showcased the two-sided nature of AI, that is how AI might be a useful asset for humanity but equally has the potential to inflict great damage.

The findings of this research indicate that there are several challenges raised by AI-driven information manipulation and this calls for a comprehensive response. There is a need for international collaboration for creation of a strong fact-checking system promoting media literacy. The objective of the paper was to draw attention to the need to raise awareness of FIMI risks and threats while leveraging the potential of AI for the development of a more open and self-directed digital space.

This underlines the mutual responsibilities of governments, tech companies, and civil society to combat the misuse of Generative AI in the information environment.

References:

- Akhtar, M. M., Masood, R., Ikram, M., & Kanhere, S. S. (2024, July). SoK: False Information, Bots and Malicious Campaigns: Demystifying Elements of Social Media Manipulations. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security* (pp. 1784-1800). <https://arxiv.org/pdf/2308.12497>
- Allegri, M. R. (2024). The impact of disinformation on the functioning of the rule of law and democratic processes in the EU. *Interdisciplinary Journal of Research and Development*, 11(1 S1), 98. <https://doi.org/10.56345/ijrdv11n1s116>
- Au, A. (2023, October 20). China vs US Approaches to AI Governance. *The Diplomat*. <https://thediplomat.com/2023/10/china-vs-us-approaches-to-ai-governance/>
- Barman, D., Guo, Z., & Conlan, O. (2024). The Dark Side of Language Models: Exploring the potential of LLMs in multimedia disinformation generation and dissemination. *Machine Learning With Applications*, 16, 100545. <https://doi.org/10.1016/j.mlwa.2024.100545>
- Battista, D. (2024). Political communication in the age of artificial intelligence: an overview of deepfakes and their implications. *Society Register*, 8(2), 7–24. <https://doi.org/10.14746/sr.2024.8.2.01> [pdf]
- Bendett, S., Boulègue, M., Connolly, R., Konaev, M., Podvig, P., Zysk, K., & Chatham House, the Royal Institute of International Affairs. (2021). Advanced military technology in Russia: Capabilities and implications. In Chatham House. <https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-23-advanced-military-technology-in-russia-bendett-et-al.pdf>
- Bergh, A. (n.d.). Being there: content, cognition, and strategic competition. In STO-MP-HFM-361 (pp. P14–P14). [pdf].
- Bjurling, B., Thore, A., & Riad, S. (2024). Foreign Information Manipulation & Interference: A Large Language Model Perspective. <https://www.diva-portal.org/smash/get/diva2:1844832/FULLTEXT01.pdf>
- Carroll, M., Chan, A., Ashton, H., & Krueger, D. (2023). Characterizing manipulation from AI systems. In *Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO '23)*, October 30–November 01, 2023, Boston, MA, USA. ACM, New York, NY, USA, 13 pages. <https://doi.org/10.1145/3617694.3623226>
- Chyzhova, O. (2024, October 8). FIMI as part of Russian war machine: Ukraine's fight - Prism Ua. Prism Ua. <https://prismua.org/en/english-fimi-as-part-of-russian-war-machine-ukraines-fight/>
- Egelhofer, J. L., & Lecheler, S. (2019). Fake news as a two-dimensional phenomenon: a framework and research agenda. *Annals of the International Communication Association*, 43(2), 97–116. <https://doi.org/10.1080/23808985.2019.1602782>
- Elbashir, M. (2024, April 22). EU AI Act sets the stage for global AI governance: Implications for US companies and policymakers. Atlantic Council. <https://www.atlanticcouncil.org/blogs/geotech-cues/eu-ai-act-sets-the-stage-for-global-ai-governance-implications-for-us-companies-and-policymakers/>
- European External Action Service (EEAS). (2024). *2nd EEAS report on foreign information manipulation and interference threats: A framework for networked defence*. <https://eeas.europa.eu>
- European Parliament and the Council of European Union. (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. In *Official Journal of the European Union [Legislative acts]*. [pdf]
- European Parliamentary Research Service. (2024, April). *Online information manipulation and information integrity* (EPRS Briefing No. 762.416). [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI\(2024\)762416_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI(2024)762416_EN.pdf)
- Feldstein, S. (2023). Evaluating Europe's push to enact AI regulations: how will this influence global norms? *Democratization*, 31(5), 1049–1066. <https://doi.org/10.1080/13510347.2023.2196068>
- Gil, R., Virgili-Gomà, J., López-Gil, J., & García, R. (2023). Deepfakes: evolution and trends. *Soft Computing*, 27(16), 11295–11318. <https://doi.org/10.1007/s00500-023-08605-y>
- Gupta, S., Modgil, S., Lee, C. K., & Sivarajah, U. (2023). The future is yesterday: Use of AI-driven facial recognition to enhance value in the travel and tourism industry. *Information Systems Frontiers*, 25(3), 1179–1195. <https://link.springer.com/article/10.1007/s10796-022-10271-8#citeas>
- Hinds, J., Williams, E. J., & Joinson, A. N. (2020). “It wouldn't happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, 143, 102498. <https://www.sciencedirect.com/science/article/abs/pii/S1071581920301002>
- <https://www.cirsd.org/files/000/000/010/82/21e461a985f43655b1731b3c1b50cdcb631afaf.pdf>
- Hunter, L. Y., Albert, C. D., Henningan, C., & Rutland, J. (2023). The military application of artificial intelligence technology in the United States, China, and Russia and the implications for global security. *Defense & Security Analysis*, 39(2), 207–232. [pdf]

- Ienca, M. (2023). On artificial intelligence and manipulation. *Topoi*, 42(3), 833–842. <https://doi.org/10.1007/s11245-023-09940-3v>
- infodemic. (2024). <https://dictionary.cambridge.org/dictionary/english/infodemic>
- Islas-Carmona, J. O., Gutiérrez-Cortés, F. I., & Arribas-Urrutia, A. (2024). Disinformation and political propaganda: An exploration of the risks of artificial intelligence. *Explorations in Media Ecology*, 23(2), 105–120. https://doi.org/10.1386/eme_00199_1
- Ivanova, Y. & European Commission. (2021). Generative AI and the AI Act. <https://www.europarl.europa.eu/cms-data/277774/02.Yordankalvanova.pdf>
- Kachelmann, M., Reiners, W., Managing Global Governance, & German Institute of Development and Sustainability. (2023). The European Union's governance approach to tackling disinformation. In *L'Europe En Formation* (Issue no 396). <https://shs.cairn.info/journal-l-europe-en-formation-2023-1-page-11?lang=en#s1n2>
- Kuznetsova, E., Makhortykh, M., Vziatyshva, V., Stolze, M., Baghumyan, A., & Urman, A. (2023). In Generative AI we Trust: Can Chatbots Effectively Verify Political Information?. arXiv preprint arXiv:2312.13096. <https://arxiv.org/pdf/2312.13096>
- Lowry, A. (2020). Russia's Digital Economy Program: an effective strategy for digital transformation? In Springer eBooks (pp. 53–75). https://doi.org/10.1007/978-3-030-42855-6_4
- Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., Department of Computer Science, University of Engineering and Technology-Taxila, Pakistan, Department of Computer Science and Engineering, Oakland University, Rochester, MI, USA, & Electrical and Computer Engineering Department, University of Michigan-Dearborn, MI, USA. (2021). Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward. In Department of Computer Science, University of Engineering and Technology-Taxila, Pakistan [Journal-article]. <https://arxiv.org/pdf/2103.00484>
- Olan, F., Jayawickrama, U., Arakpogun, E. O., Suklan, J., & Liu, S. (2022). Fake news on Social Media: The Impact on Society. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-022-10242-z>
- Osasona, N. F., Amoo, N. O. O., Atadoga, N. A., Abrahams, N. T. O., Farayola, N. O. A., & Ayinla, N. B. S. (2024). REVIEWING THE ETHICAL IMPLICATIONS OF AI IN DECISION MAKING PROCESSES. *International Journal of Management & Entrepreneurship Research*, 6(2), 322–335. <https://doi.org/10.51594/ijmer.v6i2.773>
- Reisach, U. (2021). The responsibility of social media in times of societal and political manipulation. *European journal of operational research*, 291(3), 906–917. <https://doi.org/10.1016/j.ejor.2020.09.020>
- Rodillosso, E. (2024). Filter Bubbles and the Unfeeling: How AI for Social Media can Foster extremism and Polarization. *Philosophy & Technology*, 37(2). <https://doi.org/10.1007/s13347-024-00758-4>
- Rothkopf, D. J. (2003, May 11). When the Buzz Bites Back. *The Washington Post*. <https://www.washingtonpost.com/archive/opinions/2003/05/11/when-the-buzz-bites-back/bc8cd84f-cab6-4648-bf58-0277261af6cd/>
- Savaryn, H. (2023). Warfare & Social Media: Disinformation and Propaganda in the Digital age. In Central European University, Central European University. [pdf]
- Saxon, D. (2024). Military AI and accountability of individuals and states for war crimes in the Ukraine. In *Chapman and Hall/CRC eBooks* (pp. 169–191). <https://doi.org/10.1201/9781003410379-11>
- Sheehan, M. (2023). China's AI regulations and how they get made [Journal article].
- Siau, K., & Wang, W. (2020). Artificial intelligence (AI) ethics: ethics of AI and ethical AI. *Journal of Database Management (JDM)*, 31(2), 74–87. https://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=1356&context=bio_inftec_facwork
- Soetekouw, L., & Angelopoulos, S. (2022). Digital resilience through training protocols: Learning to identify fake news on social media. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-021-10240-7>
- State Service of Special Communications and Information Protection of Ukraine. (2023.). *Cyberattacks, artillery, propaganda: An overview of the dimensions of Russian aggression*. Retrieved from <https://cip.gov.ua/en/news/kib-erataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi>
- Szczepański, M. (2024). United States approach to artificial intelligence. [https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA\(2024\)757605_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf)
- Tahraoui, M., Krätzer, C., & Dittmann, J. (2023). Defending Informational Sovereignty by Detecting Deepfakes: Risks and Opportunities of an AI-Based Detector for Deepfake-Based Disinformation and Illegal Activities. In B. Herlo, & D. Irrgang (Eds.), *Proceedings of the Weizenbaum Conference 2022: Practicing Sovereignty - Interventions for Open Digital Futures* (pp. 142–161). Berlin: Weizenbaum Institute for the Networked Society - The German Internet Institute. <https://doi.org/10.34669/wi.cp/4.14>
- Tsotniashvili, Z. (2024). Silicon Tactics: Unravelling the Role of Artificial Intelligence in the Information Batt lefield of the Ukraine Conflict. *Asian Journal of Research*, 9(1-3), 54–65. [pdf]

- U.S. Cyber Command. (2024). Russian disinformation campaign “DoppelGänger” unmasked: a web of deception. <https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/>
- Ünver, H. A., (2024). Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights. In B. REISS & K. WILHELMSSON (Eds.), European Parliament. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA\(2024\)754450_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf)
- Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Legal accountability and ethical considerations of AI in financial services. *GSC Advanced Research and Reviews*, 19(2), 130-142. [pdf]
- Virtosu, I., & Goian, M. (2023). Disinformation using artificial intelligence technologies—a key component of Russian hybrid warfare. In Smart Cities International Conference (SCIC) Proceedings (Vol. 11, pp. 197-222). [pdf]
- VRT Innovation. (2025, April 3). VRT’s commitment to fact-checking and combatting disinformation. VRT International. <https://www.vrtinternational.com/news/how-does-vrt-combat-disinformation>
- Williamson, S. M., & Prybutok, V. (2024). The era of Artificial Intelligence Deception: unraveling the complexities of false realities and emerging threats of misinformation. *Information*, 15(6), 299. <https://doi.org/10.3390/info15060299>
- Yang, K.-C., Menczer, F., & Observatory on Social Media. (2023). Anatomy of an AI-powered malicious social bot-net. In arXiv (Vols. 2307–16336v1) [Journal-article]. <https://arxiv.org/pdf/2307.16336.pdf>
- Young-Brown, F. (2019). Fake news and propaganda. Cavendish Square Publishing, LLC.. Retrieved from https://www.google.gr/books/edition/Fake_News_and_Propaganda/ha3XDwAAQBAJ?hl=el&gbpv=0
- Yuan, L., Jiang, H., Shen, H., Shi, L., & Cheng, N. (2023). Sustainable Development of Information Dissemination: A review of current fake news detection research and practice. *Systems*, 11(9), 458. <https://doi.org/10.3390/systems11090458>
- Yuskiv, B., & Karpchuk, N. (2024). Russian Federation’s FIMI prior to its Intervention in Ukraine. *State-Sponsored Disinformation Around the Globe*, 250. [pdf]
- Zimdars, M., & Mcleod, K. (2020). *Fake news: Understanding Media and Misinformation in the Digital Age*. MIT Press. Retrieved from https://www.google.gr/books/edition/Fake_News/1WPMDwAAQBAJ?hl=el&gbpv=0
- Zysk, K. (2024). High Hopes Amid Hard Realities: Defense AI in Russia. In: Borchert, H., Schütz, T., Verbovszky, J. (eds) *The Very Long Game*. Contributions to Security and Defence Studies. Springer, Cham. https://doi.org/10.1007/978-3-031-58649-1_16