

Memetic warfare as a threat to cognitive security. Legal approaches and non-legal safeguards in Poland

Wojny memiczne jako zagrożenie dla bezpieczeństwa kognitywnego. Podejścia prawne i zabezpieczenia pozaprawne na gruncie polskim

Abstract

This article examines the phenomenon of “memetic warfare” as a growing threat to cognitive security and democratic processes. The authors argue that memes – due to their virality, simplicity, and humorous nature – can be an effective tool for narrative manipulation, capable of shaping public opinion, deepening social polarization, and amplifying political and extremist propaganda. The development of artificial intelligence further facilitates the mass distribution of memes, increasing the scale and speed of their impact. At the same time, the balance between protection against disinformation and respect for freedom of speech and artistic creation remains a challenge, especially in the area of satire and parody. The article discusses potential legal and non-legal responses against memetic warfare, emphasizing the importance of targeting inauthentic behavior, strengthening social and cognitive resilience, narrative monitoring activities, and strategic communication. The study indicates that effective defense requires a multidimensional approach, encompassing regulations, technologies, psychological measures, and active social participation in shaping the information space.

SŁOWA KLUCZOWE: wojny memiczne, memy, dezinformacja, zagrożenia kognitywne, Akt o usługach cyfrowych

KEYWORDS: memetic warfare, memes, disinformation, cognitive warfare, DSA

MATEUSZ ŁABUZ – PhD, Institute for Peace Research and Security Policy at the University of Hamburg (IFSH), e-mail: labuz@ifsh.de,
ORCID – 0000-0002-6065-2188.

KATARZYNA MIKA-ŁABUZ – PhD, Pontifical University of John Paul II in Cracow, e-mail: katarzyna.mika-labuz@upjp2.edu.pl,
ORCID – 0009-0008-3872-7105.

I | Introduction

With the ongoing shift of social interactions to the online environment, the number of threats encompassing information security has significantly increased[1]. Threat actors operating in information space target narratives to shape opinions, views, and attitudes of targeted audiences[2]. Employed strategies might include subtle cognitive manipulation tailored to the audience and amplified by algorithms on social media.

An example of such activities is the use of memes – usually funny ideas and cultural artifacts that quickly spread through the internet – that can serve as fuel for information operations. „Memetic warfare” should currently be seen as one of the tactics within the broader scope of cognitive activities[3]. Memes enable the implementation of hidden messaging at scale, due to their quantity, virality, and often imperceptible potential for cognitive manipulations. They allow for the creation of specific associations, the decoding of which at the later point may significantly alter the perception of reality by human audiences[4]. Democratic actors need to be aware of the challenges that memetic warfare poses to the security of information space and, subsequently, to social and political processes[5].

The specific nature of memes, especially the difficulty of classifying them as classic forms of speech and the elusiveness of the context, make it difficult

1 Emily Denniss, Rebecca Lindberg, „Social media and the spread of misinformation: infectious and a threat to public health” *Health Promotion International* 40, No. 2 (2025): 3-4.

2 Andrii Paziuk, Dmytro Lande, Elina Shnurko-Tabakova, Phillip Kingston, „Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict” *Frontiers in Artificial Intelligence* 8 (2025): 2.

3 Tine Munk, *Far-right extremism online. Beyond the fringe* (London: Routledge, 2024); Tine Munk, „Digital Defiance. Memetic Warfare and Civic Resistance” *European Journal on Criminal Policy and Research* 31 (2025): 501-528.

4 Gordon Pennycook, Tyrone Cannon, David Rand, „Prior exposure increases perceived accuracy of fake news” *Journal of Experimental Psychology: General* 147, No. 12 (2018): 1865-1880; Douglas Youvan, „Memetic Cognition: The Compression of Complexity in the Human Psyche”, ResearchGate. https://www.researchgate.net/publication/389278599_Memetic_Cognition_The_Compression_of_Complexity_in_the_Human_Psyche [accessed: 15.06.2026].

5 Mateusz Łabuz, Christopher Nehring, „Information apocalypse or overblown fears – what AI mis- and disinformation is all about? Shifting away from technology toward human reactions” *Politics & Policy* 52, No. 4 (2024): 884-885.

to adapt legal provisions to such contemporary forms and tools of expression. Memetic creations regularly hide under the guise of satire and artistic creations, thus evading content moderation, which creates further regulatory challenges. This affects potential counter-strategies that must simultaneously safeguard security of information space, rights of third parties, but also freedom of speech and artistic expression[6].

The purpose of this article is to present the concept of „memetic warfare”, draw attention to the threats it poses, and highlight the difficulties in developing appropriate legal responses in Poland. The authors analyze legal acts, case law, and employ functional interpretation, supplemented by an analysis of literature at the intersection of information security and digital communications.

This article presents a formal-dogmatic legal analysis concerning mainly Poland aimed at crafting better legal and non-legal responses to safeguard information and cognitive security of democratic systems.

Therefore, the article focuses on the research question: *To what extent can memetic warfare be addressed within the existing legal framework in Poland, and what areas should be prioritized?*

Based on the difficulties in formulating legal solutions and after analyzing the psychological impact of memetic warfare on recipients, we point to the need to significantly strengthen the cognitive defenses of society. We propose specific measures in this area that can be implemented at the institutional, political, and social levels.

2 | „Memetic warfare” as a concept

The term „memes” was coined by evolutionary biologist Richard Dawkins in the 1970s, who saw them as units of cultural transmission[7]. Dawkins drew an analogy between biological genes that reproduce between organisms and the spread of ideas among society. Memes were originally meant as objects of cultural and societal replication, with the most fitting ideas having a greater

6 Andrea Wiesner, Svenja Schäfer, Sophie Lecheler, „Navigating the gray areas of content moderation: Professional moderators’ perspectives on uncivil user comments and the role of (AI-based) technological tools” *new media & society* 27, No. 3 (2025): 1223.

7 Richard Dawkins, *The Selfish Gene* (Oxford: Oxford University Press, 2006).

potential to be transmitted within the information ecosystem[8].

The concept of transmission has evolved over the years. Although the term originally referred to an idea, behavior pattern, or style that spreads within a culture, nowadays memes are most commonly associated with humorous images equipped with text snippets that go viral on the internet. They are also „digital artefacts such as slogans and catch-phrases that transcend cultural boundaries”[9]. Memes have gradually become one of the forms of online communication and a kind of modern cultural phenomenon, allowing for quick and simplified expression of opinions, most often in an accessible visual form adjusted to the demands of online communities. This has changed the meaning of the term, at least in the public consciousness.

However, the core idea remains unchanged: memes still function as information transmitters across populations. Moreover, along with their popularization and new dissemination mechanisms, the potential for influencing public opinion has become strategically significant[10]. This also leads to their weaponization, which accompanies the development of tactics used for information operations. As a consequence, in the digital age, memes have undergone a transformation from simple tools of entertainment to powerful tools of persuasion, capable of shaping public opinion, polarizing societies, strengthening political propaganda, or influencing political outcomes[11].

The potential of memes as a means of communication has been recognized by disinformation actors. This has led to the development of a new field of competition for narratives. So-called „memetic warfare” should currently be seen as an element of broader cognitive activities undertaken by state and non-state actors, and it refers to the deliberate creation and dissemination of memes to influence cultural or political beliefs, behaviors, or actions of a targeted audience[12]. This topic receives little attention in Polish literature, which is why analyses by Anglo-American authors predominate. NATO experts[13] defined

8 Gavan Gray, „Memetic Narratives in Information Warfare: The Danger of Viral Self-Contamination” *Hestia Review* 1 (2021): 15.

9 Munk, „Digital Defiance...”, 4.

10 Yelena Mejova, Arthur Capozzi, Corrado Monti, Gianmarco De Francisci Morales, „Narratives of War: Ukrainian Memetic Warfare on Twitter” *Proceedings of the ACM on Human-Computer Interaction* 9, No. 2 (2025): 2.

11 Munk, „Digital Defiance...”, 2-3.

12 Gray, „Memetic Narratives...”, 14-16.

13 Jeff Giese, „It's time to embrace memetic warfare” *Defence Strategic Communications* 1 (2016): 67-68.

„memetic warfare” nearly a decade ago, perceiving it as a „competition over narrative, ideas, and social control in a social-media battlefield”, while memes were supposed to be used „independently or in conjunction with cyber, hybrid, or conventional efforts”. In this sense, memetic warfare can complement the rich arsenal used in hybrid activities.

The use of the notion „warfare” might in itself spark debate due to its connotations of militarization and conflict. For that reason, it may be seen as disproportionate or suggest acts of aggression potentially governed by international law[14]. However, the term is used metaphorically in the context of memes, and it underscores the increasingly adversarial nature of online influence operations.

Munk[15] defines the term „memetic warfare” as „a form of information warfare conducted online through memes and other tactics to achieve political, strategic, or ideological objectives”. The aim of such activities is „offensive or defensive circulation of content to influence public opinion, disrupt discourse, and advance the interests of those engaged in the campaign”.

Memetic warfare originates from short messages, pictorial symbolism, associations, and emotional resonance[16]. It leverages the viral nature of memes and their anchoring in the everyday life of online communities to shape opinions, influence behaviors, and sway public preferences. This dual role as both cultural artifact and strategic tool has cemented memes as a significant force in contemporary narrative and ideological rivalry[17].

All of these qualities are perfectly suited to the fast-paced dynamics of social media and changing forms of mass online communication. This is a derivative of the dynamic changes in the ecosystem of information exchange observed in the last two decades. Traditional media, previously perceived as key suppliers of information, but also responsible for its selection, have been losing importance in favor of digital platforms that allow for quicker exchange, reaching new and

14 Waseem Ahmad Qureshi, „Information Warfare, International Law, and the Changing Battlefield” *Fordham International Law Journal* 43, No. 3 (2020): 901-905.

15 Tine Munk, *Memetic War. Online Resistance in Ukraine* (London: Routledge, 2024), 62-63.

16 Mateusz Łabuz, „Memetic Warfare – sind wir bereit für dieses Schlachtfeld?”, Tagesspiegel Background Digitalisierung. <https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/memetic-warfare-sind-wir-bereit-fuer-dieses-schlachtfeld> [accessed: 15.02.2026].

17 Anastasia Denisova, *Internet memes and society: Social, cultural, and political contexts* (New York: Routledge, 2019); Gray, „Memetic Narratives...”, 16.

wider audiences, with limited control mechanisms.

3 | Influence of memetic warfare

The impact of memes on the target audience is difficult to capture. Psychology, cognitive science, or even neuroscience can play an important role in this respect. Hoyle et al. [18] examined responses to Russian state-sponsored media narratives, revealing that such content can elicit significant psychological reactions. Ördén [19] discussed manipulating cognitive processes of the audiences to achieve specific objectives. Research by Pennycook et al. [20] showed that prior exposure increases perceived accuracy of fake news. These studies underline the potential for cognitive manipulations and shaping public perception through different tools of expression and narrative-building.

The power of memes lies in their ability to distill complex ideas into digestible, shareable formats. A single image or short video, paired with a catchy caption, can be a convenient source of communication with an audience, or a way to reinforce cognitive biases, which accompany thought processes and are based on a simplified perception of reality. By bypassing critical thinking, memes are embedding a specific vision of reality in the viewer's subconsciousness, creating associations that can be decoded in the future and influence decision-making processes [21]. The ease with which a meme's message can be recalled makes it more likely to be perceived as true or important, especially given their repetitive and viral nature.

Mememes thus bypass the cognitive safety system, e.g., by reducing extremism to the level of an acceptable joke. In the classic psychologically-oriented approach of Kahneman [22], they bypass the second mode of thinking, which is

18 Aiden Hoyle, Charlotte Wagnsson, Helma van den Berg, Bertjan Doosje, Martijn Kitzen, „Cognitive and Emotional Responses to Russian State-Sponsored Media Narratives in International Audiences” *Journal of Media Psychology* 35, No. 6 (2023): 362-375.

19 Hedvig Ördén, „The neuropolitical imaginaries of cognitive warfare” *Security Dialogue* 55, No. 6 (2024): 607-609.

20 Gordon Pennycook, Tyrone Cannon, David Rand, „Prior exposure increases perceived accuracy of fake news” *Journal of Experimental Psychology: General* 147, No. 12 (2018): 1865-1880.

21 Pennycook, Cannon, Rand, „Prior exposure...”; Łabuz, „Memetic Warfare – sind wir bereit...”.

22 Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

responsible for rationalism and logic, and reduce the decision-making process to emotions and instincts. The use of simplifications, in turn, enables the anchoring of a specific worldview or mindset, or the reinforcement of already existing biases. This is, in fact, the assumption behind some of the propaganda creations, in which the power of stereotype is exploited by visualizing antagonistic values and creating simplified dichotomous associations[23].

Moreover, memes often exploit humor, parody, and satire, which makes them more attractive to potential recipients and thus increases the likelihood of sharing. Simultaneously, it also lowers the recipients' vigilance, as they might be treated as an innocent joke or artistic creation.

4 | Amplification and role of artificial intelligence

Influencing the information environment through memetic warfare is strongly dependent on the ability to access the audience, which in turn is a derivative of the use of communication channels adjusted to the specific needs of recipients. Creating engaging content, therefore, requires considerable skills and a good „feeling” for the audience's expectations. It is also crucial to adapt to these expectations, which in turn requires understanding specific cultural contexts and the mechanics of virality. As in Dawkins' original idea, the key to spreading ideas lies in their ability to replicate; however, the specifics of the information space differ significantly between communities or societies[24].

Artificial intelligence (AI) is playing an increasingly important role in this respect. On the one hand, it increases the reach – whether by enhancing traffic by automated mechanisms (e.g., bots), or through so-called algorithmic amplification within the digital platforms, as maximization of users' engagement is preferred by algorithms. In turn, users follow and enhance trends[25]. Additionally, emerging technologies, including generative AI, allow for a significant simplification of the generation and dissemination processes, and they are used to streamline some processes while freeing up other resources[26]. This

²³ Janosch Delcker, „AI fakes, cyberattacks threaten German election”, Deutsche Welle. <https://amp-dw-com.cdn.ampproject.org/c/s/amp.dw.com/en/from-ai-fakes-to-cyberattacks-threats-to-german-elections/a-70972702> [accessed: 15.06.2026].

²⁴ Dawkins, *The Selfish Gene*.

²⁵ Hany Farid, „On Algorithmic Amplification” *Inference* 6, No. 1 (2021).

²⁶ Łabuz, Nehring, „Information apocalypse...”, 884; Katja Muñoz, „The AI Election Year: How to Counter the Impact of Artificial Intelligence” *DGAP Memo* 1 (2024): 1-4.

does not automatically mean that memes can be produced solely by AI without human oversight, as hitting trends still requires analytical activities and appropriate adjustments. However, AI has significant potential to automate selected processes and support production in areas where synthetic creations can be used (e.g., images of targeted identifiable people that do not reflect reality, but only imitate it).

AI supports the (re)production of memes in the first place, not their creative design, which still requires recognition of cultural context, irony, and the specificity of online subcultures. On the other hand, it enables the flooding of social media and the mass replication of content that is mind-numbing but also engaging for users. Memes remain primarily a social practice and many audiences prefer low-quality aesthetics, which AI can reproduce. An example of such a phenomenon is the mass use of motivational videos with the voices of Donald Trump or Elon Musk on the TikTok platform. The total reach generated by this type of content was estimated at several hundred million views[27].

The most important element for amplification is therefore the concept behind the content and knowledge of the mechanisms of dissemination, which has foundations both in understanding the technological aspects of how algorithms work and social psychology, including social susceptibility to cognitive biases[28].

Recently, a lot of attention has been devoted to research on deepfakes. They are referred to as AI-generated or manipulated images, audio, or video content that resembles existing persons, objects, places, entities, or events and would falsely appear to a person to be authentic or truthful[29]. Their essential feature is their hyperrealism, that is, the ability to faithfully imitate reality, which significantly distinguishes them from meme creations that do not mirror reality but visibly distort it.

Contrary to popular belief and some media hype surrounding deepfakes, they do not necessarily have to be the primary tool for conducting information

27 Emanuel Maiberg, „AI Slop of Musk and Trump on TikTok Racks Up 700 Million Views”, 404 Media. <https://www.404media.co/ai-slop-of-musk-and-trump-on-tiktok-racks-up-700-million-views> [accessed: 15.06.2026].

28 Hoyle, Wagnsson, van den Berg, Doosje, Kitzen, „Cognitive and Emotional Responses...”, 368-371.

29 Artificial Intelligence Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

manipulation operations. According to Microsoft[30], in many cases external actors like China, Russia, or Iran do not use sophisticated creations that faithfully imitate reality but low-quality content that is intended to anchor a specific impression in the recipients, or sow confusion[31]. Memes also play an important role in this matter.

5 | Psychological operations

As previously mentioned, from the perspective of cognitive psychology, the effectiveness of memetic warfare can be explained based on dual-processing models, in particular the System 1 and System 2 theory proposed by Kahneman[32]. Memes are designed to activate fast, intuitive, and affective cognitive processes (System 1), bypassing the slower, reflective, and analytical processing characteristic of System 2. The brevity of the message, strong visual stimuli, and humor promote peripheral processing, where attitude change occurs without deep analysis of arguments[33]. In addition, the activation of mechanisms of the mere exposure effect and the illusory truth effect means that repeated exposure to a given meme increases its subjective credibility, regardless of its factual accuracy. In this way, memes can stabilize certain associations and narratives in the memory of the audience.

Memetic warfare, due to its adaptability and ease of creation, can be widely used to conduct influence campaigns. The superior goal might be promoting certain meta-narratives to gradually change the views and sentiment of public opinion[34]. Memes are used by disinformation actors to discredit opponents, but there is also no shortage of politicians who reach for memes to increase their own attractiveness or to incept certain ideas. Presenting Joe Biden as an incapacitated old man or Kamala Harris as a communist during the US presidential campaign in 2024 was intended to instill specific negative associations

30 Microsoft, *Same targets, new playbooks: East Asia threat actors employ unique methods* (Redmond: Microsoft, 2024).

31 Microsoft, „Protecting Election 2024 from foreign malign influence: lessons learned help us anticipate the future”. <https://msblogs.thesourcemediaassets.com/sites/5/2023/11/MTAC-Report-2024-Election-Threat-Assessment-11082023-2-1.pdf> [accessed: 15.02.2026].

32 Kahneman, *Thinking, Fast and Slow*.

33 Richard Petty, John Cacioppo, „The elaboration likelihood model of persuasion” *Advances in Experimental Social Psychology* 19 (1986): 123-205.

34 Munk, *Memetic War...*

in the recipients. Narendra Modi playing the guitar and singing songs had a humorous tone and served to warm up the politician's image[35]. Supporters of Indonesian President Prabowo Subianto, known for ruling with an iron fist, disseminated his fairy-tale memetic alter-ego, depicting him on the one hand as a funny grandpa and on the other as a cuddly mascot[36]. Similar schemes are used, among others, by Donald Trump, who publishes pastiche photos of himself as the Pope, a Jedi, or illustrating the takeover of Greenland by the US[37].

Supporters of populist parties also commonly apply meme creations, e.g., „völkisch” associations are used to promote a specific worldview and favor the right-wing AfD party in Germany[38]. Similar patterns are used by extremist and terrorist groups as they employ memes to appeal to younger audiences, abusing humor and pop culture references to normalize radical ideologies. At the height of its power, ISIS used memes to attract new followers, which showed that even such radical groups were aware of the mechanisms of cognitive manipulation and were able to adapt their messaging[39]. At the end of 2025, Spanish fact-checking organization Maldita discovered a network of accounts promoting fascism themes in an artistic way (e.g., images of Benito Mussolini wearing pink sunglasses or singing modern songs), and called this phenomenon „pop fascism”[40].

In that context, humor serves as a tool for radicalization and allows the true

35 Nilesh Christopher, „AI Modi started as a joke, but it could win him votes”, Rest of World. <https://restofworld.org/2023/ai-voice-modi-singing-politics> [accessed: 15.02.2026].

36 Rumman Chowdhury, „AI-fuelled election campaigns are here – where are the rules?” *Nature* 628 (2024): 237.

37 Stuart Thompson, „How Trump Is Using Fake Imagery to Attack Enemies and Rouse Supporters”, *The New York Times*. <https://www.nytimes.com/interactive/2025/10/21/business/media/trump-ai-truth-social-no-kings.html> [accessed: 15.06.2026].

38 Deutschlandfunk, „Die völkischen KI-Memes von ‚Wilhelm Kachel’”. <https://www.deutschlandfunk.de/rechtsextreme-memes-kuenstliche-intelligenz-wilhelm-kachel-propaganda-100.html> [accessed: 15.06.2026].

39 Ally McCrow-Young, Mette Mortensen, „Countering spectacles of fear: Anonymous’ meme ‚war’ against ISIS” *European Journal of Cultural Studies* 24, No. 4 (2021): 832–834.

40 Maldita, „Memes, football and songs: how ‚Pop Fascism’ paves the way for disinformation”. <https://maldita.es/investigaciones/20251013/memes-songs-disinformation-pop-fascism> [accessed: 15.06.2026].

purpose to be efficiently hidden under the guise of permitted uses. Regina^[41] draws attention to the combination of ease of dissemination and a kind of trivialization of threats: „The seeming banality of memes serves as a perfect cover for more sinister content, allowing extremist groups to establish presence in mainstream digital spaces without immediate detection”. It subsequently leads to the normalization of radical views, whereas „the rapid-fire nature of meme consumption makes it difficult for individuals to engage in critical analysis, creating perfect conditions for subtle indoctrination”^[42].

From that perspective, memetic warfare influences the processes described in Tajfel and Turner’s social identity theory^[43], which primarily refers to normative social influence. In that context, memes function as markers of group membership – understanding them requires knowledge of specific cultural codes, which reinforces the boundaries between „in-group” and „out-group”^[44]. Humor and irony serve here as a mechanism for reducing psychological resistance, making violations more acceptable, as they are perceived as harmless. As a result, radical or dehumanizing content can be gradually internalized, and the mechanism of normalization through habituation allows for shifting the boundaries of acceptable discourse.

Memetic warfare can, therefore, serve the long-term shaping of cognitive and emotional frameworks within which certain political attitudes begin to be perceived as natural, obvious, or socially rewarding. This potential for cognitive influence has already been recognized by state actors.

China has systematically integrated „cognitive warfare” into its official military strategy, emphasizing the manipulation of information and psychological influence to achieve strategic objectives without direct military confrontation^[45]. This approach is encapsulated in the „Three Warfares” doctrine, which comprises public opinion warfare, psychological warfare, and legal warfare. It

41 Gitau Regina, „Meme warfare: How Extremist Groups Weaponize Internet Humor to Normalize Radical Ideologies”, Center of Diplomatic Insight. <https://centerfordiplomaticinsight.substack.com/p/meme-warfare-how-extremist-groups> [accessed: 15.06.2026].

42 Regina, „Meme warfare...”.

43 Henri Tajfel, John Turner, „An integrative theory of inter-group conflict”, [in:] *The Social Psychology of Inter-group Relations*, ed. William G. Austin, Stephen Worchel (Monterey: Brooks/Cole, 1979), 33-47.

44 John Turner, Rupert Brown, Henri Tajfel, „Social comparison and group interest in ingroup favouritism” *European Journal of Social Psychology* 9, No. 2 (1979): 187-204.

45 Elsa Kania, „The PLA’s Latest Strategic Thinking on the Three Warfares” *China Brief* 16, No. 12 (2016): 10-14.

guides China in leveraging information to influence perceptions and achieve strategic goals in a longer term^[46]. This strategy also uses memetic warfare, which serves to simplify and amplify narratives, disseminate propaganda, undermine adversaries, or promote a specific vision of the world while mocking the West at the same time. This is complemented by engaging the public, also through the use of inauthentic social media accounts that amplify a specific messaging. Observing these developing trends, Microsoft^[47] noted: „Chinese influence actors [...] honed their techniques and experimented with new media. [...] The influence actors behind these campaigns have shown a willingness to both amplify AI-generated media that benefits their strategic narratives, as well as create their own video, memes, and audio content. Such tactics have been used in campaigns stoking divisions within the United States and exacerbating rifts in the Asia-Pacific region – including Taiwan, Japan, and South Korea”.

6 | Legal countermeasures

Weaknesses of the current legal order

From a legal perspective, memetic warfare exposes several structural weaknesses inherent both in the Polish legal order and the EU regulatory framework. These weaknesses stem mostly from the hybrid nature of memes as indirect, context-dependent forms of expressions that combine visual, textual, and symbolic layers.

Their meaning cannot be captured through traditional speech typologies that underpin constitutional and statutory protections of expression. Memes, by their very nature, are based on simplifications, associations, and a distorted vision of the world. They successfully navigate the natural tension between protecting cognitive security and the conventionally guaranteed freedom of speech or artistic expression. Similar difficulties are recognized in the discourse on classic disinformation, the definition of which is missing in the Polish law^[48].

⁴⁶ Laura Jackson, „Revisions of Reality: The Three Warfares – China’s New Way of War”, [in:] *Information at War: From China’s Three Warfares to NATO’s Narratives*, ed. Peter Pomerantsev (London: The Legatum Institute, 2015), 5.

⁴⁷ Microsoft, *Same targets, new playbooks...*

⁴⁸ Magdalena Dziedzic, „Przeciwdziałanie dezinformacji w kontekście wybranych regulacji Aktu o usługach cyfrowych oraz Aktu o Sztucznej Inteligencji” *Prawo i Więź*, No. 6(53) (2024): 228.

Moreover, memes are not classic verbal statements, but complex visual and textual messages, often allusive and elusive in nature. This makes it difficult to assign a clear meaning to the statement, which affects the possibility of subsuming it under types of prohibited acts such as defamation or insult if they are aimed against third parties. Copyright law also provides additional legal guarantees through the principle of fair use for the purposes of parody or pastiche (Article 29). However, the doctrine indicates that it is difficult to imagine a conviction for a meme based on copyright law^[49]. At the adjudicative level, any decisions in that matter would be based on a high degree of discretion.

Additionally, even if a meme damages a reputation, it is almost impossible to demonstrate the *mens rea* of the author, and even more difficult to identify the author. In most of the cases, the content is created anonymously and replicated mechanically by the users, with a single click. Different entities are responsible for creating the content, and others for sharing it, which might further complicate legal proceedings. A relative ease of anonymization results in weaker enforcement of any legal provisions that could be introduced against memes, which in turn would automatically undermine the legitimacy of their introduction.

At the level of national law in Poland, freedom of expression is guaranteed by Article 54 of the Constitution, whereas Article 73 protects freedom of artistic creation^[50]. The problem of spreading false information, or disinformation, is not explicitly addressed in Polish criminal law^[51], with the exception of Article 132 of the Penal Code, which addresses a specific type of prohibited act: intelligence disinformation^[52]. With the current wording, there is no significant anchoring point with memes as a phenomenon, but in the future this provision could possibly be subject to an expanded interpretation. We will return to these provisions later in our discussion.

Potential solutions could be sought in the protection of third party rights. However, they should only be seen as a subsidiary solution. Articles 212-216

⁴⁹ Mateusz Wiktorek, „Więzienie za mema – ŁĄCZY NAS KARNE z Krzysztofem Krupą i dr. Bohdanem Widłą”, Karne24. <https://karne24.com/wiezienie-za-mema> [accessed: 15.06.2026].

⁵⁰ Grzegorz Maroń, „Fact-checking a wolność słowa” *Radca Prawny. Zeszyty Naukowe*, No. 1(3) (2022): 95.

⁵¹ Dorota Domalewska, „Dezinformacja jako zagrożenie dla demokracji i regulacje prawne w zakresie jej przeciwdziałania w Polsce i wybranych krajach europejskich” *Politeja*, No. 5(92) (2024): 359-379.

⁵² Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 1997 nr 88 poz. 553).

of the Penal Code guarantee protection against defamation and insult, which might encompass memes, too[53]. However, the line between satire and a crime is problematic. These Articles presuppose a relatively direct communicative act capable of conveying a specific factual allegation or degrading message, which in the case of memes is difficult to prove. Additionally, under constitutional and European standards, public figures must tolerate a broader range of satire, which additionally raises the threshold for any legal intervention. Therefore, the real possibility of criminal prosecution for memes is, in practice, negligible[54].

Articles 255a, 256, and 257 of the Penal Code (public incitement to crime, hatred, or violence) could apply to radicalizing memes. This is a potential starting point for prosecution, but it would be limited to absolutely obvious situations of radical and extremist content.

Additionally, Articles 23-24 of the Civil Code guarantee protection of personal rights, which might serve as a basis for requesting removal of a meme. However, lengthy proceedings, lack of compliance on the side of digital platforms, and lack of quick remedies in a situation of dynamic dissemination of content should be seen as problematic[55]. It also does not solve the problem of permissible satire and artistic expression, which can be a convenient smoke-screen for disinformation actors weaponizing memes.

Meanwhile, the distinction between disinformation, i.e., deliberately disseminated false or manipulated content, and legitimate artistic or satirical expression remains the fundamental regulatory challenge[56]. The European Commission, in its policy documents (e.g., Communication on Tackling Online Disinformation), points to the need to counter harmful content while respecting Article 11 of the Charter of Fundamental Rights of the EU and Article 10 of the European Convention on Human Rights, as both provide for guaranteeing freedom of expression. The European Court of Human Rights has consistently held that satire enjoys an elevated level of protection due to its expressive nature, inherent exaggeration, and tendency to provoke. However, derogatory

53 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 1997 nr 88 poz. 553).

54 Magdalena Banasik, Wiktoria Bocheńska, Wiktoria Dziubaczka, Aleksandra Bodziony, „Prawne aspekty walki z dezinformacją i fake newsami w przestrzeni internetowej” *Rocznik Administracji Publicznej* 11, No. 1 (2025): 11.

55 Banasik, Bocheńska, Dziubaczka, Bodziony, „Prawne aspekty walki z dezinformacją...”, 11.

56 European Commission, *Tackling online disinformation: a European Approach*, COM(2018) 236 final, 4.

content containing hate speech is not protected when it goes beyond typical satirical outcome[57]. Here, too, discretion is a key factor.

Realistically, it is worth considering whether the concept of classifying memes as a criminal phenomenon would be socially desirable. It is difficult to imagine a situation in which political parties decide to introduce anti-meme legislation, risking a strong backlash given the already strong entrenchment of memes in the culture of online expression[58]. This obstacle is rarely addressed in legal analysis and concerns social perceptions of legal sanctions. Memes have become embedded in youth culture and are widely understood as a playful, informal modality of expression, even if they may infringe on the rights of third parties or promote attitudes that are widely considered socially harmful. Enforcing legal liability for memes could be perceived as excessive repression, especially by younger demographics. As a result, legal action could be counter-productive, fueling accusations of authoritarianism and censorship[59].

Legal responses to inauthentic behavior

Searching for legal solutions, therefore, requires a shift in the logic of countering memetic warfare. Memes can be used as memetic warfare only when they meet certain criteria. The fundamental harmfulness and disinformation potential of memes is deeply imprinted in their steered amplification, especially through interconnected networks of inauthentic accounts. Identifying such networks and counteracting inauthentic behavior online should be the primary goal of legal interventions.

It may form the basis for further legal actions, especially by cutting off disinformation actors from algorithmic amplification. In this context, it is essential to create synergy between actions that can be taken at national level and utilizing mechanisms introduced by the EU legislation, such as the Digital Services Act, the so-called DSA. However, this will not be possible without an appropriate system for monitoring online content and establishing a framework for having situational awareness. It also requires the development of appropriate monitoring and flagging procedures following the implementation of the EU

57 Adam Wiśniewski, „The European Court of Human Rights and Internet-Related Cases” *Białostockie Studia Prawnicze* 26, No. 3 (2021): 124.

58 Peter Ling, „One Does Not Simply Upload a Meme – Internet Memes and the Parody Exemption in Europe”, [in:] *Developments and Directions in Intellectual Property Law: 20 Years of The IPKat*, ed. Hayleigh Bosher, Eleonora Rosati (Oxford: Oxford University Press, 2023), 303.

59 Wiesner, Schäfer, Lecheler, „Navigating the gray areas...”, 1227.

DSA^[60] in Poland.

For legal clarity, it would be advisable to consider whether Article 132 of the Penal Code should be supplemented with appropriate provisions penalizing inauthentic behavior online, aimed at spreading false narratives, regardless of its connection to intelligence disinformation. In its original wording, Article 132 of the Penal Code refers to the activities of foreign intelligence: *Anyone who, while rendering intelligence services to the Republic of Poland, misleads a Polish state authority by providing forged or altered documents or other items, or by concealing true information or providing false information of significant importance to the Republic of Poland, shall be subject to imprisonment for a term of between one and 10 years*^[61].

Kosmaty points to the uniqueness of the Polish regulation, which has no equivalent in other European countries, and sees it as „a deliberate misleading or manipulation of information to achieve strategic, political or military advantages. It is used by states or intelligence organisations that use false or distorted data to weaken their opponents, cause confusion or strengthen their own position. It may include spreading false information, forging documents and controlling the narrative in the media”^[62]. Such wording opens up certain possibilities for classifying online activities within the scope of „memetic warfare” as criminal offenses, provided that certain conditions are met. However, proving a connection between the activities and foreign intelligence services requires evidence, which in turn raises the issue of attribution, as well as the directionality of actions aimed directly at Polish authorities within the framework of specific activities.

In its current wording, the provision does not provide sufficient protection against memetic warfare aimed at influencing the narrative in the Polish information space. It defines too narrowly the set of entities to which it could apply, excluding a significant proportion of disinformation actors who, for various reasons, may attempt to influence the information environment in Poland. In light of the arguments presented above, it seems reasonable to conclude that the focus should be shifted from the narrative to the actors and mechanisms of its dissemination, and to identify potential behaviors that could be criminal-

⁶⁰ Digital Services Act, 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.

⁶¹ Piotr Kosmaty, „Selected legal aspects of the crime of intelligence disinformation” *Internal Security Review* 33 (2025): 327; Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 1997 nr 88 poz. 553).

⁶² Kosmaty, „Selected legal aspects...”, 328.

ized without undermining freedom of speech.

In our opinion, such behavior should include the use of a network of inauthentic accounts and the artificial amplification of their reach. As in the case of Article 132 of the Penal Code, specific objectives of the actor would still have to be proven, but no longer in connection with foreign intelligence activities, but with illegal methods of operation. For that reason, it would be necessary to introduce a specific provision penalizing the use of inauthentic behavior. Additionally, focusing on the actors behind the process might also have some practical implications, as it would allow the law enforcement to identify the source of a message and track its further spread.

The definition of protected goods also requires consideration, although the mechanism itself may be sufficient grounds in this case. The use of networks of inauthentic accounts is, per se, an attempt at manipulation and should be considered harmful.

Support in this regard can be provided through the appropriate use of EU tools. The DSA introduces obligations for so-called very large online platforms[63], including assessing and mitigating systemic risks related to disinformation (Articles 34 and 35)[64]. These provisions provide basic protection against the spread of disinformation but offer only limited protection against memetic warfare[65]. As memes, in principle, should not be qualified as illegal, they allow for bypassing the safeguards introduced on digital platforms, which are usually aimed against misleading and deceptive creations that faithfully imitate reality[66]. However, the shift in focus toward inauthentic behavior would open up the possibility of invoking systemic risks, which are to be mitigated by digital platforms covered by the DSA regulations.

The dynamic development of AI poses an additional threat to cognitive security. The EU Artificial Intelligence Act[67] introduces obligations to label syn-

63 Dziedzic, „Przeciwdziałanie dezinformacji...”, 229-231.

64 Digital Services Act, 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.

65 Dziedzic, „Przeciwdziałanie dezinformacji...”, 230.

66 Mateusz Łabuz, „Deep fakes and the Artificial Intelligence Act – An important signal or a missed opportunity?” *Policy & Internet* 16, No. 4 (2024): 783-800; Iwona Bień-Węglowska, „Deepfake w świetle aktu w sprawie sztucznej inteligencji” *Prawo i Więź*, No. 5(58) (2025): 151-169.

67 Artificial Intelligence Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

thetic content (that might have memetic dimension, too), whereas Article 50 reserves important exceptions for satirical content[68]. At the moment, at the national level in Poland, there is no comprehensive regulation that would address AI-generated content, which creates a widening legal gap. In this case, it is important to note that civil law has not kept pace with the rapid development of generative AI technology, which allows for hyper-realistic reproduction of others' images and using it for meme creation, defamation, financial scams, etc. Therefore, legislators should consider strengthening image protection for third parties. It is also advisable to monitor solutions implemented in other countries to draw from the best practices (e.g., in Denmark image protection is supposed to be embedded in personal data protection).

7 | Non-legal countermeasures

Proactivity

Institutionally coordinated anti-memetic activities are not common worldwide. This, in turn, opens up significant scope for action, especially for countries that are under great pressure from disinformation actors. Preparing for memetic warfare takes place mainly at the level of building social resilience, creating synergy between different levels of communication, and shaping the information space proactively. It also requires preemptive actions.

Education and cognitive security

Public education and developing interpretive skills for understanding the mechanisms of online content dissemination are crucial in this regard[69]. The introduction of a new Health Education course in the school curriculum in Poland should provide an opportunity to address issues of information and cognitive security. However, the confusion surrounding the introduction of the subject into schools is not conducive to promoting digital literacy.

The term „cognitive defenses” could therefore refer to strategies and capabilities for protecting individuals and groups from manipulation, disinformation, or other types of psychological influence aimed at targeting perception, decision-making, or beliefs. It might involve enhancing critical thinking, media literacy, and psychological resilience. It may also include specific activities

68 Łabuz, „Deep fakes and the Artificial Intelligence Act...”.

69 Łabuz, Nehring, „Information apocalypse...”, 885.

in the information space aimed at creating narratives and counter-narratives.

Monitoring

Monitoring narrative trends is important to understand what narratives are permeating public opinion. It is therefore necessary to invest in tools and capabilities that enable comprehensive media watching, which is largely carried out in Poland by Naukowa i Akademicka Sieć Komputerowa (NASK, Scientific and Academic Computer Network). The activities of independent fact-checking organizations are equally important in terms of demystifying the sources of specific narratives[70]. In the context of legal solutions in Poland, it would be important to strengthen the institutional position of NASK in order to create pre-emptive situational awareness, monitor inauthentic behavior and respond appropriately, also at the level of offensive cyber-capabilities in the event of an identified external threat.

Digital platforms

A key element of the disinformation supply chain is digital platforms. Recognizing narratives should be accompanied by recognizing the sources of movement and engagement. It is therefore advisable to focus on the channels and actors of dissemination. Multiplication of the same content and its artificial amplification between compromised or fake accounts may be the key to understanding the mechanisms of information operations conducted by adversaries. A meme itself is not necessarily a manifestation of cognitive or memetic warfare. Its amplification and instrumental use by state actors and their proxies definitely is.

Whole-of-a-society approach

Several nations have already developed innovative approaches to combat memetic warfare and actively respond to it. Safeguards are in many ways synonymous with commonly recognized counter-disinformation strategies based on strengthening social resilience[71]. The Ukrainian model is based on a „whole-of-a-society approach” and was developed over many years of experience with high-intensity information warfare[72]. The inclusion of society in

⁷⁰ Anna Łukaszuk, „„Whole of Government’ oraz „Whole of Society’ – skuteczne działania w budowaniu świadomości i odporności społeczeństwa na zagrożenia w przestrzeni informacyjnej – przeciwdziałanie dezinformacji w Polsce” *Zeszyty Prawnicze* 23, No. 3 (2023): 179.

⁷¹ Łukaszuk, „„Whole of Government’ oraz „Whole of Society’...”, 169-171.

⁷² Munk, *Memetic War...*

strategic activities increases its competences, allows for gradual psychological inoculation against Russian propaganda and disinformation, and emphasizes the importance of ordinary citizens within the framework of state-level activities. The success of Ukraine is precisely based on experience, sense of unity, and the implementation of a „defence strategy that integrates grassroots movements, digital activism, and innovative methods such as the extended use of online communication and memes”[73]. This model is designed to bring together different stakeholders, including public authorities, military, and individuals, and requires the mobilization of masses, including activists and celebrities, to enhance its outreach.

Another example might be Taiwan’s „humor over rumor” strategy that leverages the power of satire and wit to combat Chinese disinformation[74]. By responding to falsehoods with humorous and shareable content, Taiwanese authorities can diffuse tensions and reduce the virality of misleading narratives. From a strategic point of view, it resembles waging a guerrilla war, which, however, requires a sense of humor and a great understanding of trends[75].

Therefore, the response to memes can be memetic, and the given examples of the so-called „whole-of-a-society approach” should be an important point of reference. Countries that face strategic communication deficits can benefit from such experiences, although one has to consider regional, geopolitical, and cultural specificities.

Psychological counter-operations

It might be wondered whether democracies should participate in the memetic arms race and use them as active measures – not only to defend themselves, but also to counterattack[76]. It is therefore necessary to constantly monitor trends and invest in skills that are difficult to even be called „soft skills”, because they relate to a sense of humor. Something that is difficult to teach. However, shaping the information space requires understanding the technical mechanisms of creating content on a mass scale and distributing it on social

73 Łabuz, „Memetic Warfare – sind wir bereit...”; Expert interview with Tine Munk conducted by the authors on 15 January 2025.

74 Arwa Mahdawi, „Humour over rumour? The world can learn a lot from Taiwan’s approach to fake news”, The Guardian. <https://www.theguardian.com/commentisfree/2021/feb/17/humour-over-rumour-taiwan-fake-news> [accessed: 15.06.2026].

75 Giese, „It’s time to embrace memetic warfare”, 70.

76 Giese, „It’s time to embrace memetic warfare”, 70.

media in order to maximize reach and interaction, which in turn entails the necessity to build competences in the area of content management.

One could plausibly advocate for the possibility of trolling adversaries by using relatively simple methods of ridiculing. Giese[77] suggested that „if propaganda and public diplomacy are conventional forms of memetic warfare, then trolling and PSYOPs are guerrilla versions”. However, such activities, based on active co-shaping of the information space by state institutions, may be subject to significant constitutional restrictions in some EU countries.

As discussed, memes have become an element of the cognitive defense of Ukrainian society in the information warfare against Russia, and allow for the active involvement of citizens, giving them an additional sense of belonging[78]. „Memes demoralize Russian forces and expose the flaws in their propaganda strategy while using humor, creativity, and digital activism to counter falsehoods, boost morale, and highlight successes such as attacks on the Russian Black Sea Fleet and the Kursk incursion. Humorous and satirical memes mobilize citizens, activists, and independent groups and transform digital platforms into arenas for civic defence”[79]. They are also picked up externally, which includes the narrative-shaping and fund-raising efforts from the North Atlantic Fella Organization (NAFO), which helps to strengthen the Ukrainian case in the international space and mock Russia, using humor as an offensive tool[80].

The key in this respect was to find shareable and easy-to-arouse leitmotifs. One such successful motif was the use of a record of a conversation between the defenders of Ukrainian Snake Island and a Russian warship, which ended with the words, „Russian warship, go fuck yourself”. This slogan was distributed on a mass scale, strengthening the Ukrainian sense of belonging, the will to resist, and at the same time ridiculing the Russian army[81].

77 Giese, „It’s time to embrace memetic warfare”, 70.

78 Łabuz, „Memetic Warfare – sind wir bereit...”.

79 Expert interview with Tine Munk conducted by the authors on 15 January 2025.

80 Munk, „Digital Defiance...”, 1-3.

81 Andrew Keen, „Go Fuck Yourself’. On Putin’s Propaganda and the Week in Ukrainian Resistance”, Literary Hub. <https://lithub.com/go-fuck-yourself-on-putins-propaganda-and-the-week-in-ukrainian-resistance> [accessed: 15.06.2026].

8 | Conclusion

Disinformation actors do not need sophisticated creations for effective cognitive manipulation and further erosion of democratic processes. Memes, with their high shareability, can often reach far larger audiences than traditional forms of content. By exploiting cognitive biases and existing tensions, they aim for deepening societal divides and eroding social cohesion. At the same time, they negatively affect the epistemic value of public debate and lead to the symbolization of meanings. Their weaponization is possible through steered and coordinated use, especially in the case of artificial amplification using inauthentic behavior. For that reason, memetic warfare has a significant potential to shape ideas and attitudes.

Recognizing the threats to security of information space requires legal action. Currently, criminal law does not guarantee adequate protection against memetic warfare. Selected provisions can be applied in a subsidiary manner and primarily address the content of the meme, which limits their applicability. Memes are generally protected under the right to freedom of expression and the boundaries of satire, especially against public figures, are significantly shifted. Moreover, the cultural and social context lends memes legitimacy and complicates the effective enforcement of defamation and libel laws. Therefore, due to legal barriers and social perception, criminal responses to memes are, in practice, marginal and carry a high risk of censorship.

Hence, we propose, first of all, focusing on the ways and actors of disseminating content in order to include memetic warfare in existing frameworks to counteract coordinated disinformation activities. In our opinion, it is necessary to pay attention to inauthentic behavior as a source of amplifying the reach of memes and to strengthen institutional mechanisms of pre-emptive situational awareness and social media monitoring. In the Polish system, NASK should play such a role, closely coordinating activities with counterintelligence and law enforcement agencies.

At the moment, the current legal framework in Poland does not effectively counter memetic warfare as a phenomenon and requires adaptation to the rapidly changing technological reality. Significant support, mainly in counteracting algorithmic amplification on digital platforms, may be provided in the future by EU regulations, including the DSA and AI Act, in particular in the area of counteracting systemic risks or the misuse of AI systems.

Additionally, democratic actors must constantly implement multidimen-

sional protective strategies that encompass educational, psychological, technical, and communicational aspects. The „competition over narrative, ideas, and social control”[82] must be fully realized, so that memes are not viewed through the prism of their superficial informational value, but as a powerful tool of communication capable of shaping opinions in the short and long term.

References

- Banasik, Magdalena, Wiktoria Bocheńska, Wiktoria Dziubaczka and Aleksandra Bodziony. „Prawne aspekty walki z dezinformacją i fake newsami w przestrzeni internetowej.” *Rocznik Administracji Publicznej* 11, No. 1 (2025): 9-18. <https://doi.org/10.4467/24497800RAP.25.001.21293>.
- Bień-Węglowska, Iwona. „Deepfake w świetle aktu w sprawie sztucznej inteligencji.” *Prawo i Więź*, No. 5(58) (2025): 151-169. <https://doi.org/10.36128/4dr67e80>.
- Chowdhury, Rumman. „AI-fuelled election campaigns are here – where are the rules?” *Nature* 628 (2024): 237. <https://doi.org/10.1038/d41586-024-00995-9>.
- Christopher, Niles. „AI Modi started as a joke, but it could win him votes.” *Rest of World*. <https://restofworld.org/2023/ai-voice-modi-singing-politics>.
- Dawkins, Richard. *The Selfish Gene*. Oxford: Oxford University Press, 2006.
- Delcker, Janosch. „AI fakes, cyberattacks threaten German election.” *Deutsche Welle*. <https://amp-dw-com.cdn.ampproject.org/c/s/amp.dw.com/en/from-ai-fakes-to-cyberattacks-threats-to-german-elections/a-70972702>.
- Denisova, Anastasia. *Internet memes and society: Social, cultural, and political contexts*. New York: Routledge, 2019.
- Denniss, Emily and Rebecca Lindberg. „Social media and the spread of misinformation: infectious and a threat to public health.” *Health Promotion International* 40, No. 2 (2025): 1-10. <https://doi.org/10.1093/heapro/daaf023>.
- Deutschlandfunk. „Die völkischen KI-Memes von ‚Wilhelm Kachel’.” <https://www.deutschlandfunk.de/rechtsextreme-memes-kuenstliche-intelligenz-wilhelm-kachel-propaganda-100.html>.
- Domalewska, Dorota. „Dezinformacja jako zagrożenie dla demokracji i regulacje prawne w zakresie jej przeciwdziałania w Polsce i wybranych krajach europejskich.” *Politeja*, No. 5(92) (2024): 359-379. <https://doi.org/10.12797/Politeja.21.2024.92.16>.
- Dziedzic, Magdalena. „Przeciwdziałanie dezinformacji w kontekście wybranych regulacji Aktu o usługach cyfrowych oraz Aktu o Sztucznej Inteligencji.” *Prawo i Więź*, No. 6(53) (2024): 223-238. <https://doi.org/10.36128/PRIW.VI53.1103>.
- European Commission. *Tackling online disinformation: a European Approach*. Commu-

- nication from the Commission, COM(2018) 236 final, 2018.
- Farid, Hany. „On Algorithmic Amplification.” *Inference* 6, No. 1 (2021). <https://doi.org/10.37282/991819.21.10>.
- Giese, Jeff. „It’s time to embrace memetic warfare.” *Defence Strategic Communications* 1 (2016): 67-75. <https://doi.org/10.30966/2018.RIGA.1.4>.
- Gray, Gavan. „Memetic Narratives in Information Warfare: The Danger of Viral Self-Contamination.” *Hestia Review* 1 (2021): 14-26.
- Hoyle, Aiden, Charlotte Wagnsson, Helma van den Berg, Bertjan Doosje and Martijn Kitzen. „Cognitive and Emotional Responses to Russian State-Sponsored Media Narratives in International Audiences.” *Journal of Media Psychology* 35, No. 6 (2023): 362-374. <https://doi.org/10.1027/1864-1105/a000371>.
- Jackson, Laura. „Revisions of Reality: The Three Warfares – China’s New Way of War.” In *Information at War: From China’s Three Warfares to NATO’s Narratives*, ed. Peter Pomerantsev, 5-15. London: The Legatum Institute, 2015.
- Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.
- Kania, Elsa. „The PLA’s Latest Strategic Thinking on the Three Warfares.” *China Brief* 16, No. 12 (2016): 10-14.
- Keen, Andrew. „Go Fuck Yourself’. On Putin’s Propaganda and the Week in Ukrainian Resistance.” *Literary Hub*. <https://lithub.com/go-fuck-yourself-on-putins-propaganda-and-the-week-in-ukrainian-resistance>.
- Kosmaty, Piotr. „Selected legal aspects of the crime of intelligence disinformation.” *Internal Security Review* 33 (2025): 327-345. <https://doi.org/10.4467/20801335PBW.25.034.22651>.
- Ling, Peter. „One Does Not Simply Upload a Meme – Internet Memes and the Parody Exemption in Europe.” In *Developments and Directions in Intellectual Property Law: 20 Years of The IPKat*, ed. Hayleigh Bosher and Eleonora Rosati, 303-313. Oxford: Oxford University Press, 2023. <https://doi.org/10.1093/oso/9780192864475.003.0019>.
- Łabuz, Mateusz. „Deep fakes and the Artificial Intelligence Act – An important signal or a missed opportunity?” *Policy & Internet* 16, No. 4 (2024): 783-800. <https://doi.org/10.1002/poi3.406>.
- Łabuz, Mateusz. „Memetic Warfare – sind wir bereit für dieses Schlachtfeld?” Tagesspiegel Background Digitalisierung. <https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/memetic-warfare-sind-wir-bereit-fuer-dieses-schlachtfeld>.
- Łabuz, Mateusz and Christopher Nehring. „Information apocalypse or overblown fears – what AI mis- and disinformation is all about? Shifting away from technology toward human reactions.” *Politics & Policy* 52, No. 4 (2024): 874-891. <https://doi.org/10.1111/polp.12617>.
- Łukaszuk, Anna. „‘Whole of Government’ oraz ‘Whole of Society’ – skuteczne działania w budowaniu świadomości i odporności społeczeństwa na zagrożenia

- w przestrzeni informacyjnej – przeciwdziałanie dezinformacji w Polsce.” *Zeszyty Prawnicze* 23, No. 3 (2023): 163-184. <https://doi.org/10.21697/zp.2023.23.3.08>.
- Mahdawi, Arwa. „Humour over rumour? The world can learn a lot from Taiwan's approach to fake news.” *The Guardian*. <https://www.theguardian.com/commentisfree/2021/feb/17/humour-over-rumour-taiwan-fake-news>.
- Maiberg, Emanuel. „AI Slop of Musk and Trump on TikTok Racks Up 700 Million Views.” *404 Media*. <https://www.404media.co/ai-slop-of-musk-and-trump-on-tiktok-racks-up-700-million-views>.
- Maldita. „Memes, football and songs: how ‚Pop Fascism’ paves the way for disinformation.” <https://maldita.es/investigaciones/20251013/memes-songs-disinformation-pop-fascism>.
- Maroń, Grzegorz. „Fact-checking a wolność słowa.” *Radca Prawny. Zeszyty Naukowe*, No. 1(3) (2022): 83-104. <https://doi.org/10.4467/23921943RP.22.007.15809>.
- McCrow-Young, Ally and Mette Mortensen. „Countering spectacles of fear: Anonymous’ meme ‚war’ against ISIS.” *European Journal of Cultural Studies* 24, No. 4 (2021): 832-849. <https://doi.org/10.1177/13675494211005060>.
- Mejova, Yelena, Arthur Capozzi, Corrado Monti and Gianmarco De Francisci Morales. „Narratives of War: Ukrainian Memetic Warfare on Twitter.” *Proceedings of the ACM on Human-Computer Interaction* 9, No. 2 (2025): 1-28. <https://doi.org/10.1145/3711037>.
- Microsoft. *Protecting Election 2024 from foreign malign influence: lessons learned help us anticipate the future*. <https://msblogs.thesourcemediaassets.com/sites/5/2023/11/MTAC-Report-2024-Election-Threat-Assessment-11082023-2-1.pdf>.
- Microsoft. *Same targets, new playbooks: East Asia threat actors employ unique methods*. Redmond: Microsoft, 2024.
- Munk, Tine. *Far-right extremism online. Beyond the fringe*. London: Routledge, 2024.
- Munk, Tine. *Memetic War. Online Resistance in Ukraine*. London: Routledge, 2024.
- Munk, Tine. „Digital Defiance. Memetic Warfare and Civic Resistance.” *European Journal on Criminal Policy and Research* 31 (2025): 501-528. <https://doi.org/10.1007/s10610-025-09613-4>.
- Munk, Tine. Expert interview conducted by the authors of the study on 15 January 2025.
- Muñoz, Katja. „The AI Election Year: How to Counter the Impact of Artificial Intelligence.” *DGAP Memo* 1 (2024): 1-4.
- Ördén, Hedvig. „The neuropolitical imaginaries of cognitive warfare.” *Security Dialogue* 55, No. 6 (2024): 607-624. <https://doi.org/10.1177/09670106241253527>.
- Paziuk, Andrii, Dmytro Lande, Elina Shnurko-Tabakova and Phillip Kingston. „Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict.” *Frontiers in Artificial Intelligence* 8 (2025): 1-16. <https://doi.org/10.3389/frai.2025.1566022>.
- Pennycook, Gordon, Tyrone Cannon and David Rand. „Prior exposure increases

- perceived accuracy of fake news." *Journal of Experimental Psychology: General* 147, No. 12 (2018): 1865-1880. <https://doi.org/10.1037/xge0000465>.
- Petty, Richard and John Cacioppo. „The elaboration likelihood model of persuasion." *Advances in Experimental Social Psychology* 19 (1986): 123-205. [https://doi.org/10.1016/S0065-2601\(08\)60214-2](https://doi.org/10.1016/S0065-2601(08)60214-2).
- Qureshi, Waseem Ahmad. „Information Warfare, International Law, and the Changing Battlefield." *Fordham International Law Journal* 43, No. 3 (2020): 901-938.
- Regina, Gitau. „Meme warfare: How Extremist Groups Weaponize Internet Humor to Normalize Radical Ideologies." Center of Diplomatic Insight. <https://centerfordiplomaticinsight.substack.com/p/meme-warfare-how-extremist-groups>.
- Tajfel, Henri and John Turner. „An integrative theory of inter-group conflict." In *The Social Psychology of Inter-group Relations*, ed. William G. Austin and Stephen Worchel, 33-47. Monterey: Brooks/Cole, 1979.
- Thompson, Stuart. „How Trump Is Using Fake Imagery to Attack Enemies and Rouse Supporters." *The New York Times*. <https://www.nytimes.com/interactive/2025/10/21/business/media/trump-ai-truth-social-no-kings.html>.
- Turner, John, Rupert Brown and Henri Tajfel. „Social comparison and group interest in ingroup favouritism." *European Journal of Social Psychology* 9, No. 2 (1979): 187-204. <https://doi.org/10.1002/ejsp.2420090207>.
- Wiesner, Andrea, Svenja Schäfer and Sophie Lecheler. „Navigating the gray areas of content moderation: Professional moderators' perspectives on uncivil user comments and the role of (AI-based) technological tools." *new media & society* 27, No. 3 (2025): 1215-1234. <https://doi.org/10.1177/14614448231190901>.
- Wiktorek, Mateusz. „Więzienie za mema – ŁĄCZY NAS KARNE z Krzysztofem Krupą i dr. Bohdanem Widłą." *Karne24*. <https://karne24.com/wiezienie-za-mema>.
- Wiśniewski, Adam. „The European Court of Human Rights and Internet-Related Cases." *Białostockie Studia Prawnicze* 26, No. 3 (2021): 109-133. <https://doi.org/10.15290/bsp.2021.26.03.06>.
- Youvan, Douglas. „Memetic Cognition: The Compression of Complexity in the Human Psyche." ResearchGate. https://www.researchgate.net/publication/389278599_Memetic_Cognition_The_Compression_of_Complexity_in_the_Human_Psyche.

