sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXXI No 1 2025

COGNITIVE WARFARE IN THE DIGITAL AGE: IMPLICATIONS FOR EU SECURITY POLICY

Lorina ARITON

National Defence University "Carol I", Bucharest, Romania
lorinaariton@yahoo.com

Abstract: *Cognitive warfare, understood as the deliberate deployment of informational and psychological operations to influence human perception and decision-making, has emerged as a threat within the European Union's (EU) security environment. This article contributes to the conceptual clarity of Cognitive Warfare by analyzing how it is framed and addressed across EU policy frameworks and institutional narratives. Findings reveal increasing institutional awareness, as reflected in instruments like the Strategic Compass and the Digital Services Act. Yet, challenges persist, including fragmented responses, weak civil–military coordination, and vulnerability to AI-driven disinformation. The article advocates for an integrated cognitive security strategy built on democratic resilience, regulatory foresight, and intersectoral cooperation, emphasizing the need for continued research on ethical and anticipatory governance.*

Keywords: Cognitive Warfare, Disinformation, EU Security Policy, Influence Operations, Artificial Intelligence

1. Introduction

Cognitive warfare has emerged as a defining threat in the digital security environment, targeting perceptions and emotions rather than infrastructure. Described by NATO as a war "fought not with bombs and missiles, but with lies and manipulation," it aims to undermine democratic cohesion from within [29]. Rooted in traditional propaganda, its reach has been magnified by digital platforms, enabling disinformation to serve as a cornerstone of hybrid threats and foreign information manipulation and interference (FIMI) [7]. Russia's campaigns during the war in Ukraine exemplify this approach, combining cyber operations with strategic influence to exploit societal divisions [29, 15]. The rise of artificial intelligence has significantly intensified these dynamics. Generative AI now powers adaptive, scalable operations using tools like deepfakes, bots, sentiment analysis, and network mapping [15]. These techniques support highly personalized, persistent influence, a phenomenon Floridi (2023) terms "hypersuasion". In response, the EU is advancing regulations such as the AI Act and the Digital Services Act, which aim to align security measures with democratic safeguards [10]. AI tools play both offensive and defensive roles. While hostile actors deploy affective computing, psychographic targeting, and algorithmic manipulation to sow discord [6], EU institutions utilize similar technologies for detection and response. Initiatives like WeVerify, SocialTruth, and vera.ai assist journalists and analysts in identifying manipulation patterns [15], while ENISA

DOI: 10.2478/kbo-2025-0001

and NATO's StratCom COE apply sentiment and network analysis for early threat identification [16, 30]. Emotion recognition and biometric targeting have raised ethical concerns, prompting precautionary bans in sensitive domains [8], [25]. Institutionally, the EU integrates regulation, strategic communication, and cross-sectoral cooperation. EEAS coordinates FIMI responses, while cybersecurity and defense agencies incorporate cognitive threats into broader frameworks [11]. The Strategic Compass identifies information manipulation as a core hybrid threat, prompting the development of a comprehensive counter-FIMI toolbox and coordinated transatlantic efforts [13, 21].

As NATO now considers the cognitive domain an operational arena requiring defensive innovation, the convergence of psychological and technological tools compels the EU to rethink its security posture [26, 29]. This article investigates these emerging challenges, focusing on how AI-enhanced cognitive warfare is reshaping EU strategic priorities and driving the development of new policy instruments to protect democratic integrity.

2. Cognitive Warfare as a Strategic Threat Assessment

The European Union increasingly views cognitive warfare as a critical component of hybrid threats to democratic resilience. The Strategic Compass identifies foreign information manipulation and interference (FIMI) as a strategic concern, calling for the development of a comprehensive countermeasures' toolbox [11]. The European External Action Service (EEAS) echoes this view, warning of disinformation's corrosive effects on trust and democratic discourse, with High Representative Josep Borrell describing it as a form of strategic aggression [13]. NATO has adopted a similar position, with its 2022 Strategic Concept and Allied Command Transformation designating cognitive warfare as a distinct operational domain requiring targeted responses [29]. Artificial intelligence has transformed influence operations, enabling scalable and adaptive manipulation through tools such as deepfakes, bots, and generative language models [6]. The spread of synthetic media, exemplified by a fake video of President Zelenskyy during the Ukraine conflict, underscores the operational risks of AI-enabled deception [28]. Beyond isolated incidents, AI facilitates mass personalization of persuasive content, complicating attribution and accelerating disinformation [18, 13].

However, the EU's response is constrained by institutional fragmentation, legal limitations, and technological dependencies. Counter-cognitive efforts remain dispersed across various bodies, with mechanisms like the Rapid Alert System lacking integration into a unified doctrine [26, 9]. Legal safeguards for expression and privacy hinder preemptive interventions, while reliance on non-EU platforms creates enforcement asymmetries [10, 32]. The rapid evolution of generative AI continues to outpace detection capabilities [36].

Societal vulnerabilities—such as polarization, low media literacy, and eroding trust—further weaken resilience. Adversaries exploit these divides to destabilize cohesion, particularly during crises [13]. While the EU has taken important steps to address cognitive threats, it must enhance coordination, technological preparedness, and civic awareness to effectively counter AI-driven influence operations.

3. Methodology

This study applies a qualitative content analysis to examine how cognitive warfare and AI-enabled influence operations are framed within EU security discourse. Given the emergent and interdisciplinary nature of cognitive warfare, which lacks a clear definition in policy and academic contexts,

a qualitative approach enables exploratory, interpretive analysis rather than hypothesis testing [8]. The method allows systematic coding of texts to uncover latent narratives, a technique well-established in security studies for dissecting complex or ambiguous concepts like hybrid threats [23].

Designed as a cross-sectional and comparative study, the research focuses on interpreting meaning from a carefully selected corpus of texts—such as strategic documents and expert commentary—rather than quantifying events. This design prioritizes depth, examining how cognitive warfare is articulated and addressed across contexts, which is critical for analyzing a threat that operates at the level of perception and influence [6]. The qualitative design aligns with the goal of mapping how EU actors conceptualize and respond to this evolving domain.

3.1. Data Collection and Sources

The dataset comprises 30 purposefully sampled sources published between 2015 and early 2025, covering EU and NATO policy documents, strategic assessments, academic articles, and practitioner commentaries. Key EU sources include strategy papers from the European Commission, EEAS, and European Council. NATO's Allied Command Transformation publications were included due to NATO's doctrinal influence on EU security policy [26]. Think tank reports and training course material—such as a 2024 pilot course describing the mind as the battlefield—add practitioner perspectives [27].

Documents were selected using keyword-based searches focused on "cognitive warfare", "disinformation", and "AI in security", with attention to relevance for EU or transatlantic policy. The final corpus balances official institutional perspectives with critical academic voices. It includes doctrinal frameworks, case studies of AI-enabled disinformation, and legal-ethical assessments. All sources were drawn from reputable and verifiable outlets, ensuring a credible empirical foundation for the qualitative analysis.

3.2. Analytical Framework

The directed content analysis employed a coding scheme targeting four main dimensions: (1) threat framing, (2) AI tools, (3) policy and institutional responses, and (4) doctrinal evolution. Initial codes were based on sensitizing concepts from the literature and refined inductively. Each document was coded line-by-line to identify language framing cognitive warfare as, for example, a "battle for the mind" or "propaganda 2.0", with particular attention to metaphors and narratives used in policy documents [26, 27].

AI was analyzed both as a threat vector (e.g., deepfakes, algorithmic manipulation) and as a defensive asset. For instance, instances where AI-generated content incited hate or confused voters during elections were flagged as key threat narratives [36]. Conversely, proposals to use AI for content detection and strategic communication were coded as institutional countermeasures [26]. This dual coding approach captures AI's complex role as both enabler and mitigator of cognitive threats.

We also coded for references to concrete responses—e.g., new units, education campaigns, or legislative initiatives—categorizing them under capacity-building, legal regulation, or international cooperation. Notably, EU sources often emphasized democratic values and societal resilience as core elements of their approach [24]. The framework allowed us to assess the coherence between threat narratives and strategic responses, and to identify gaps where rhetoric may outpace policy action.

To enhance rigor, coding consistency was maintained across documents and supplemented with modest quantification—e.g., noting how many documents employed specific frames [23]. This helped differentiate dominant from marginal narratives and supported the credibility of interpretive insights. Beyond the initial framework, several emergent themes were

inductively coded and incorporated into the analysis. These included the fragmentation of media governance within the EU, national disparities in threat perception and response capacity, legal and ethical constraints on disinformation regulation, technological asymmetries between democratic and authoritarian actors, and the uneven development of societal cognitive resilience. While the approach is qualitative and interpretive in nature, modest quantification was applied to assess the relative prominence of these themes across the corpus. This facilitated the estimation of proportional weights for each category as visualized in the Figure 1: policy and institutional responses (15%), AI as a threat vector (14%), threat framing (12%), and so on.

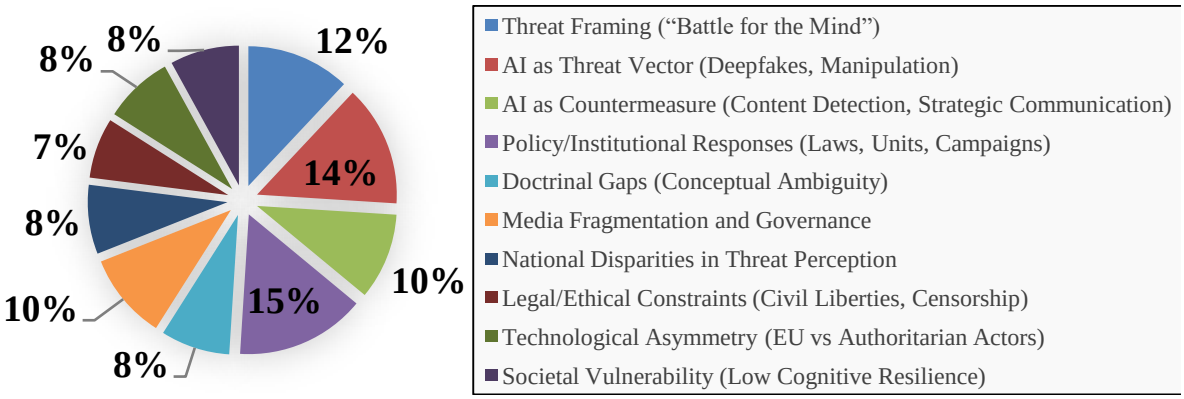

Figure 1: Discursive and Strategic Emphases in EU Cognitive Warfare Policy (2015–2025)

The findings suggest that EU strategic discourse places greatest emphasis on institutional responses—such as legislation, capacity-building, and public awareness campaigns—followed closely by concerns about AI-enhanced threats. The role of AI as a defensive asset, as well as structural vulnerabilities like media fragmentation and public susceptibility to disinformation, receive less consistent attention. These results reflect a discourse that prioritizes formal mechanisms of response, while still grappling with conceptual ambiguity and evolving technological dynamics. The chart thus provides a synthesized visual representation of the dominant and emerging narratives that characterize the EU’s evolving approach to cognitive warfare and information security.

3.3. Addressing Bias and Limitations

As with all qualitative research, this study has limitations. The corpus primarily reflects EU and allied perspectives, potentially reinforcing a securitized narrative centered on state-based threats, particularly Russia [26], while non-Western views remain underrepresented. The analysis is interpretive in nature and lacks intercoder reliability testing, though definitions were clarified and all claims grounded in direct textual evidence.

The conceptual ambiguity of “cognitive warfare”, which overlaps with propaganda, cyber, and psychological operations, further complicates coding [6]. Emphasis was placed on content explicitly referencing cognitive or influence dimensions. Additionally, the study examines institutional discourse and policy intent, not the measurable impact of operations—an important distinction, as some studies suggest limited real-world effects from AI-generated disinformation [36].

Although the rapid evolution of AI may render some insights quickly outdated, the inclusion of sources through 2025 ensures

the findings reflect current trends in EU strategic thinking. Overall, the methodology offers a credible foundation for tracing how cognitive threats are conceptualized and addressed in EU security discourse.

4. Challenges and Vulnerabilities

The European Union's open information environment, while central to its democratic identity, also exposes it to key vulnerabilities in the context of cognitive warfare. Fragmented media governance across member states enables disinformation to transcend borders, while policy responses remain inconsistent and largely national in scope. EU digital policy has oscillated between securitization and voluntary cooperation with tech platforms, leading to a fragmented defense posture [5]. The absence of a unified legal framework on disinformation until recently further undermined collective resilience [14].

A major challenge is the disparity in threat perception and response capacity across the EU. While Finland has adopted proactive measures due to past exposure to Russian influence operations, others like Austria remain more neutral, weakening coordinated action [35]. Initiatives such as the Rapid Alert System have seen limited uptake due to low trust among member states [2].

Legal and ethical constraints also complicate regulation, as disinformation often falls outside the scope of existing legal prohibitions. AI-driven moderation tools have raised civil liberties concerns, and although the Digital Services Act aims to balance transparency with freedom of expression, implementation remains slow and uneven [26, 14].

Technological asymmetry further impairs EU readiness. Authoritarian actors face fewer constraints and exploit AI-driven tools—such as bots and deepfakes—more rapidly than the EU can respond [2]. Meanwhile, reliance on non-European tech companies limits enforcement capabilities.

Finally, societal cognitive resilience remains weak. Varying levels of media literacy and declining trust in traditional media increase susceptibility to manipulation [35]. Although education initiatives exist, their implementation is patchy [14], and social media polarization continues to amplify vulnerabilities, as seen during crises such as the COVID-19 pandemic and the war in Ukraine [4].

Collectively, the EU's cognitive security is undermined by fragmented governance, asymmetrical capacities, and limited public resilience. Addressing these requires an integrated strategy that aligns regulation, reinforces institutional coordination, and invests in societal awareness [4, 35].

5. Policy Recommendations

To address the strategic threat of cognitive warfare, the European Union must establish a dedicated cognitive defense doctrine. While current efforts fall under broader hybrid threat frameworks, a specialized doctrine would define operational roles, ethical boundaries, and coordination procedures tailored to cognitive security [19, 17]. NATO's recognition of cognitive warfare further emphasizes the urgency of formalizing the EU's approach [6]. This doctrine must uphold democratic principles, ensuring that countermeasures respect freedom of expression and privacy [24], and should serve as a roadmap for coherent policy and resource allocation [1].

Cognitive threats transcend civil-military divides, requiring integrated monitoring and response systems. The EU should enhance cooperation between intelligence services, military units, and civilian agencies such as EEAS StratCom. Existing bodies like INTCEN could be expanded into a joint information-sharing and analysis center [34, 17]. Joint monitoring initiatives and scenario-based exercises—such as Integrated Resolve—can strengthen operational readiness across sectors [3].

Strengthening societal resilience is equally crucial. A digitally literate and critically

aware public remains the best defense against manipulation. EU-backed programs such as the Digital Education Action Plan and "Media Literacy for All" should be scaled and standardized across member states [17, 5]. Cross-border educational initiatives and national curriculum integration would help reduce susceptibility to disinformation.

Given the role of technology in modern influence campaigns, the EU must invest in detection tools and enforce digital accountability. AI-powered systems to identify disinformation and algorithmic manipulation should be prioritized. Legislation such as the Digital Services Act and the updated Code of Practice on Disinformation create a foundation for regulating platforms [22]. Ensuring compliance through algorithm audits and promoting transparency are essential [5]. An independent EU observatory could enhance real-time monitoring and cross-linguistic threat detection [1].

A rapid response mechanism is also imperative. The Rapid Alert System, established in 2019, should be enhanced with a permanent task force capable of coordinating fact-checking and counter-narratives across institutions [17]. Regular simulation exercises and faster briefings to policymakers and journalists can improve response speed. Recent successes, such as the EU's rebuttal efforts during the Ukraine conflict, demonstrate the value of such agility [33, 5].

Each recommendation is mutually reinforcing. A formal doctrine offers strategic clarity; civil-military integration enhances preparedness; education builds resilience; regulation imposes costs on malicious actors; and rapid response mechanisms minimize impact. Together, these elements form a holistic strategy that can future-proof the EU against evolving cognitive threats [20].

6. Conclusions

This study used qualitative content analysis of policy, academic, and institutional sources to examine the growing strategic relevance of cognitive warfare and AI-enhanced influence operations. Defined by the deliberate manipulation of perception and decision-making, cognitive warfare is now considered a legitimate domain of conflict, with NATO warning that "the human mind is becoming the battlefield of tomorrow" [37]. Adversaries such as Russia and China increasingly exploit AI tools to amplify propaganda and erode public trust, as seen in disinformation campaigns surrounding the war in Ukraine [8, 17]. The expanding reach and sophistication of these operations underline the need to treat cognitive security as a strategic priority [6].

The EU has responded by combining regulatory, informational, and institutional measures. Since 2015, bodies like the EEAS and EUvsDisinfo have worked to expose foreign manipulation, while the 2018 Action Plan and 2019 Rapid Alert System enhanced coordination [12, 9]. Legislative tools such as the Digital Services Act and Code of Practice aim to increase platform accountability [22], and EU strategy emphasizes democratic resilience, media literacy, and cooperative action with NATO [1, 5].

Nonetheless, substantial challenges persist. Legal protections around speech and privacy constrain proactive interventions [26], and fragmented national capabilities hinder cohesive responses [24]. Rapid AI advances and attribution difficulties further complicate timely detection and countermeasures [20].

To address these gaps, cognitive security should be institutionalized within major EU frameworks like the Strategic Compass and CSDP. A unified doctrine would enable coordinated threat assessments and responses while upholding transparency and public trust [17]. Strengthening digital literacy, intelligence-sharing, and NATO cooperation—as well as developing

deterrents like sanctions—will be essential [34]. As cognitive warfare evolves, its implications—from election interference to wartime deception—require a proactive and unified EU approach. Operationalizing cognitive resilience alongside cyber defense will be critical to preserving democratic integrity and strategic autonomy in an increasingly contested information space.

References

[1] Bond, I., Scazzieri, L. Europe's new defence ambitions. London: Centre for European Reform; 2022. Available from: https://www.cer.eu/publications/archive/policy-brief/2022/europes-new-defence-ambitions [cited 2025 May 23].

[2] Brattberg E, Maurer T. Russian election interference: Europe's counter to fake news and cyber-attacks [Internet]. Washington (DC): Carnegie Endowment for International Peace; 2018. Available from: https://carnegieendowment.org/research/2018/05/russian-election-interference-europes-counter-to-fake-news-and-cyber-attacks.

[3] Buvarp M. AI-driven influence operations and democratic security [Internet]. Riga: NATO Strategic Communications Centre of Excellence; 2024. Available from: https://stratcomcoe.org/publications [cited 2025 May 23].

[4] Cao G, Duan Y, Edwards JS, Dwivedi YK. Understanding managers' attitudes and behavioral intentions towards using artificial intelligence for organizational decision-making. Technovation. https://doi.org/10.1016/j.technovation.2021.102312.

[5] Casero-Ripollés A, Tuñón J, Bouza-García L. The European approach to online disinformation: geopolitical and regulatory dissonance. Palgrave Commun. 2023; 10:657.

[6] Claverie B, du Cluzel F. Cognitive warfare [Internet]. NATO Innovation Hub; 2021 [cited 2025 May 23]. Available from: https://www.innovationhub-act.org/cognitive-warfare.

[7] Deppe C, Schaal GS. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Front. Big Data. 2024; 7: https://doi.org/10.3389/fdata.2024.1452129.

European Commission. Action Plan against Disinformation [Internet]. Brussels: European Commission; 2018 Available from: https://commission.europa.eu/publications/action-plan-against-disinformation-communication-commission_en. [cited 2025 May 23].

[8] European Commission. AI Act – Proposed Regulation on Artificial Intelligence [Internet]. Brussels: European Commission; 2024 Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 [cited 2025 May 20].

[9] European Commission. European Democracy Action Plan [Internet]. Brussels: European Commission; 2020 Available from: https://ec.europa.eu/commission/presscorner/detail/en/ FS_20_1057 [cited 2025 May 23]

[10] European Commission. Guidance on strengthening the Code of Practice on Disinformation [Internet]. Brussels: European Commission; 2021 Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0262:contentReference[oaicite:0]{index=0} [cited 2025 May 23].

[11] Council of the European Union. Strategic Compass for Security and Defence [Internet]. Brussels: Council of the EU; 2022 Available from: eeas.europa.eu. [cited 2025 May 23].

[12] European External Action Service (EEAS). EUvsDisinfo database [Internet]. 2021 Available from: https://euvsdisinfo.eu:contentReference[oaicite:2]{index=2} [cited 2025 May 20].
[13] European External Action Service (EEAS). Foreign information manipulation and interference – EEAS press release on COVID-19 disinformation [Internet]. Brussels: European External Action Service; 2023 Available from: https://www.eeas.europa.eu/eeas/foreign-information-manipulation-and-interference-threats-1st-eeas-technical-report_en [cited 2025 May 23].
[14] European Court of Auditors. Our activities in 2021: annual activity report of the European Court of Auditors. Luxembourg: Publications Office of the European Union; 2022. Available from: https://www.eca.europa.eu/en/publications/AR-2022 [cited 2025 May 20].
[15] European Digital Media Observatory (EDMO). Annual reports and research outputs [Internet]. 2020 Available from: https://edmo.eu/edmo-reports-and-outputs [cited 2025 May 20].
[16] European Union Agency for Cybersecurity (ENISA). Publications [Internet]. Luxembourg: Publications Office of the European Union; [n.d.] Available from: https://www.enisa.europa.eu/publications [cited 2025 May 20].
[17] European Parliament. Resolution on foreign interference in all democratic processes in the European Union, including disinformation [Internet]. Brussels: European Parliament; 2023 Available from: eur-lex.europa.eu. [cited 2025 May 30].
[18] Floridi L. Hypersuasion in the age of AI. Philos Technol. 2023; 36(3):47–58.
[19] Giannopoulos G, Smith H, Theocharidou J. The landscape of hybrid threats: a conceptual model. Luxembourg: Publications Office of the EU; 2020.
[20] Glasser H, Rickli A, Mantellassi M. Mapping cognitive attacks in the EU: challenges and opportunities. Helsinki: Hybrid Centre of Excellence; 2023.
[21] Green, Y., Gully, A., Roth, Y., Roy, A., Tucker, J. A., Wanless, A., Evidence-based misinformation interventions: Challenges and opportunities for measurement and collaboration. Washington, DC: Cargengie Endowment for International Peace 2023; 9. Available from: https://www.gisf.ngo/wp-content/uploads/2023/01/202212Wanless_et_al_MisinfoInterventions2.pdf
[cited 2025 May 23].
[22] Goujard C. EU's disinformation crackdown collides with platform cuts [Internet]. Politico Europe; 2023 Mar 3. Available from: https://www.politico.eu/article/eu-brussels-ban-tiktok-europe-has-questions/ [cited 2025 May 20].
[23] Janičatová S, Mlejnková P. The ambiguity of hybrid warfare: a qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities. Contemp Secur Policy. 2021; 42(1):1–33.
[24] Karami A, Dastenaei AM. The European Union's approach to cognitive warfare's command and control. J Electr Syst. 2024; 11(s):2721–2734 Available from: journal.esrgroups.org [cited 2025 May 23].
[25] Klemm N. Political AI and regulatory challenges in Europe. London: Centre for Data Ethics and Innovation; 2024.
[26] Lahmann H. European security and the threat of 'cognitive warfare' [Internet]. Verfassungsblog; 2024 Nov 3 Available from: verfassungsblog.de [cited 2025 May 23].
[27] McCreight R. The war inside your mind: unprotected brain battlefields and neuro-vulnerability. Academia Biol. 2024; 2(1).

[28] Mozur P, Zhong R. A deepfake of Zelenskyy was amplified on social media [Internet]. The New York Times; 2023 Mar 16. Available from: https://www.nytimes.com [cited 2025 May 23].
[29] NATO. NATO 2022 Strategic Concept [Internet]. Brussels: NATO Public Diplomacy Division; 2022 Available from: act.nato.int [cited 2025 May 23].
[30] NATO StratCom COE. Countering AI-enhanced disinformation. Riga: NATO Strategic Communications Centre of Excellence; 2022.
[31] Johns Hopkins University; Imperial College London. Countering cognitive warfare: awareness and resilience [Internet]. NATO Review Magazine; 2021 May 20 Available from: nato.int [cited 2025 May 23].
[32] Osadchuk, R. AI tools usage for disinformation in the war in Ukraine [Internet]. DFRLab – Atlantic Council; 2024 Jul 9 Available from: dfrlab.org [cited 2025 May 20].
[33] Pamment, J. Resilience to information influence: a policy framework. Riga: NATO Strategic Communications Centre of Excellence; 2020.
[34] Reding, V., Wells, E. Digital sovereignty and cognitive resilience. Eur View. 2022; 21(2):101–111.
[35] Pichler, D. Disinformation and foreign interference: a challenge for the EU and its Member States [Internet]. Vienna: Austrian Society for European Politics (ÖGfE); 2024 Jun 6 Available from: https://www.oegfe.at/policy-briefs/disinformation-and-foreign-interference-a-challenge-for-the-eu-and-its-member-states/?lang=en [cited 2025 May 23].
[36] Stockwell, S. AI-enabled influence operations: threat analysis of the 2024 UK and European elections [Internet]. London: Alan Turing Institute; 2024. Available from: https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-threat-analysis-2024-uk-and-european-elections [cited 2025 May 23].
[37] Van der Klaauw, C. The 21st-Century Game Changer: Cognitive Warfare, 2023 Available from: https://www.jwc.nato.int/application/files/7216/9804/8564/CognitiveWarfare.pdf [cited 2025 May 23].