Marco Marsili Associate Researcher at the Centre for International Studies (CEI-Iscte), Iscte - University Institute of Lisbon.

EUROPE'S COGNITIVE SECURITY: GENERATIVE AI, HYBRID CONFLICT AND DEMOCRATIC RESILIENCE

27 April 2026

The spread of generative AI, hybrid conflict and foreign information manipulation is reshaping the European security environment. The European Union is responding by moving beyond a narrow counter-disinformation approach towards a broader concept of cognitive security. Yet major gaps remain in enforcement, strategic coherence and democratic resilience.

The European Union is moving from a narrow focus on disinformation towards a broader concept of cognitive security. Russia's hybrid strategies, generative artificial intelligence (AI) and the vulnerabilities of platform ecosystems have turned information integrity into a strategic issue. The EU has built an important regulatory and institutional toolbox, but major gaps remain in enforcement, resilience and strategic coherence.

The European Union no longer faces disinformation as a peripheral communication problem, but as a structural challenge to democratic resilience, strategic autonomy and the integrity of decision-making (Marsili, 2025a; Marsili, 2025b; EPRS, 2025a). What has changed in recent years is not only the persistence of influence operations, which have long accompanied geopolitical competition, but their acceleration through platform ecosystems, synthetic media and generative artificial intelligence (Marsili, 2021; Marsili, 2023; EPRS, 2025a). The result is a denser and more unstable information environment in which hostile actors can manipulate narratives, imitate trusted sources and scale persuasive deception at lower cost and higher speed than in the past (Wardle and Derakhshan, 2017; EPRS, 2025a; EEAS, 2026).

Russia's war against Ukraine made this transformation impossible to ignore (Marsili, 2025b: 26-28; NATO, 2026). It showed that hybrid conflict operates across military and non-military domains at once, combining kinetic action with cyber operations, economic coercion, information manipulation and political interference (Marsili, 2025b: 24-31; NATO, 2026). At the same time, the spread of generative AI has widened the range of actors able to produce deceptive content, from state agencies and proxy networks to private opportunists and platform-native influence brokers (EPRS, 2025a; Marsili, 2025c). The EU is therefore being pushed towards a broader concept that may be described as cognitive security: the protection of the informational and psychological conditions required for free judgement, democratic participation and institutional trust (Marsili, 2023; Marsili, 2025a; NATO, 2026).

> Contemporary influence campaigns often do more than spread falsehoods: they saturate the information space, exploit emotional polarisation, imitate legitimate media and shape perceptions before verification mechanisms can respond.

From disinformation to cognitive security

The conceptual shift matters. Traditional counter-disinformation policies were largely designed to identify false claims, support fact-checking and reduce the visibility of manipulative content (Wardle and Derakhshan, 2017; Marsili, 2025a). Yet contemporary influence campaigns often do more than spread falsehoods: they saturate the information space, exploit emotional polarisation, imitate legitimate media and shape perceptions before verification mechanisms can respond (EPRS, 2025a; EEAS, 2026). In this sense, the target is not only truth, but attention, trust and the cognitive ability to distinguish signal from noise (Wardle and Derakhshan, 2017; Marsili, 2023).

This broader understanding is consistent with the North Atlantic Treaty Organisation (NATO) description of hybrid threats, which combine military and non-military, covert and overt means, including disinformation, cyber-attacks, economic pressure and irregular methods, in order to blur the line between war and peace and destabilise societies (NATO, 2026). NATO also stresses that what is new is the speed, scale and intensity of such attacks, facilitated by technological change and global interconnectivity (NATO, 2026). That formulation closely matches the evolution described in the literature on hybrid warfare and cognitive influence, where the novelty lies less in the existence of propaganda than in its amplification through digital infrastructures and human-machine interaction (Marsili, 2023; Giles, 2016).

The notion of cognitive warfare helps explain this evolution. In *Guerre à la Carte*, cognitive warfare is linked to the attempt to alter perception, judgement and behaviour through the convergence of cyber-influence, information operations and psychological targeting (Marsili, 2023: 108-113). The problem is especially acute in peacetime, because its main effects are political and social rather than battlefield-centric (Marsili, 2023: 110-116). The European Parliament's research service reaches a similar conclusion from a policy perspective, arguing that generative AI is making information manipulation cheaper, faster, more persuasive and harder to detect (EPRS, 2025a).

Russia, Ukraine and the European theatre

The current European debate cannot be separated from Russia's long investment in influence operations (Marsili, 2021; EEAS, 2026). Russian strategy has treated information operations as an instrument

for shaping public opinion, decision-making and geopolitical alignment across its contested neighbourhood (Marsili, 2021: 151-159). That strategy aimed not merely to persuade, but to constrain sovereignty, fragment target societies and hinder Euro-Atlantic integration in states such as Ukraine and Georgia (Marsili, 2021: 157-160; Giles, 2016).

The war in Ukraine exposed how deeply these practices had become embedded in a wider hybrid repertoire (Marsili, 2025b: 26-31; NATO, 2026). The invasion of 2022 revealed vulnerabilities in European crisis governance and intensified cooperation with NATO, especially in cyber defence, energy resilience and counter-disinformation measures (Marsili, 2025b: 29-35). The same conflict also became a laboratory for AI-enhanced manipulation, including deepfake content, impersonation of media brands, synthetic audio and false narratives designed to erode support for Ukraine inside European democracies (EPRS, 2025a; EEAS, 2025).

A European Parliamentary Research Service (EPRS) briefing offers especially strong evidence on this point. It notes that pro-Russian campaigns have used generative AI to imitate organisations, falsify audiovisual evidence and launder deceptive narratives through apparently legitimate intermediaries (EPRS, 2025a). It also warns that information laundering and data poisoning can feed manipulated narratives into AI systems themselves, thereby contaminating downstream outputs and normalising falsehoods through chatbot interactions (EPRS, 2025a). This matters because the architecture of manipulation is no longer limited to social media virality; it now increasingly passes through search, recommendation systems and conversational interfaces (EPRS, 2025a; Stanford HAI, 2025).

FIGURE 1. FROM DISINFORMATION TO COGNITIVE SECURITY IN EUROPE (2022-2026)
Source: Marsili (2025b); EPRS (2025a); EEAS (2025); European Commission (2026); EEAS (2026); NATO (2026).
Notes: EPRS = European Parliamentary Research Service; EEAS = European External Action Service; FIMI = Foreign Information Manipulation and Interference.

YEAR	DEVELOPMENT	STRATEGIC MEANING
2022	Russia's full-scale invasion of Ukraine	Hybrid conflict and information manipulation become central to EU security thinking
2025	EPRS briefing on information manipulation in the age of generative AI	EU institutions frame AI-enabled manipulation as a democratic and strategic challenge
	3rd EEAS FIMI threat report	Foreign information manipulation is treated as a persistent transnational threat
2026	European Commission AI Act implementation framework	Trustworthy AI and transparency obligations move closer to democratic protection
	4th EEAS FIMI annual report	EU monitoring capacity on manipulation networks becomes more structured
	NATO update on countering hybrid threats	Cognitive and informational resilience remains tied to collective defence

FIGURE 2. EU INSTRUMENTS RELEVANT TO COGNITIVE SECURITY
Source: EPRS (2025a); European Commission (2026); EEAS (2025); EPRS (2025b).

INSTRUMENT	MAIN FUNCTION	RELEVANCE TO COGNITIVE SECURITY	MAIN LIMITATION
AI Act	Transparency duties for AI interaction and synthetic content; framework for trustworthy AI	Addresses deepfakes, manipulative techniques and democratic autonomy	Effectiveness depends on implementation and enforcement
Digital Services Act (DSA)	Systemic risk assessment and mitigation duties for very large platforms and search engines	Links platform governance to civic discourse and electoral integrity	Relies on robust supervisory capacity and platform compliance
EEAS FIMI reporting	Mapping foreign information manipulation and interference networks	Supports attribution, pattern recognition and strategic awareness	Limited direct coercive power by itself
European Democracy Shield (EDS)	Political framework for democratic resilience and counter-interference	Pushes information integrity closer to the centre of EU policy	Still politically and institutionally evolving

The EU toolbox

The EU has not remained passive. It has gradually assembled a mixed toolbox that combines regulation, platform obligations, foreign interference monitoring and resilience-building (EPRS, 2025a; European Commission, 2026; EEAS, 2025) – *Figure 1* and *Figure 2*. The 2025 EPRS briefing identifies the main pillars relevant to AI-enabled manipulation as the Artificial Intelligence Act, the Digital Services Act (DSA), the Code of Conduct on Disinformation and the European Media Freedom Act (EPRS, 2025a).

The AI Act is especially important because it introduces transparency duties for AI systems that interact with humans and for systems that generate or manipulate image, audio or video content, including deepfakes (European Commission, 2026; EPRS, 2025a). The Commission presents the AI Act as the EU's legal architecture for trustworthy AI, while the EPRS briefing underlines that manipulative or deceptive techniques that materially distort behaviour and impair informed decision-making are directly relevant to democratic protection (European Commission, 2026; EPRS, 2025a). In other words, the EU is beginning to recognise that the challenge is not only technological safety, but democratic autonomy (EPRS, 2025a).

The Digital Services Act complements this framework by imposing systemic risk obligations on very large online platforms and search engines (EPRS, 2025a). The Parliament briefing notes that such services must assess and mitigate risks affecting civic discourse, electoral integrity, public security and fundamental rights, and that recommended mitigation measures include the labelling of AI-generated content and the adaptation of platform rules to generative AI risks (EPRS, 2025a). This is a major step, because the information crisis is inseparable from platform design, recommendation logics and monetisation incentives (Wardle and Derakhshan, 2017; EPRS, 2025a).

The external dimension is equally relevant. The European External Action Service (EEAS) has progressively developed the report on Foreign Information

Manipulation and Interference (FIMI) as a tool for mapping the infrastructure of foreign information manipulation and interference, especially by Russia and, in specific contexts, China (EEAS, 2025; EEAS, 2026). That matters because cognitive security cannot be reduced to content moderation alone; it requires attribution, pattern recognition, exposure of networks and coordination across diplomacy, security and digital policy (EEAS, 2026; NATO, 2026).

Limits and contradictions

Despite this progress, the EU still lacks full strategic coherence (Marsili, 2025b: 35-57; EPRS, 2025a). One problem is fragmentation: regulation, platform governance, intelligence analysis, electoral protection and strategic communication often remain institutionally separated (Marsili, 2025b; EPRS, 2025a). Another is asymmetry: authoritarian actors can experiment rapidly, while democratic institutions move more slowly, constrained by legality, transparency and internal pluralism (Giles, 2016; NATO, 2026).

There is also a deeper contradiction within the European model. The Union seeks to defend an open information space while relying heavily on private digital infrastructures whose business models often reward engagement, outrage and hyper-personalisation (Wardle and Derakhshan, 2017; EPRS, 2025a). The same technologies that enable creativity and efficiency can also facilitate deception, identity fraud, hallucination and persuasive manipulation at scale, as recent work on generative AI has shown (Marsili, 2025c; Stanford HAI, 2025). The concentration of frontier AI development in a relatively small number of firms reinforces this structural vulnerability (Stanford HAI, 2025).

A further difficulty concerns enforcement and societal resilience. Legal transparency rules are necessary, but labels alone do not neutralise manipulative content once it has circulated widely (EPRS, 2025a). Nor can democratic resilience rely only on fact-checking after the fact, since deceptive audiovisuals often travel faster and leave a stronger impression than later corrections (Wardle and Derakhshan, 2017; EPRS, 2025a). This is why the issue increasingly shifts from content authenticity to civic preparedness, media literacy, institutional credibility and the protection of the conditions under which citizens can still exercise reflective judgement (Marsili, 2025a; Wardle and Derakhshan, 2017).

What comes next

For the EU, cognitive security should not become a pretext for paternalism or for the vague securitisation of all digital communication (EPRS, 2025a). If framed too broadly, it risks diluting legal precision and undermining the very freedoms it seeks to protect (EPRS, 2025a). But if framed too narrowly as a problem of fake content, it misses the systemic convergence of AI, platform power, foreign interference and democratic vulnerability (EEAS, 2026; EPRS, 2025a).

A more credible European approach would rest on four priorities. First, stronger integration between digital regulation and security analysis, especially between DSA enforcement, AI Act implementation and FIMI monitoring (European Commission, 2026; EEAS, 2026). Second, investment in detection, attribution and public warning capabilities able to identify coordinated manipulation before it shapes mass perceptions (EEAS, 2026; NATO, 2026). Third, closer EU-NATO cooperation on resilience, strategic communications, cyber defence and hybrid threat awareness, an area that NATO already treats as central to collective defence (NATO, 2026). Fourth, stronger support for democratic robustness at the societal level, including trusted media ecosystems, civic education and protection against targeted synthetic abuse (Wardle and Derakhshan, 2017; EPRS, 2025a).

The European Democracy Shield (EDS) points in this direction. The initiative under discussion in the European institutional arena places information integrity, democratic resilience and counter-interference mechanisms closer to the centre of EU action (EPRS, 2025b). Yet its success will depend less on declaratory ambition than on whether Europe can align law, technology, public institutions and strategic culture around a shared understanding of cognitive vulnerability (EPRS, 2025a; EEAS, 2026).

The EU has already recognised that hybrid conflict is no longer confined to borders, battlefields or cyber infrastructure (Marsili, 2025b; NATO, 2026). The next step is to recognise with equal clarity that democracy itself depends on cognitive conditions that can now be strategically targeted, industrially amplified and algorithmically personalised (Marsili, 2023; EPRS, 2025a). In that sense, cognitive security is not an alternative to democratic openness, but one of its new conditions of possibility (Marsili, 2025a; EPRS, 2025a). ●

https://doi.org/10.26619/2183-4822.2026.CJ.5

References

EEAS (2025), *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*, European External Action Service, Brussels. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats_en

EEAS (2026), *4th EEAS Annual Report on Foreign Information Manipulation and Interference Threats*, European External Action Service, Brussels. https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en

EPRS (2025a), *Information manipulation in the age of generative artificial intelligence*, European Parliament Research Service, Brussels, PE 779.259, December. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779259/EPRS_BRI(2025)779259_EN.pdf

EPRS (2025b), *European democracy shield*, European Parliament Research Service, Brussels, PE 775.835, June. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775835/EPRS_BRI(2025)775835_EN.pdf

European Commission (2026), *AI Act, Shaping Europe's Digital Future*, European Commission, Brussels. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Union (2022), Regulation (EU) 2022/2065 ... (Digital Services Act), OJ L 277, 27.10.2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

European Union (2024), Regulation (EU) 2024/1689 ... (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024. http://data.europa.eu/eli/reg/2024/1689/oj

Giles, K. (2016), *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence, Riga. https://www.stratcomcoe.org/keir-giles-next-phase-russian-information-warfare

Marsili, M. (2021), 'The Russian Influence Strategy in Its Contested Neighbourhood', in H. Mölder, V. Sazonov, A. Chochia and T. Kerikmäe (eds), *The Russian Federation in Global Knowledge Warfare: Influence Operations in Europe and Its Neighbourhood*, Springer, Cham, pp. 149-172. https://doi.org/10.1007/978-3-030-73955-3_8

Marsili, M. (2023), 'Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse', *Applied Cybersecurity & Internet Governance*, 2(1), pp. 106-120. https://doi.org/10.60097/ACIG162861

Marsili, M. (2025a), 'Disinformation and Democratic Resilience in the European Union: Lessons from the Covid-19 Pandemic and Election Interference', *Studia Administracji i Bezpieczeństwa*, 19, pp. 195-220. https://doi.org/10.5604/01.3001.0055.6584

Marsili, M. (2025b), 'The European Union's Strategic Adaptations to Hybrid Conflicts and the Influence of External Actors', *Studia Administracji i Bezpieczeństwa*, 19, pp. 23-60. https://doi.org/10.5604/01.3001.0055.6583

Marsili, M. (2025c), 'DeGen Artificial Intelligence: Challenges and Opportunities of AI Applications', *European Cybersecurity Journal*, 10(1), pp. 67-78.

NATO (2026), *Countering hybrid threats*, North Atlantic Treaty Organization, Brussels. https://www.nato.int/cps/en/natohq/topics_156338.htm

Stanford HAI (2025), *AI Index Report 2025, Stanford Institute for Human-Centered Artificial Intelligence*, Stanford University. https://hai.stanford.edu/ai-index/2025-ai-index-report

Wardle, C. and Derakhshan, H. (2017), *Information Disorder: Toward an interdisciplinary framework for research and policymaking*, Council of Europe, Strasbourg. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c