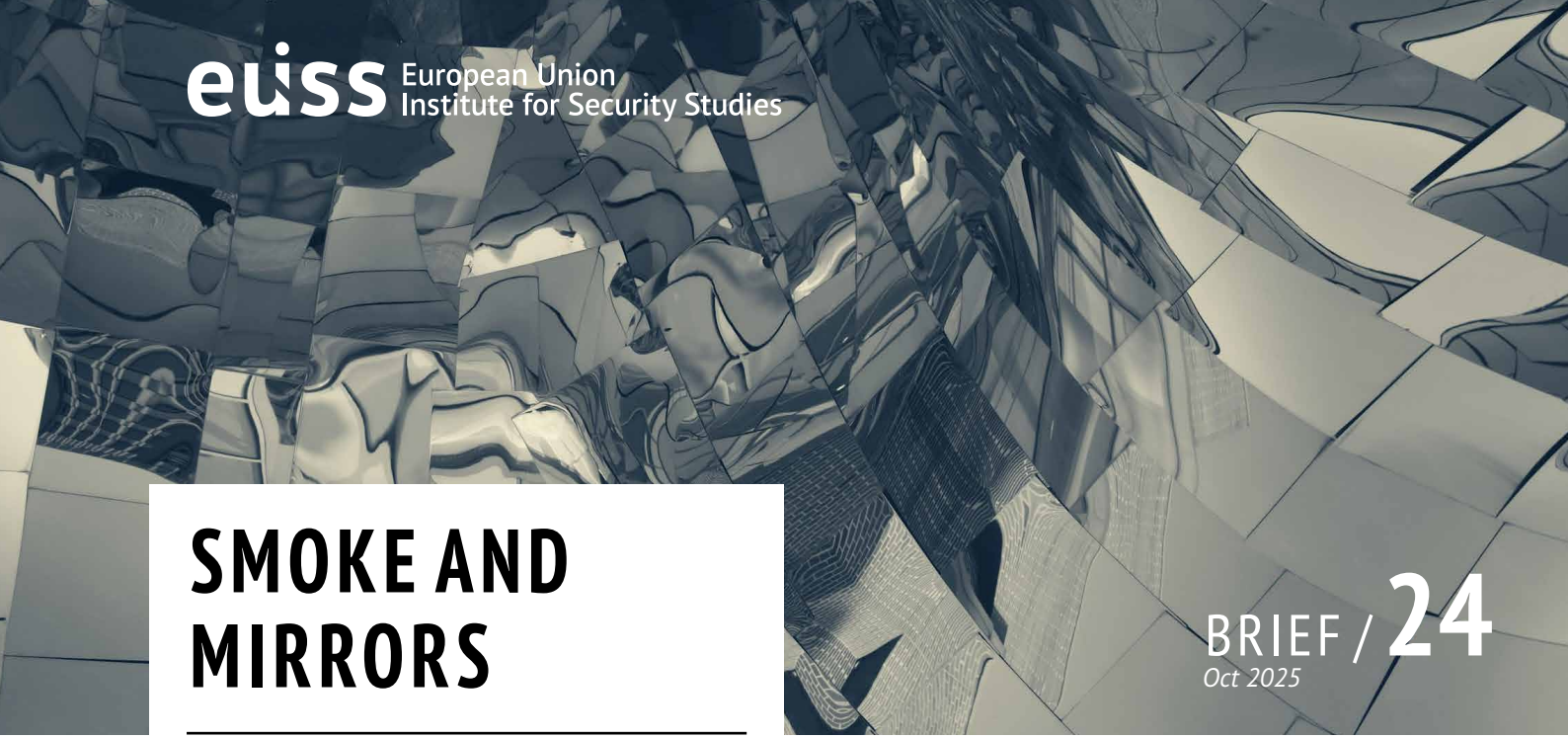
European Union Institute for Security Studies



SMOKE AND MIRRORS

BRIEF / 24
Oct 2025

Building EU resilience against manipulation through cognitive security

The EUISS is an agency of the European Union

by

Beatrice Catena
War Studies Department, King's College London

Ondrej Ditrych
Senior Analyst, EUISS

Naďa Kovalčíková
Senior Analyst, EUISS

Recent violations of the airspaces of Poland, Romania and Estonia illustrate how Russia uses psychological operations to distort perceptions and manipulate behaviour – effectively setting a cognitive trap. Both underreaction and overreaction risk provoking even more reckless Russian actions in the future, while at the same time deepening public anxiety over possible escalation to an open conflict. Cognitive security – the protection of human perceptual and decision-making processes from external manipulation – offers a useful approach to addressing these rapidly evolving vulnerabilities. It highlights how malign actors exploit such weaknesses to erode trust, undermine societal resilience and threaten transnational security. As a concept, it has emerged only recently, building on military understandings of 'cognitive warfare' developed within NATO circles from the early 2000s.

Summary

- Generative-AI, deepfakes and psychometric profiling provide adversaries like Russia with unprecedented opportunities to shape perception and behaviour. So far, the EU response has only addressed these critical cognitive dimensions tangentially.
- Building on earlier work – such as NATO's conceptualisation of cognitive warfare – the cognitive security framework shifts the focus from enemy tactics to the EU's widening security deficits. It zeroes in on psychological vulnerabilities – such as cognitive biases and emotional contagion – that hostile actors actively exploit. Russia's war against Ukraine offers ample examples of the associated risks.
- The urgency of EU action on cognitive security is clear. A three-tier roadmap – strategic, operational and tactical – can help the EU and Member States both better understand cognitive risks and build resilience. The EU must integrate cognitive security into its defence frameworks, ensuring preparedness in an evolving threat landscape.

Funded by the European Union

Countering Foreign Interference

CLEARING THE SMOKE: GRASPING COGNITIVE SECURITY

Technological advancements are enabling adversaries to manipulate perception and decision-making on an unprecedented scale and with growing precision. By mining vast volumes of publicly available data – from social media to geolocation information – illiberal states and non-state actors aligned with them can design targeted influence campaigns that exploit psychological vulnerabilities and corrode public trust in democratic institutions.

Recent exercises have revealed how easy it is to harvest soldiers' data and track troop movements [1]. Finland's 2022 Digipower investigation revealed how digital platforms can easily be used to amplify polarisation and influence the views of top politicians [2]. The rollout of generative AI has further accelerated operations. A 2025 Joint Research Centre study warns that synthetic media is lowering cost barriers for foreign information manipulation and interference (FIMI) at scale [3]. Yet the full cognitive impact of these technologies, and the consequences of their weaponisation, remains poorly understood. In response, defence departments, civil society and international organisations like NATO are reevaluating and expanding their understanding of conflict [4].

The concept of cognitive warfare developed under NATO's Allied Command Transformation (ACT) provides a starting point for the broader conversation around cognitive threats. It explores how adversaries exploit human cognition to manipulate perceptions, disrupt decision-making and influence behaviour [5]. By integrating behavioural sciences and technology, NATO has begun to expose psychological manipulation as a battlefield, revealing cognitive vulnerabilities long overlooked in traditional defence planning, such as emotional contagion in digital ecosystems and the strategic weaponisation of personnel identities during operations. In this context, cognitive security has emerged as a concept that blends insights from diverse disciplines and focuses on the intersection of technology and social engineering in hybrid campaigns. While cognitive warfare is an emerging military concept focused on hostile tactics, yet to be formalised into a doctrine or domain, the concept of cognitive security extends this logic into a broader defensive framework.

The EU is not being caught off guard. It has bolstered its ability to address threats to its societies and political institutions by adopting the Strategic Compass (in 2022) [6] and cyber, hybrid and FIMI toolboxes, and by deploying hybrid rapid response teams. The adoption of a cognitive security framework is the next logical and necessary step. Cognitive security goes further than tracking and countering FIMI or hybrid threats; it shifts the focus to the perceptual and behavioural vulnerabilities that make manipulation possible in the first place. Drawing on psychology and neuroscience, it offers policymakers a lens to identify and reduce those vulnerabilities, including through interdisciplinary research. Cognitive security calls for more than traditional defence measures. It requires a direct response to the strategic targeting of perception and knowledge in covert political warfare.

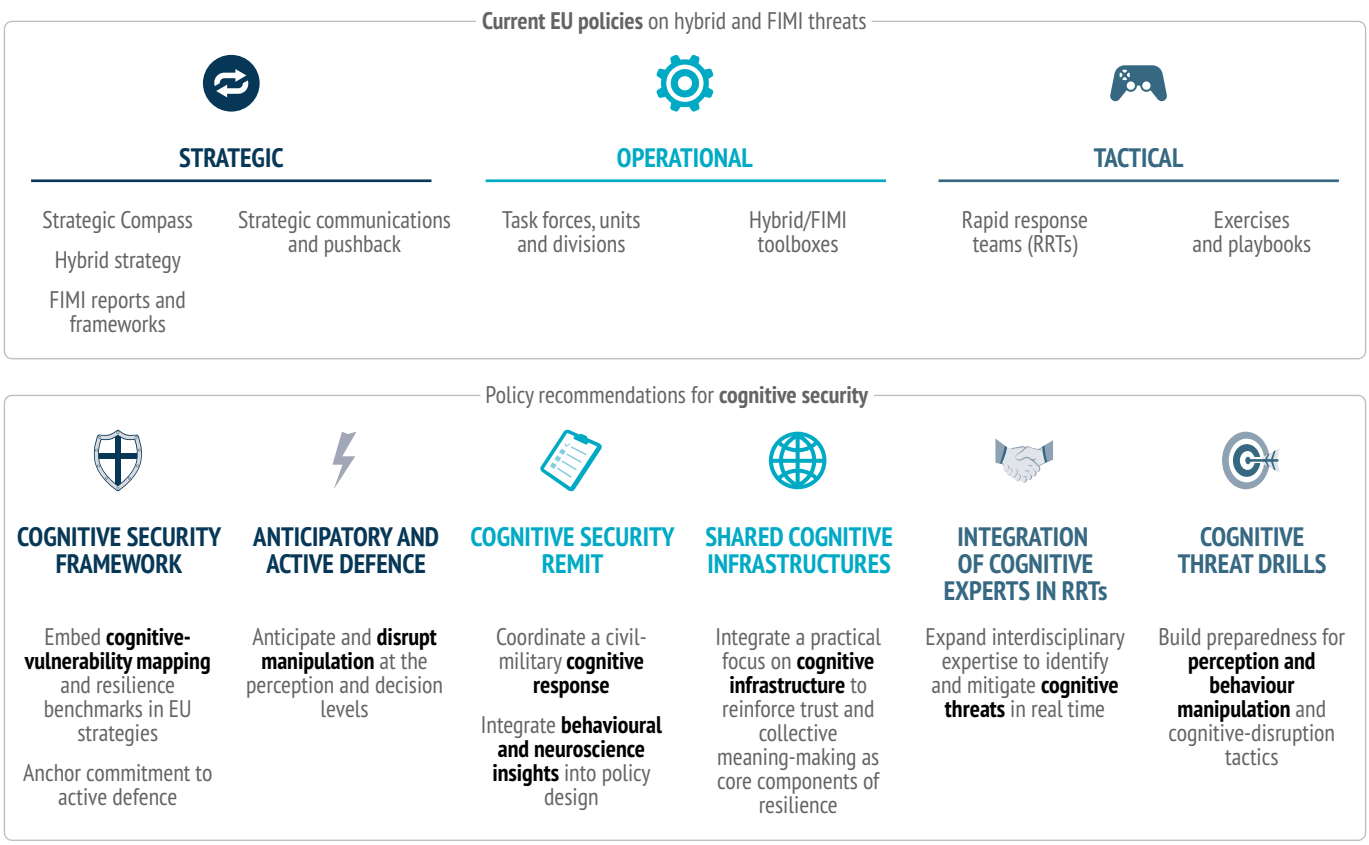
SEEING THROUGH MIRRORS: TARGETING HUMAN PERCEPTIONS

This is not the first time in history that the human mind has been targeted by foreign adversaries. What is new today is the scale and depth of these tactics: altering human cognition for strategic ends, weaponising brain science and biotechnology, and exploiting social media data using AI-backed analytics to conduct advanced social engineering. These practices strike at the very foundations of social order. Systemic disinformation, the manufacture of false collective memories, information overload and AI-facilitated coordinated inauthentic behaviour, together with deepfakes and other sophisticated forgeries, extend beyond manipulating individuals at key decision points.

AI is used to confuse and corrupt. Bots saturate the information space, forcing users to rely on cognitive shortcuts. They also simulate and amplify popular sentiment on social media. Large language models (LLMs) can be deployed to generate noise, while tools like CopyCop demonstrate how ChatGPT can subtly alter legitimate media content *en masse*. *Döppelganger* disinformation campaigns, run by Russia's Social Design Agency (SDA), as well as the widespread media coverage of their exposure, show how the information space can be penetrated by cloning legitimate media and government sites, making the line between fiction and reality increasingly blurred for online audiences. Russia has also manipulated interpretive frames in Ukraine: shaping not just the information environment as part of its war, but how people perceive battlefield events [7]. In parallel it has been circulating false historical narratives targeting international audiences, seeking to weaken support for Ukraine by denying its claim to sovereignty – a principle that Russia claims to uphold in other contexts. In this rewriting of history, the iniquitous West is blamed not only for the current war but also for erecting the Iron Curtain after World War II [8].

Cognitive security roadmap

Existing instruments and the case for cognitive security



Data: Authors' compilation based on official EU and EEAS documents (2015–2025), including the Joint Framework on Countering Hybrid Threats (2016), the Action Plan against Disinformation (2018), the Strategic Compass (2022) and the Council Conclusions on the EU Hybrid Toolbox (2022) and Rapid Response Teams (2024), among others.

Cognitive security offers a useful framework for understanding and responding to these tactics. It moves beyond addressing the creation and consumption of intentionally misleading information – traditional propaganda and more familiar FIMI – and focuses rather on the risks that arise from the way people process information through pre-existing heuristics and interpretive narrative frames. At its core, cognitive security addresses tactics that manipulate information intake. These include stimulating cognitive shortcuts, encouraging dissociation or motivated reasoning[9] (driven by goals other than accuracy), as well as emotional responses to events. The aim is to ensure that 'spontaneous interpretations' of events fall within a predictable and even desirable range. Such tactics do not just reshape processes of truth-formation and contestation in democratic debate: they target the cognitive faculties themselves, creating powerful filters for processing reality. The tactics and actors in Russia's cognitive war machine are diverse, each with its own parochial agenda – the SDA being a case in point. But they follow a single strategic direction: drawing individuals into a parallel reality, where their perceptions are moulded, thereby advancing Russia's geopolitical objectives while eroding its opponents' ability to resist.

Cognitive security can be understood as the twin of societal resilience. Where resilience is a collective property that allows for continuity and adaptation in the face of adversity, cognitive security concerns individual capacities and faculties. Rather than promoting a facile notion of incontestable truth, it serves as a counterweight to the technological determinism that has dominated disinformation research. While the latter focuses on algorithmic structuring of content, a cognitive security approach emphasises individual human predispositions as well as the structural, temporal and spatial contexts in which this content is consumed, amplified and even coproduced.

THE EU'S PATH TO COGNITIVE SECURITY

To move beyond the existing cognitive warfare framework – which focuses on adversaries' exploitation of human cognition – the EU and its Member States should adopt a proactive and systematic approach. This means addressing the perceptual and behavioural vulnerabilities that enable manipulation, while bolstering citizens' ability to protect themselves against cognitive threats. This requires action on three levels: strategic, operational and tactical[10]. This multilayered approach can build on the EU's established playbooks for countering hybrid threats, including FIMI, extending them into the cognitive domain.

Strategic level: The EU should make cognitive security a core pillar of its security culture, with two goals. The first should be to provide an EU-wide Cognitive Resilience Framework to improve understanding of related risks. This would help integrate cognitive resilience benchmarks into the EU Strategic Compass and national defence strategies, mandating cognitive threat assessments in all hybrid threat evaluations and civilian-military scenario planning. Using existing tools such as the Deception, Intention, Disruption and Interference (DIDI) model[11] can make it easier to identify illegitimate cognitive influence at both individual and collective levels. Such models help develop technological and human capacities to detect a lack of transparency about the sources, origins and purpose of manipulative techniques (D); identify intent to harm (I); and establish when disruption is disproportionate to any potential benefits (D) through deciphering covert operations to destabilise society (I).

Second, the EU should develop and implement measures to mitigate cognitive influence at the strategic level and push back, following the example of the Swedish Psychological Defence Agency[12], or build on the tools and expertise of the Finnish Advisory Board for Defence Information. This will enable the EU and Member States to anticipate and counter cognitive threats before they gain momentum, rather than playing catch up.

Operational level: The EU should consider integrating and mainstreaming a cognitive security lens across its institutions to increase awareness and reinforce interinstitutional efforts – both civil and military. It could launch a Civil-Military Scientific advisory group on Cognitive Threats to harness expertise from the fields of behavioural science, neuroscience, digital technologies and security studies. This group would help the EU and Member States to better assess the vulnerabilities created by cognitive insecurity and devise actionable practices to address them. In the longer term, the EU should invest in national education programmes focused on critical thinking, media literacy and digital fluency, as well as cognitive bias awareness, complementing the work on the European Democracy Shield and the 'Europe's Digital decade' programme.

Tactical level: Countering specific cognitive influence campaigns requires immediate, frontline action. Recent investigations have revealed that malicious publication of private data (doxing) is increasingly penetrating the European internet as a tool of cognitive warfare. The EU must secure channels for operational exchange on ongoing adversarial campaigns with partners such as those in its Eastern neighbourhood, the United Kingdom, or others. The EU and its Member States need to set up and train cognitive defence teams, possibly expanding the mandate, resources and expertise of hybrid rapid response teams. These teams must be able to deploy swiftly to protect civilian, military and journalists' data in both the EU and in partner countries. These measures would help shield civilians from being monitored and from having their perceptions manipulated by hostile actors.

The EU stands at a crossroads: it can either dismiss cognitive vulnerabilities as inevitable human imperfections, or recognise that cognition itself has become a battlefield and weave cognitive resilience into every layer of security policy.

References

(1) NATO Strategic Communications Centre of Excellence, 'Camouflage for the digital domain', 9 March 2020. (https://stratcomcoe.org/publications/camouflage-for-the-digital-domain/59).

(2) Finnish Innovation Fund (Sitra), 'Digipower investigation: top politicians unknowingly part of invisible networks of influence', Sitra News, 1 April 2022. (https://www.sitra.fi/en/news/digipower-investigation-top-politicians-unknowingly-part-of-invisible-networks-of-influence/).

(3) Abendroth-Dias, K., Arias Cabarcos, P. et al., 'Generative AI outlook report: Exploring the intersection of technology, society and policy', Joint Research Centre, *Science for Policy Report* (EUR 40337 EN), European Commission, 2025.

(4) See for example: Ministero della Difesa, 'Cognitive warfare: La competizione nella dimensione cognitiva', 2023. (https://www.difesa.it/assets/allegati/29459/4.cognitive_warfare___la_competizione_nella_dimensione_cognitiva._ed.2023.pdf).

(5) NATO Allied Command Transformation, 'Cognitive warfare', 2021 (https://www.act.nato.int/activities/cognitive-warfare/).

(6) European External Action Service, 'A strategic compass for security and defence', 2022. (https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en).

(7) Stepanenko, V., 'Shaping critical thinking as a factor of the local security in wartime conditions', *Prawo i bezpieczenstwo*, Vol. 3, No. 2, 2024; Taranenko, A., 'КОГНІТИВНА БЕЗПЕКА ЯК ВИМІР РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ', *Політологічний вісник*, No. 92, 2024.

(8) See Litvinova, D., 'How the Kremlin weaponised Russian history – and has used it to justify the war in Ukraine', Associated Press, 21 February 2024 (https://apnews.com/article/russia-ukraine-war-history-putin-propaganda-80cb70fff9820357eddb83170695bdbb).

(9) Ziemer, C.T. and Rothmund, T., 'Psychological underpinnings of disinformation countermeasures: A systematic scoping review' (https://osf.io/preprints/psyarxiv/scq5v).

(10) Bugayova, N. and Stepanenko, K., 'A Primer on Russian Cognitive Warfare', Institute for the Study of War (ISW Press), 30 June 2025.

(11) Pamment, J., Nothhaft, H., Agardh-Twetman, H. and Fjällhed, A., 'Countering information influence activities: The state of the art', Swedish Civil Contingencies Agency (MSB) Research Report MSB1261, July 2018, p. 16.

(12) Pamment, J. and Tsurtsumia, D., *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency*, Swedish Psychological Defence Agency, 2025, pp. 192 – 194 (https://mpf.se/psychological-defence-agency/publications/archive/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency).

euiss

Published by the European Union Institute for Security Studies.
Printed in Luxembourg by the Publications Office of the European Union.

Cover image credit: Jacky Pun/Unsplash

Publications Office of the European Union

PRINT ISBN 978-92-9462-417-8
CATALOGUE NUMBER QN-01-25-024-EN-C
ISSN 2599-8943
DOI 10.2815/5889883

WEB ISBN 978-92-9462-416-1
CATALOGUE NUMBER QN-01-25-024-EN-N
ISSN 2315-1110
DOI 10.2815/8072408