The Mind as Battleground: Cognitive Warfare and the Future of European Security

Myrto J. Demetriou, MA

April 2026

The Mind as Battleground

Cognitive Warfare and the Future of European Security

Myrto J. Demetriou, MA — Co-Founder, Cyprus Security and Intelligence Institute (CySII)

Opinion Paper • Intelligence & Cognition • April 2026

Wars used to begin at borders. Today, they begin in minds.

The most consequential battlefield of the twenty-first century has no coordinates on any military map. It has no coastline to defend, no airspace to patrol, no infrastructure to harden. It is the human cognitive space, which in essence is the domain of perception, belief, attention, and decision-making, and it is under sustained, systematic attack.

This is not metaphor, but rather an operational reality. State actors, most prominently Russia but by no means exclusively, have invested heavily in the science and practice of cognitive warfare: the deliberate manipulation of how individuals and societies perceive the world, form judgements, and act upon them. The objective is not to destroy an adversary's army but to hollow out an adversary's will. Specifically, to make populations doubt their governments, distrust their institutions, question their allies, and lose confidence in the very capacity of democratic society to protect itself.

For Cyprus, sitting at the fault lines of European security, energy geopolitics, and unresolved territorial contestation, the cognitive dimension of modern conflict is not a distant theoretical concern. It is an immediate, documented threat with concrete consequences for national security and democratic governance.

What Cognitive Warfare Actually Is

NATO's Allied Command Transformation, which has invested substantially in understanding and countering cognitive threats, defines cognitive warfare in its *Cognitive Warfare Exploratory Concept* (NATO ACT, 2024) as "activities conducted in synchronisation with other instruments of power, to affect attitudes and behaviour by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary." The definition is deceptively simple but its implications are profound.

Cognitive warfare is not propaganda, even though it uses propaganda as one instrument, and it is not psychological operations as traditionally understood, even though it draws on their techniques. Rather, it is a broader, more systematic effort to exploit the structural vulnerabilities of human cognition itself: our tendency toward confirmation bias, our susceptibility to emotionally charged narratives, our difficulty distinguishing authentic from fabricated content, and our deep need for coherent explanations in the face of complexity.

What makes contemporary cognitive warfare qualitatively different from historical influence operations is the convergence of three enabling factors. First, the ubiquity of social media platforms as unmediated information environments. Second, the availability of artificial intelligence tools capable of generating persuasive content at scale and at minimal cost. Third, the accumulated scientific knowledge of cognitive psychology, behavioural economics, and neuroscience, which adversaries are now actively using as a weapon.

Russia's Cognitive Campaign: A Doctrine, Not a Tactic

Russia's approach to cognitive warfare is not improvised as one would assume, on the contrary, it is doctrinal. The Russian concept of "reflexive control" which encapsulates shaping an adversary's decision-making by feeding it carefully crafted information so that it arrives, independently, at conclusions favourable to Russian interests, has been a feature of Soviet and Russian strategic thinking since the 1960s. What has changed is the scale, the speed, and the technological sophistication with which this doctrine is now implemented.

Russian investment in cognitive warfare infrastructure has been estimated at approximately one to two billion US dollars annually, depending on methodology, distributed across a sprawling ecosystem of state media, proxy outlets, social media amplification networks, and covert influence operatives. The objectives are consistent across target societies: foster distrust in democratic institutions, amplify existing social divisions, erode confidence in the EU and NATO, and create a background noise of uncertainty and disorientation within which rational collective decision-making becomes progressively harder.

The Russia–Ukraine conflict has served as a live laboratory for cognitive warfare techniques. AI-generated deepfake videos of Ukrainian leadership, algorithmically amplified false narratives about alleged atrocities, coordinated flooding of information spaces with contradictory claims are all designed not necessarily to convince audiences of a specific falsehood, but to overwhelm their capacity for discernment altogether. When citizens cannot reliably distinguish truth from fabrication, the result is not skepticism but paralysis.

The Cypriot Dimension: A Uniquely Exposed Society

Cyprus presents cognitive warfare actors with a target environment of particular vulnerability and particular value. The island's communal division creates deep-seated identity fractures and information silos that are readily exploitable by targeted influence operations. A 2024 media literacy assessment ranked Cyprus 28th of 41 European

countries surveyed by the Open Society Institute–Sofia Media Literacy Index (Open Society Institute–Sofia, 2024). Far from being an abstract statistic this represents a measurable gap between the sophistication of attacks being mounted and the societal resilience available to absorb them.

Reports in January 2026 described an incident in which fabricated content distributed across spoofed news sites alleged high-level corruption within the Cypriot Government (Washington Post, 2026). Cypriot authorities and international media noted methodological similarities to known patterns of state-sponsored information-warfare activity, although formal attribution to any specific state actor has not been publicly confirmed. Whatever the eventual attribution, the incident followed a pattern consistent with cognitive-warfare doctrine in terms that it targeted not military capability but institutional trust, its weapon was not a missile but a manufactured narrative, algorithmically distributed through platforms designed to reward emotional engagement over factual accuracy, its aim was not to destroy Cyprus's government but to make foreign investors, European partners, and Cypriot citizens doubt it.

The timing was striking since the incident emerged as Cyprus was finalising its EU Council Presidency programme. Whether or not the timing was deliberate, the pattern is consistent with a textbook cognitive-warfare objective which is to degrade the target's capacity to lead before leadership begins.

The Intelligence Response: Protecting the Cognitive Layer

Defending against cognitive warfare requires capabilities and frameworks that the intelligence community has not historically been structured to provide. Traditional intelligence work focuses on secrets. Classified capabilities, covert intentions and clandestine activities amongst others. Cognitive warfare, however, operates largely in the open, through publicly accessible platforms, through content that is technically legal, through narratives that exploit genuine grievances and real social fault lines. It is therefore difficult to stop because much of it is not, strictly speaking, illegal.

What is required is a shift in analytical focus. Intelligence services must develop robust capabilities for attribution in terms of tracing the origins and funding of influence operations back to their state sponsors. They must invest in behavioural science expertise, enabling them to assess the cognitive impact of information operations on target populations. And they must build relationships with the research community, the media sector, and technology platforms that allow for rapid identification and disruption of inauthentic amplification networks.

Crucially, intelligence services must also shift from a reactive to a predictive posture. Cognitive warfare campaigns follow identifiable patterns such as preparatory narrative seeding, amplification escalation and crisis exploitation which can, with appropriate analytical investment, be identified before they reach full operational effect. The goal must be to expose the architecture of an operation while it is still being constructed, not after the damage is done.

A European Imperative — and a Cypriot Opportunity

The European Union has begun to take cognitive warfare seriously, but progress has been uneven. The Foreign Information Manipulation and Interference (FIMI) framework, the Code of Practice on Disinformation, and the Digital Services Act's provisions on systemic risk all represent meaningful steps. However, they remain primarily reactive, platform-focused, and insufficiently integrated with the intelligence and defence communities that understand the operational dimensions of the threat.

Cyprus's 2026 EU Council Presidency offers a rare opportunity to address this gap. As a member state that has experienced cognitive warfare operations firsthand, that sits at the intersection of multiple active threat vectors, and that has developed practical knowledge of cognitive warfare's effects on a small, divided society, Cyprus brings an authority to this debate that few other EU members can match.

The Presidency should be used to advance a coherent European doctrine for cognitive security, one that integrates intelligence analysis, platform regulation, media literacy investment, and civil society resilience into a unified framework. The defensive doctrine that responds to cognitive warfare, what the institute will subsequently develop as *cognitive security*, a defensive domain on equal footing with territory, economy, energy, and cyber, must be built on this same political will. Europe does not lack the tools but what it has lacked, until now, is the political will to treat the protection of the cognitive layer as a first-order security priority equivalent to the protection of physical infrastructure.

The stakes are not abstract. When citizens lose the capacity to form accurate beliefs about their world, democratic governance loses its foundations. When institutions are systematically delegitimised through fabricated narratives, the social contract that underpins collective security begins to dissolve. Cognitive warfare does not aim to win battles. It aims to make its adversaries incapable of fighting them.

Europe must learn the lesson before the cost of ignorance becomes irreversible. The mind is the battleground and it is time our defences reflected that reality.

About the Author

Myrto J. Demetriou, MA is a co-founder of the Cyprus Security and Intelligence Institute (CySII) with hands-on experience in national security. Her research focuses on intelligence studies, Cognitive warfare, and Eastern Mediterranean security dynamics.

The views expressed in this opinion paper are those of the author.

References

1. NATO Allied Command Transformation. (2024). *Cognitive Warfare Exploratory Concept*. Norfolk: NATO ACT. https://www.act.nato.int/activities/cognitive-warfare/

2. Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*, 7. https://doi.org/10.3389/fdata.2024.1452129
3. Institute for the Study of War. (July 2025). *A Primer on Russian Cognitive Warfare*. Washington, DC: ISW.
4. Royal United Services Institute (RUSI). (2025). *Russia, AI and the Future of Disinformation Warfare*. London: RUSI.
5. Paziuk, A., Lande, D., Shnurko-Tabakova, E., & Kingston, P. (2025). Decoding manipulative narratives in cognitive warfare: A case study of the Russia–Ukraine conflict. *Frontiers in Artificial Intelligence*. https://doi.org/10.3389/frai.2025.1566022
6. Washington Post. (9 January 2026). *Cyprus says video alleging the country is corrupt is likely the product of Russian disinformation*.
7. Center for the Study of Democracy. (July 2025). *Seizing the Edge in Cognitive Warfare*. Sofia: CSD.
8. New Eastern Europe. (September 2024). *Russia in the Trenches of Cognitive Warfare*.
9. Cyprus Presidency of the Council of the EU. (2026). *Programme and Priorities*. Brussels: Council of the EU. https://cyprus-presidency.consilium.europa.eu
10. Open Society Institute–Sofia. (2024)