Cognitive Warfare Dynamics: Understanding the Influence of Non-State Actors in NATO's Information Environment

Charikleia Thomopoulou

Assistant Research Supervisor, IDIS

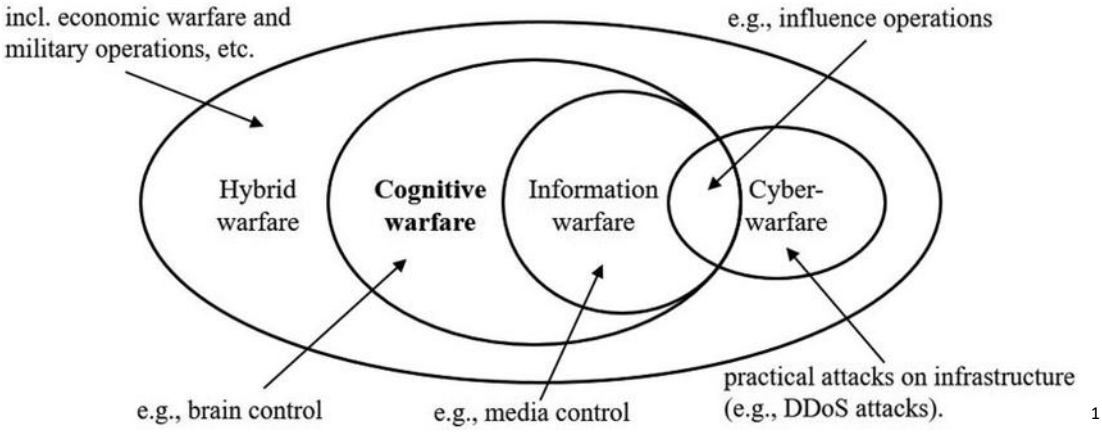
Abstract

Contemporary conflict is currently expanding towards the cognitive domain, where even non-state actors utilize influence strategies, in order to exploit societal vulnerabilities, erode cohesion and circumvent conventional security mechanisms. This paper explores how said non-state actors —utilizing ideological movements, extremists, and digital influence networks— operate within NATO's information environment, through the use of memetic tactics, disinformation, and psychological operations. Drawing on case studies from the MENA region, as well as diaspora networks in Europe, this paper highlights the need for a more proactive approach aiming at resilience in the cognitive domain. Finally, existing counter measures regarding cognitive warfare are assessed, and recommendations for further ways for improvement are made, in order for NATO's state members to be able to effectively adapt to the growing challenges of facing cognitive threats.

Introduction

Whether one considers the new domain of operations to be the cognitive domain or simply that of the human mind (Le Guyader, 2022), cognitive warfare has emerged as the new trend of contemporary conflict and NATO has integrated it in its deterrence and defense strategies (Saari et al., 2024) (J. Janzen, 2024). It is defined as "*the activities conducted in synchronization with other instruments of power, to affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage*"(Giordano, 2023).

Although it is threats related to state actors that dominate the debate on cognitive warfare, non-state actors have also demonstrated a growing capacity to influence NATO's information environment. Within this environment, non-state actors seem to be adapting pretty quick and effectively, by utilizing influence strategies in a decentralized manner, thus not restricting themselves by operating only in the physical domain. For the Alliance, whose strength lies not only in interoperability but in common values and policies, cognitive threats are both a strategic challenge and an opportunity for growth and further improvement.



[1]

The cognitive battlespace, as stated before, involves the domain that focuses on the human mind, where perceptions are shaped and behaviors can be influenced. Its operations lie below the threshold of war, making either their legalization or attribution particularly difficult compared to traditional kinetic operations. While information warfare targets systems, cognitive warfare targets the minds and the subconscious. It doesn't merely aim to deceit, but to influence and destabilize; to affect perceptions and create further polarization in the society that's being targeted, thus weakening people's ability to defend it (Bernal, Alonso et al., 2020). Non-state actors seem to have gradually acquired a better understanding of how the manipulation of the information environment —either through disinformation, or narratives that are either emotionally charged or of a religious context— is often more effective than direct conflict.

NATO, being a civil-military alliance of democratic states, is particularly vulnerable when it

[1] Image source: https://www.researchgate.net/figure/The-conceptual-relationship-among-cognitive-warfare-and-other-types-of-warfare-Each-type_fig1_362163528

comes to cognitive threats, just like open societies in general. Pluralistic, liberal societies can be led to fragmentation either by political, ethnic or religious criteria. The Freedom of Press and the openness of social media platforms that flourishes within the borders of such societies can be easily exploited for the circulation of unverified claims and fake news. Also, unlike societies ruled by authoritarian regimes, public opinion is more likely to have a substantial influence on national foreign policy, especially when it comes to prolonged operations. In sum, for opponents of NATO —whether it's state or non-state actors— its societal cohesion, credibility and deterrence can be weakened through manipulating perceptions, even without any kind of confrontation of military nature. This paper focuses on the aspects of non-state actors' influence within the cognitive domain, thus contributing to a more nuanced understanding of cognitive warfare dynamics.

The Evolving Role of Non-State Actors

As the contemporary battlefield evolves, the role of non-state actors (such as cyber militias, civilian groups or even private enterprises) evolves too. By leveraging cyber and information technologies, their actions usually aim to achieve low-cost strategic effects with high reach, influencing public opinion and consequently disrupting NATO operations. These actors can either act independently, or even sometimes in coordination with state actors. Their asymmetric tactics blur the lines between peace and conflict, and often further polarize society.

A fine example of such non-state actors is terrorist organizations like Al-Qaeda, ISIS and Hay'at Tahrir al-Sham, which have honed their ability of creating, adapting and utilizing narratives (KhosraviNik & Amer, 2022). Their cognitive strategies include a *framing of victimization*, thus portraying NATO as a "neo-crusader" force, and *appeals of religious legitimacy*, mostly tailored for local audiences (Celso, 2019). The messages are often embedded in either a humanitarian, political or cultural context. Additionally, the means used to disseminate them follow a *digitally decentralized* plan, making use of anonymous channels on Telegram, TikTok reels or WhatsApp groups. Despite their apparent territorial defeat, ISIS and those affiliated with it maintain a strong virtual presence, and try to recruit, radicalize and delegitimize NATO and its partners (Bernal, Alonso et al., 2020) (B.-G. J. Janzen, 2019).

Apart from conflict zones though, such non-state actors target also the diaspora communities within the borders of NATO's member states. Through cultural associations, digital networks of religious nature and eco-chambers in social media, they take advantage of tensions regarding migrant identity, such as feelings of alienation (commonly found among second-generation migrants), perceived double standards in Western foreign policy and narratives that promote polarization in the pretext of facing the concepts of Islamophobia, imperialism or injustice (Rudner, 2017). This results in creating cognitive frictions, which shape public opinion and undermine support towards NATO operations or national counter-terrorism policies, affecting societal cohesion.

Among the aforementioned tactics used for propaganda dissemination in the social media, memes and emotionally charged images are also popular tools besides short videos and reels (Huey, 2015). The aim is as usual, to bypass the mind's rational processing and analysis of information and appeal directly to cognitive biases that instinctively activate through emotional stimuli. This kind of memetic tactics take advantage of algorithms and societal fragmentation, and utilize social media platforms as a kind of accelerant to further instigate cognitive conflict. Such examples can be found in audiovisual material that glorifies martyrdom, as well as troll accounts that promote disinformation about NATO and its member states, with the aim to gain more followers and at the same time, provoke public outrage.

Building Resilience: From Counter-Narratives to Cognitive Readiness

NATO's main response to cognitive threats can be summed up by the following key countermeasures: *enhancing cyber and information resilience, leveraging strategic communication and narratives, and improving public education and awareness* in order to build societal resistance to foreign manipulation. More explicitly, building cyber resilience and protecting the information systems of the Alliance helps reduce systemic vulnerabilities that can be exploited (Radu, 2025). In addition to that, fostering information-sharing practices among the member states amplifies the effectiveness of such initiatives. On the other hand, communication strategies whose purpose is to introduce factual and credible narratives, as well as localized storytelling (Saari et al., 2024), can also be instrumental to preventing

disinformation from spreading online. Moreover, unified and value-based narratives that get disseminated, can consequently enhance credibility, legitimacy and cultivate public trust. Additionally, initiatives that include monitoring, exposing or countering disinformation campaigns make a significant contribution to NATO's efforts. This kind of initiatives sometimes include working with social media platforms or banning hostile outlets (Nistor, 2023). Lastly, initiatives that promote digital literacy and critical thinking are equally important and help boost societal resilience against cognitive threats. An example of such initiatives, is the CogWar newsletter[2] by the Allied Command Transformation (ACT).

Of course, even when it comes to defending against cognitive threats, there are ethical limits NATO must adhere to when influencing domestic audiences (Avădănei, 2022). These kinds of restrictions may reduce the operational effectiveness of such defensive operations, but ethical constraints aren't the only impediment. The problem of attribution behind cognitive attacks can pose quite a challenge (Miller, 2023), to the extend that it hinders the possibility of responding in a more straight forward manner. Also, as mentioned before, non-state actors have been adapting and evolving rapidly, which consequently prompts NATO to refine its strategies and doctrines, and keep them up to date (Deppe & Schaal, 2024).

Lastly, the advancement of relevant legal frameworks, as well as the integration of cognitive defense across NATO's member states remain in early stages. Although the broader warfare regulations regarding hybrid and information warfare (which mainly refer to countering cyber, psychological and information operations) have legal frameworks embedded that concern cognitive threats as well, there is still not a unified, binding legal standard that's specifically dedicated to cognitive defense (Deppe & Schaal, 2024; Saari et al., 2024). Despite ongoing efforts to integrate joint doctrines and operational initiatives across member states, the progress faces difficulties due to legal, definitional and implementation challenges. So what can NATO do to better equip itself and its members to deal with cognitive threats?

[2] https://www.act.nato.int/activities/cognitive-warfare/

Recommendations

Building upon NATO's Cognitive Warfare Concept[3], the formalization of a *NATO-wide Cognitive Doctrine* is recommended. Establishing a unified framework will help the Alliance to achieve and maintain cognitive superiority (Hartley III & Jobson, 2021), an emerging core element of the ever evolving battlespace. Although challenges may still remain, regarding conceptual clarity and integration with doctrines that are already in place, the importance of cognition and its central role in modern conflict has already positioned the Alliance to prioritize resilience and operational advantage within a rapidly evolving information environment. The formal adoption of a Cognitive Doctrine is bound to occur and will ultimately come to fruition. It is in NATO's benefit to speed up the process.

Additionally, the transformation of the Applied Cognitive Effects (ACE)[4] team into a *NATO Centre of Excellence on Cognitive Security* is also recommended. This would be a significant step forward in institutionalizing the Alliance's approach to cognitive security. Whether a Cognitive Doctrine gets formalized first or not, a new CoE could either support its development or assist with its implementation. Further promoting relevant training and education, as well as operational support beyond research and innovation, a CoE on Cognitive Security could prove vital in driving innovation and unifying the Alliance's efforts in regards to countering cognitive threats. This development could significantly assist NATO in anticipating, detecting and responding to adversarial actions that concern the cognitive battlefield.

An investment in *mapping the "human terrain"* of NATO's information environment could also prove to be beneficial regarding threat assessments, particularly in combination with monitoring non-state actors. Better understanding the social, cultural and emotional landscape can be important, especially when it concerns critical zones or partners. NATO should further invest in tools that monitor public sentiment, as well as analyze discourse in diaspora networks across the North-Atlantic region. The information produced by this kind of tools could provide insights that can help improve both policy and operational messaging in fragile environments.

[3] https://www.act.nato.int/article/cogwar-concept/
[4] https://www.act.nato.int/wp-content/uploads/2025/10/20251001_CogWar-Newsletter-October.pdf

Another potential tool that could help battle cognitive threats is that of specialized *Awareness Teams*. Modeled by existing cybersecurity and defense teams and in combination with the aforementioned CoE, they could be deployed during NATO missions in order to monitor influence dynamics in real-time, provide consultation regarding cognitive risk factors and coordinate with civil society with the purpose of identifying the dissemination of hostile narratives. These Awareness Teams could also act as liaison with digital platforms and academic institutions that specialize in narrative warfare, as well as anthropology and behavioral psychology in the digital space. That could simultaneously help strengthening NATO's cooperation with civil society.

Conclusion

In the contemporary battlefield, it's not just territories that may be under threat but also people's mind and subconscious. Although state actors remain central when it comes to the debate on cognitive warfare, the findings of this paper highlight that non-state actors also contribute to the cognitive pressures affecting NATO's information environment. Non-state actors have proven to be rather adverse in navigating the cognitive terrain, by utilizing digital tools and strategies that take advantage cultural and psychological elements of society, in order to destabilize and divide. For NATO, the path forward is not merely defensive; by acknowledging the emerging cognitive threats a core strategic concern, the Alliance should further enhance its resilience and its operational effectiveness, in order to face the conflicts of tomorrow.

So far, NATO has developed a multi-faceted approach for countering cognitive threats. By focusing on enhancing cyber and information resilience, leveraging strategic communication and increasing societal awareness, the Alliance has taken important steps in regards to cognitive warfare. Despite ethical constraints and attribution challenges, as well as the rapid evolution and adaptability of non-state actors in the modern battlespace, NATO has been continuously refining its strategies and doctrines. However, the progress of legal frameworks and the integration of cognitive defense across the member states of the Alliance remain in

early stages. Therefore, challenges remain regarding the standardization and operationalization of a cohesive, legally grounded response against cognitive threats.

In this paper, further recommendations were made, in order to support and reinforce NATO's initiatives against cognitive threats. The formalization of NATO-wide Cognitive Doctrine, the founding of a NATO Centre of Excellence on Cognitive Security, the enhancement of the tools for mapping the "human terrain" of NATO's information environment, and finally, the establishment of specialized Awareness Teams, could all provide a new, robust strategic toolkit for NATO's operational arsenal. The integration of these initiatives could help the Alliance to further develop resilience and achieve cognitive superiority, as well as maintain a strategic edge across all domains of modern conflict.

Bibliography

Avădănei, A.-K. (2022). Influence Operations, between the Ethical and Critical Facet. *„Samoilă Mârza" PSYOPS Centre*, *2022*.
https://doi.org/10.55535/RMT.2022.3.05

Bernal, Alonso et al. (2020). Cognitive Warfare: An Attack on Truth and Thought. *John Hopkins University*.
https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf

Celso, A. (2019). The Jihadist Threat to Europe: From Al Qaeda to the Islamic State. *International Journal of Political Science*.
https://doi.org/10.20431/2454-9452.0501005

Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*.
https://doi.org/10.3389/fdata.2024.1452129

Giordano, P. (2023, April 5). Cognitive Warfare: Strengthening and Defending the Mind. *NATO's ACT*.
https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

Hartley III, D. S., & Jobson, K. O. (2021). *Cognitive Superiority: Information to Power*. Springer International Publishing.
https://doi.org/10.1007/978-3-030-60184-3

Huey, L. (2015). This is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming. *Contemporary Voices: St Andrews Journal of International Relations*.
https://doi.org/10.15664/jtr.1159

Janzen, B.-G. J. (2019). What if the Pen is a Sword? Communicating in a Chaotic, Sensational, and Weaponized Information Environment. *PUBLIC AFFAIRS*.

Janzen, J. (2024). THE ROLE OF STRATEGIC COMMUNICATION WITHIN CONTEMPORARY INFORMATION WARFARE. *The Journal of Intelligence, Conflict, and Warfare*. https://doi.org/10.21810/jicw.v6i3.6399

KhosraviNik, M., & Amer, M. (2022). Social media and terrorism discourse: The Islamic State's (IS) social media discursive content and practices. *Critical Discourse Studies*. https://doi.org/10.1080/17405904.2020.1835684

Le Guyader, H. (2022). Cognitive Domain: A Sixth Domain of Operations. In B. Claverie, B. Prébot, N. Buchler, & F. du Cluzel (Eds.), *Cognitive Warfare: The Future of Cognitive Dominance*, NATO Collaboration Support Office. https://hal.science/hal-03635898

Miller, S. (2023). Cognitive warfare: An ethical analysis. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-023-09717-7

Nistor, D. I. A. (2023). Target Audiences' Characteristics and Prospective in Countering Information Warfare. *European Conference on Cyber Warfare and Security*. https://doi.org/10.34190/eccws.22.1.1169

Radu, R. (2025). Building Cyber Resilience to Face the Challenges of Cognitive Warfare. *European Conference on Cyber Warfare and Security*. https://doi.org/10.34190/eccws.24.1.3520

Rudner, M. (2017). "Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror. *Studies in Conflict & Terrorism*. https://doi.org/10.1080/1057610X.2016.1157403

Saari, D., Häkkinen, T., & Moilanen, P. (2024). A Comprehensive Analysis of Narratives within NATO's Doctrines. *European Conference on Cyber Warfare and Security*. https://doi.org/10.34190/eccws.23.1.2240