INFO FLASH
Finabel
The European Land Force
Commanders Organisation

FINABEL - THE EUROPEAN LAND FORCE COMMANDERS ORGANISATION

NOVEMBER 2025

INFOFLASH

From Drones to Doubt: Russia’s Cognitive Attack in Poland

WRITTEN BY
AURORA D’AURIA

EDITED BY
JACKSON ELDER

SUPERVISED BY
ELISE ALSTEENS & KEVIN WHITEHEAD

Introduction

On September 10, 2025, around 20 Russian drones entered the Polish airspace, prompting NATO to launch fighter jets to shoot down the unmanned aircraft (Iwaniuk, 2025). This is one of the first, but growing, instances in which NATO had to open fire on enemy flying objects in EU airspace (Buz, 2025). While the Polish government described this attack as "an act of aggression that created a real threat to the safety of our people," the violation of the country's airspace is only one of the many and increasing Russian disturbances in the EU and its airspace since the beginning of the war in Ukraine (Iwaniuk 2025). Although the number of such kind of incidents has increased over time, what separates the drone incursions on the September 10 from the rest is that they were then followed by a massive "tsunami" of disinformation, which Moscow started with the objective of making it seems like Ukraine was responsible for the attack, "dragging Poles in a war that it is not theirs." (Iwaniuk. 2025). The result of this disinformation attack was devastating. Res Futura, a Polish digital intelligence think tank, analysed the content that flooded the country's digital space and noted that, while 34% of the analysed material blamed Russia for the drone incursion, 38% held Ukrainians guilty for the attacks and a considerable share accused NATO of the strike (Iwaniuk, 2025).

The disinformation campaign in Poland exemplifies the ongoing and long-term effort by the Kremlin to manipulate information in the EU, especially regarding its invasion of Ukraine (Mkaylward, 2024; Krzysztoszek, 2025). This case exemplifies how stand-off provocations are paired with online narratives to conduct a new kind of warfare, illustrating how a drone incursion can be leveraged (often with the use of technological breakthroughs) to seed doubt and strain institutional credibility across the EU (Catena et al., 2025). Against this background, the concept of cognitive security and cognitive warfare is increasingly gaining importance and relevance to understand and counter this new way to conduct war (Catena et al., 2025). This research applies cognitive security and cognitive warfare to better comprehend the aftermath of the Russian stand-off provocation in Poland, arguing that Moscow exploited cognitive vulnerabilities to distort public perception and institutional credibility.

This paper will proceed in structured steps, beginning with an examination of the concepts of cognitive warfare and cognitive security. Then, the paper will provide an in-depth overview of the September 10 drone incident, its immediate online aftermath, and the disinformation narratives, techniques and cognitive mechanisms used by Moscow in the wake of the incursion. The third section will then examine the implications of this cognitive attack for EU security and resilience, paying particular attention to Poland's role in deterrence and the potential for spill-over. This section will also provide policy recommendations to improve the EU's readiness in case of a future cognitive attack and to close its current vulnerabilities. Finally, this research will conclude with a summary of the analysis's main findings.

This paper aims to find that perception, emotion and information flows can be manipulated to achieve strategic effects without confrontation. Here, Russia is placing increasing attention on cognitive sovereignty, eroding public trust, provoking emotional overreaction and fragmenting the EU's societal cohesion. In other words, the core argument of this paper is that the Russian cognitive operation aimed to redirect public attention from an objective reconstruction of the incident, thereby accelerating distrust toward the Polish government, NATO and Ukraine.

This paper argues that strengthening cognitive resilience is therefore crucial for the EU's defence and societal stability.

2. Cognitive Warfare and Cognitive Security

Rapid technological developments are transforming how states and non-state actors conduct warfare, enabling parties to develop, promote, and disseminate propaganda, hostile narratives and disinformation campaigns with greater reach, scope and speed (Casino, 2025; Rickli et al., 2023). Contemporary digital information ecosystems are becoming increasingly complex, exposing vulnerabilities to cognitive warfare and manipulation within EU societies (Rickli & Knappe, 2025). There are multiple examples, such as the hybrid attacks by Russia during Romania's 2024 elections, that underscore how third-party actors can conduct disinformation campaigns to influence Member States' (MSs) political environment, highlighting the difficulties democratic societies face in responding to cognitive attacks (Rickli & Knappe, 2025). While disinformation as a form of warfare is not a new phenomenon, recent years have registered an expansion in the scope and reach of these operations, which, in turn, undermines state legitimacy and information integrity; moreover, and more importantly, this situation creates the perfect conditions for adversaries to conduct cognitive warfare (Rickli & Knappe, 2025).

Cognitive warfare, here described as the "intentional use of information and psychological methods to influence how people think and make decisions aimed at weakening and distorting an individual's or society's ability to perceive reality, understand events and choose rationally" (Du Cluzel, 2021, p. 6-7), is increasingly becoming the alternative to conventional, confrontational warfare (Rickli & Mantellassi, 2023). Through a combination of social media platforms and technological advances (such as artificial intelligence), cognitive warfare can often alter public opinion through purposively spreading misleading information, influencing public debates, and creating public unrest by using divisive artificially originated content (Osavul). Here, it is essential to highlight that one of the main features of this rising kind of warfare is that it aims to control the responses of targets to the presented information rather than the information flow itself (Catena et al., 2025; Claverie & Du Cluzel, 2021).

Cognitive warfare techniques often take the form of psychological manipulation, narrative synchronization and the exploitation of cognitive biases. The first refers to the exploitation of feelings, such as anger and fear, to target cognitive vulnerabilities and reframe the general perception of the incident (Henschke, 2025; Paziuk et al., 2025). The second identifies adversaries aligning manipulative narratives with key geopolitical events, thereby enhancing their resonance and perceived legitimacy, creating the conditions for disinformation to breed and circulate more easily (Marsili, 2023; Paziuk et al., 2025). Finally, the last refers to the exploitation of pre-existing biases and beliefs (confirmation bias), which makes people and societies accept propaganda more easily (Nguyen, 2023; Paziuk et al., 2025).

Furthermore, the rise of artificial intelligence enables the creation of fake yet convincing content that easily gains traction on social media, allowing adversaries to produce persuasive disinformation with minimal effort (Henschke, 2025; Paziuk et al., 2025). As the level of media literacy in the EU is fragmented and non-uniform between the MSs, there are some countries that will be inevitably more exposed to the risks and consequences of cognitive warfare (Jourova, 2023). Consequently, the result is a lower level of EU societal resilience (here defined as the ability of the overall EU population to foresee, withstand and recover from an attack) (Rickli & Knappe, 2025; Lapsley & Vandier, 2025).

Nonetheless, in the age of cognitive warfare, it is possible to improve societal resilience by adopting a cognitive security framework. Cognitive security has been developed under NATO's Allied Command Transformation (ACT), and it is used to understand how adversaries exploit human cognition to manipulate perceptions, disrupt decision-making making and influence behaviour (Catena et al., 2025). This paper defines the concept of cognitive security as "a state and process in which undesired malign influence or manipulation is incapable of altering human cognition" (Rickli & Knappe, 2025, p. 2; Grahn & Taipalus, 2025, p. 8). In this context, "the cognitive security framework focuses on the behavioural and cognitive flaws that allow the manipulation to take place" (Catena et al., 2025, p. 2), with particular attention given to the dangers associated with people's processing of information using pre-existing interpretive narrative frameworks (Catena et al., 2025). Cognitive security aims to safeguard societies and institutions against malevolent online and offline influence. Three components are central to cognitive security: engagement, situational awareness, and resilience (Pierce, 2020). The cognitive security framework aims to ensure that interpretations of events fall within a controlled range (Catena et al., 2025).

Armed with a better understanding of the concepts of cognitive security and cognitive warfare, this paper will next proceed with an analysis of the disinformation campaign conducted in Poland after Russia's incursion into Polish airspace on September 10, 2025.

3. Case Study: Disinformation Campaign Against Poland

Following the Russian drone incursion into Polish airspace on September 10, a surge of social media posts appeared on Polish networks revealing a coherent pattern of strategic information operations. Res Futura analysed around 200,000 messages and social media posts spreading Russian disinformation (between 200-300 social media posts per minute) (Iwaniuk 2025). The content thread was quickly reframed away from technical facts (what flew, where and when) toward blame games and competence attacks on the Polish government and NATO (Res Futura, 2025a). The objective of the Russian cognitive attack was to dominate the discourse with emotions rather than using fact-based argumentation (Res Futura, 2025a). The operation employed repetitive phrases simultaneously spreading different explanations of the same attack (either a Russian strike, a Ukrainian provocation, or domestic government incompetence); it utilized intense emotional language to stir fear, anger and contempt; it reproduced identical phrases from multiple fake accounts to create the impression that a given narrative was the "majority opinion;" it shifted the discussion from information on the physical impacts of the drone incursion; and it attacked NATO's cohesion by spreading the narrative that the alliance will not defend Poland and the country will remain alone (Res Futura, 2025a; Res Futura, 2025b). With this cognitive attack, Moscow did not intend to convince Polish citizens of a single version of events. Instead, Russia's primary goal was to create confusion, polarize opinions and paralyze the decision-making process to divide Polish society (Res Futura, 2025a). The result of this robust Russian outreach campaign produced visible cognitive effects, with early commentary identifying a whopping 38% of social media comments linking the responsibility of the drone attack to Ukraine (compared to 34% identifying Russia as the main perpetrator, 15% the Polish government and 5% NATO and the West) (Res Futura, 2025a).

The success of the Russian disinformation operation relied on exploiting pre-existing cognitive vulnerabilities in Poland. Since 2014, Russia has continuously targeted the country with numerous disinformation campaigns to influence public opinion (Klyszcz, 2024). For example, in 2015, Russia's state-controlled news channel *Sputnik* launched a Polish-language version, which was fundamental in extending the reach of Moscow's disinformation network into Poland (Klyszcz, 2024). The news channel was fundamental in pushing an image of Russia as a stable and militarily strong partner, the US as unpredictable and instilling fear among (Polish) citizens, which, in turn, makes them easier to manipulate (Mierzynska, 2018).

From a cognitive security perspective, the drone invasion can be described as a spark that created a knowledge gap. Instead of attempting to win a fact-based argument, Moscow's strategy focused on how Polish citizens interpreted events, encouraging them to digest information quickly and emotionally rather than to make slow, evidence-based decisions (Golebiewski & Boyd, 2018). Here, the cognitive security framework emphasizes that manipulation works by exploiting those predispositions and frames, not just by spreading lies (du Cluzel, 2021). As observed in the Polish case, Moscow captured and moulded the interpretation space: the agenda moved from air-defence facts to government distrust and alliance doubt, achieving an asymmetric informational success at minimal cost and with possible spill over to other Member States' information ecosystems (Res Futura, 2025a). Here, it is possible to observe the use of common cognitive warfare techniques, such as the exploitation of pre-existing beliefs and opinions on Ukraine, recognizable historical references and the use of strong emotions (in particular, anger) to allow Moscow's disinformation to move through and contaminate the Polish digital information ecosystem easily. In turn, this led audiences to believe emotionally compelling but incorrect narratives that resonate more with individuals than evidence-based updates (Berger & Milkman, 2011; Paul & Matthews, 2016; Res Futura, 2025a). By poisoning the information ecosystem with contradicting explanations, Moscow successfully diminished the persuasive power of government and NATO statements, which appeared as just another voice in the noise, while eroding the public's trust and support for Ukraine (Res Futura, 2025b; Res Futura, 2025a; Paul & Matthews, 2016). Additionally, this cognitive attack allowed Russia to obtain an asymmetrical information victory, as the country achieved its goals (to manipulate, confuse and divide) without using brute force or incurring any military casualties (Res Futura, 2025b).

To conclude this section, the drone attack was used not only as a military attack but primarily as a tool of cognitive warfare, in which the primary arena of activity is the information space. Next, this paper will analyse how this cognitive attack impacts the broader EU's security and resilience.

4. Implications for EU Security & Recommendations

The September 10 attack highlights the need to secure a strong Poland, which is crucial to bolstering EU resilience to future cognitive operations. Poland is not just a frontline state; it is a fundamental element of EU and NATO deterrence (Kvasha 2025; Surwillo & Slakaityte, 2024). Poland's geographic position between Russia and Belarus, its logistics infrastructure (such as the POLLOG Hub in Rzeszów), and the highest defence spending in NATO (around 4.7% of GDP in 2025, up from 2.4% in 2022) make Warsaw a strategic centre of the EU's security and resilience (Kvasha 2025). On May 9, 2025, the country also signed the Treaty of Nancy with France, ushering in a new era of EU defence cooperation (Torbicka, 2025). Together, these elements make Poland a key node in the EU's protection and a high-value target for cognitive operations. In fact, the country's security is often challenged by numerous threats and destabilization linked to the Kremlin's hostile strategies (Torbicka, 2025). In this sense, cognitive warfare can destabilize Poland's position as one of the main actors in the development of EU defence (Surwillo & Slakaityte, 2024). Russia overwhelms the Polish digital information ecosystem with conflicting, emotional narratives, turning the response into a fight over what the incident means rather than what to do next. This, in turn, leads to decision latency (hesitancy on thresholds and public warnings) and coordination friction between local authorities, uniformed services, and political leaders (Paul & Matthews, 2016).

Cognitive attacks targeting Warsaw do not stay within national borders but often spill across the EU, affecting MSs' information ecosystems and cognitive landscapes (Boksa, 2019; European External Action Service (EEAS), 2024).

The European Union's open information landscape exposes Poland (and other MSs) to key vulnerabilities. Disinformation can cross national borders due to fragmented media oversight across Member States, and policy initiatives are mostly developed at the national level (Ariton, 2025). While the EU is aware of its vulnerability and has started to strengthen its resilience to cognitive warfare (for example, by adopting the Strategic Compass in 2022 or developing a hybrid strategy), its adoption and implementation are hindered by institutional fragmentation, legal limitations, and technological dependencies (Ariton, 2025; Catena et al., 2025). Another major challenge created by cognitive warfare is that different MSs have different threat perceptions and response capacity; while some countries (such as Sweden) have adopted long-term and proactive measures due to past exposure to Russian propaganda and disinformation, others (such as Austria) have yet to implement similar programs (Ariton, 2025). The differences in national approaches negatively impact the development of a coordinated EU cognitive security strategy (Ariton, 2025; Karami & Dastenaei, 2024).

To create an environment where EU citizens and institutions are prepared to detect, withstand and recover from future cognitive attacks, this paper proposes the following policy recommendations:

I. Introduce EU-level cognitive resilience framework: As cognitive warfare is becoming a prominent element in the war state and non-state actors conduct war, the EU has to develop and adopt a new approach to guard itself from this rising warfare kind. Here, it would be essential to develop an overall framework that allows the European Union to efficiently conduct threat assessments, set cognitive benchmarks and set up an operational team that can swiftly act in case of a cognitive attack. This could be done either as part of pre-existing regulation (such as ReArm Europe or the Strategic Compass) or as a new piece of legislation (Catena et al., 2025).

II. Increase Member States' resilience: As cognitive warfare is often directed towards governments and national institutions, it is crucial to build up MSs' cognitive defences. The EU should provide founding to MSs (through the European Defence Fund, for example) to ensure that they have enough resources to launch research and initiatives aimed at understanding the different vulnerabilities and strong points specific to each MS, promote collaboration, lower costs and prevent duplication (Rickli & Mantellassi, 2023).

III. Strengthen citizen-level defences: As the consequences of cognitive warfare are detrimental to citizens, it is imperative that the EU set up and roll out academic courses (at any level, so from elementary schools to university programs) to improve the level of the EU's media literacy. The syllabus should allow students and civilians to understand the information environment, identify the sources of disinformation, the different tactics used by different actors, and effectively conduct debunking (or the process of exposing deceptiveness or that a piece of information is less important/ good/true than it has been made to appear to prevent the spread of disinformation) and fact-checking (or the act of ensuring that all facts in any form of text/news/writing are correct to promote the accountability of governments, think tanks, or any kind of institutions) to delimitate the consequences of a future cognitive attack (Pamment & Lindwall, 2021).

5. Conclusion

This paper analysed the aftermath of the Russian drone incursion on September 10, 2025, highlighting how Moscow exploited pre-existing biases and vulnerabilities to confuse and manipulate Polish perceptions of the incident (Iwaniuk, 2025; Paziuk et al., 2025; Claverie & du Cluzel, 2021). By applying the concepts of cognitive security and cognitive warfare, this paper has shed light on how a stand-off provocation was paired with a disinformation campaign that seized and divided Poland's digital information ecosystem (Res Futura, 2025a; Res Futura, 2025b). Moscow employed fast, emotionally charged claims that outpaced verification to stoke fear and anger and push audiences to accept artificial stories over slower, factual reporting. Additionally, repetition and inauthentic amplification turned doubt into a perceived consensus, leading to confusion, polarization and decision latency (Paul & Matthews, 2016; Berger & Milkman, 2011; Res Futura, 2025a).

The paper also highlighted how Poland's strategic position exposes it to cognitive attacks, which, in turn, raises the risks of spill over across the EU's open, unevenly protected information ecosystem (Surwillo & Slakaityte, 2024; EEAS, 2024; Ariton, 2025).

This research argued for the development of an EU-level cognitive resilience framework (either to be integrated with existing defence instruments or developed as a new piece of legislation); sustained support for Member-State capabilities to map vulnerabilities and coordinate rapid response; and long-term citizen education to raise media literacy and debunking capacity (Catena, 2025; Rickli & Mantellassi, 2023; Rickli & Knappe, 2025; Pamment & Lindwall, 2021).

Preserving institutional trust and collective calm under pressure is essential to deny adversaries low-cost asymmetric wins and to enhance the EU’s readiness when the next cognitive provocation arrives (EEAS, 2024; Rickli & Knappe, 2025).

Bibliography

Ariton, L. (2025). Cognitive warfare in the Digital Age: Implications for EU security policy. *International Conference Knowledge-Based organization, 31*(1), 1–9. https://doi.org/10.2478/kbo-2025-0001.

Berger, J. & Milkman, K. L. (2011). What makes online content viral? In *Journal of Marketing Research*. https://doi.org/10.1509/jmr.10.0353.

Boksa, M. (2016). Russian information warfare in Central and Eastern Europe: Strategies, impact, countermeasures. In *The German Marshall Fund of the United States*. https://www.gmfus.org/sites/default/files/Russia%20disinformation%20CEE%20-%20June%204.pdf.

Buz, S. (2025, October 9). *Russian drones in NATO airspace: Probing leads Europe to 'Drone wall'*. SETA. https://www.setav.org/en/russian-drones-in-nato-airspace-probing-leads-europe-to-drone-wall.

Casino, F. (2025). Unveiling the multifaceted concept of cognitive security: Trends, perspectives, and future challenges. In *Technology in Society*. https://doi.org/10.1016/j.techsoc.2025.102956.

Catena, B. (2025). Smoke and Mirrors: Building EU resilience against Manipulation through Cognitive Security. In *European Union Institute for Security Studies*. https://www.iss.europa.eu/publications/briefs/smoke-and-mirrors-building-eu-resilience-against-manipulation-through-cognitive.

Cheplyk, R. (2025, March). *NATO takes control of arms transfers to Ukraine and military training in Poland.* GT Invest. https://good-time-invest.com/blog/nato-takes-control-of-arms-transfers-to-ukraine-and-military-training-in-poland/#:~:text=1.,NATO%20Mission:%20NSAT%2DU.

Claverie, B. & Du Cluzel. (2021). *Cognitive Warfare: The future of Cognitive Dominance*. NATO-STO Collaboration Support Office. https://www.researchgate.net/publication/359991886_Cognitive_Warfare_The_Advent_of_the_Concept_of_Cognitics_in_the_Field_of_Warfare.

Du Cluzel, F. (2021). Cognitive Warfare: the Weaponisation of Neurosciences. In *Innovation Hub* (pp. 1–45). https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf.

European External Action Service (EEAS). (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. https://euneighbourseast.eu/wp-content/uploads/2024/01/eeas-2nd-report-on-fimi-threats-january-2024_0-compressed.pdf.

Grahn, H. & Taipalus, T. (2025). Defining Comprehensive Cognitive Security in the Digital Era: Literature review and concept analysis. In Journal of Information Warfare, *Journal of Information Warfare* (Vols. 24–24, Issue 2, pp. 39–59). https://www.jinfowar.com/journal/volume-24-issue-2/defining-comprehensive-cognitive-security-digital-era-literature-review-concept-analysis.

Golebiewski, M. & Boyd, D. (2018). Data Voids. In *DATA VOIDS*. https://datasociety.net/wp-content/uploads/2019/11/Data-Voids-2.0-Final.pdf.

Henschke, A. (2025). *Cognitive Warfare: Grey Matters in Contemporary Political Conflict*. Routledge: London, UK. https://doi.org/10.4324/9781003126959.

Iwaniuk, J. (2025, October 8). Poland hit by unprecedented disinformation attack following Russian drone incursion. *Le Monde.fr*. https://www.lemonde.fr/en/international/article/2025/10/08/poland-hit-by-unprecedented-disinformation-attack-following-russian-drone-incursion_6746208_4.html.

Jourova, V. (2023). The Media Literacy Index 2023. In *Measuring Vulnerability of Societies to Disinformation*. https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf.

Karami, A. & Mottaghi Dastenaei, A. (2024). The European Union's approach to cognitive warfare's command and control. In *J. Electrical Systems* (Vols. 20–11s, pp. 2721–2734).

Klyszcz, I. (2024). *Shadow War: What Estonia and Poland tell us about Russia's clandestine operations in Europe*. Brussels School of Governance - CSDS. https://csds.vub.be/publication/shadow-war-what-estonia-and-poland-tell-us-about-russias-clandestine-operations-in-europe/.

Krzysztoszek, A. (2025, May 15). The Kremlin's information war: Manipulating minds from Ukraine to Europe. *EURACTIV.pl*. https://euractiv.pl/section/ue-fact-checking/special_report/the-kremlins-information-war-manipulating-minds-from-ukraine-to-europe/

Kvasha, K. (2025, March 6). *"Security, Europe!": Poland's rise as NATO's defence spending leader.:* Wilson Center. https://www.wilsoncenter.org/article/security-europe-polands-rise-natos-defense-spending-leader.

Lapsley, A. & Vandier, P. (2025). Resilience Reference Curriculum. In *NATO Headquarters*. https://www.nato.int/nato_static_fl2014/assets/pdf/2025/2/pdf/DEEP-resilience-reference-curriculum.pdf.

Marsili, M. (2023). Guerre à la carte: Cyber, information, cognitive warfare and the metaverse. *ACIG* 2, 1–15. https://doi.org/10.60097/ACIG/162861.

Mierzynska, A. (2022, November 14). Siewcy strachu. 10 dni z rosyjską propagandą w Polsce. "To są żołnierze w walce informacyjnej." *Oko Press*. https://oko.press/siewcy-strachu-10-dni-z-rosyjska-propaganda-w-polsce-to-sa-zolnierze-w-walce-informacyjnej.

Mikhailov, D. (2025, July). *Russian intelligence recruits refugees and migrants in NATO countries for espionage*. The Jamestown Foundation. https://jamestown.org/program/russian-intelligence-recruits-refugees-and-migrants-in-nato-countries-for-espionage.

Mkaylward. (2024, February 29). *Undermining Ukraine: How Russia widened its global information war in 2023 - Atlantic Council*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/.

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

Nguyen, T. N. (2023). Accelerated cognitive warfare via the dual use of large language models. *Preprints.* https://doi.org/10.20944/preprints202312.2279.v1.

Osavul. (2025, October 17). *Cognitive Security explained: How to protect the human mind.* https://www.osavul.cloud/blog/cognitive-security-how-to-protect-the-human-mind.

Pamment, J., Lindwall, A. K., Leon Klingborg, Ben Heap, Quentin Wight,& Kārlis Ulmanis. (2021). *Fact-Checking and Debunking: a Best Practice Guide to Dealing with Disinformation*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_coe_fact-checking_and_debunking_02-02-2021-1.pdf.

Paul, C. & Matthews, M. (2016). *The Russian "Firehose of Falsehood" propaganda model: why it might work and options to counter it.* RAND Corporation. https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.

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*, *8*. https://doi.org/10.3389/frai.2025.1566022.

Pierce, B. (2020). *A wicked problem about thinking: cognitive security*. Media at Stanford University. https://mediax.stanford.edu/program/thinking-tools-for-wicked-problems/a-wicked-problem-about-thinking-cognitive-security/#:~:text=Cognitive%20Security%20is%20presented%20in,%2C%20situational%20awareness%2C%20and%20engagement.

Res Futura. (2025a, September 10). *10.09.2025 |Raport Specjalny | Data House Res Futura - Res Futura*. Res Futura. https://resfutura.pl/polska100925/.

Res Futura. (2025b, September 16). *16.09.2025 |Polska| Data House Res futura - Res Futura*. Res Futura. https://resfutura.pl/145400-2/.

Rickli, J.-M. & Knappe, T. (2025). Enhancing cognitive security and societal resilience to counter cognitive warfare. In *Geneva Centre for Security Policy* (pp. 1–3).

Rickli, J.-M., Mantellassi, F. & Glasser, G. (2023). *Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st century*. Geneva Centre for Security Policy.

Surwillo, I., Slakaityte, V., & Danish Institute for International Studies. (2024). *Power moves east: Poland's rise as a strategic European player*. Dansk Institut for Internationale Studier.

Torbicka, K. (2025). Poland's Security in the 21st Century: Challenges, Strategies and Prospect. In *Fondation pour l'innovation politique.*