Military Leadership in the Age of Cognitive Warfare

Mikko Salminen
Finish National Defence University, Helsinki, Finland

mikko.k.salminen@mil.fi

Abstract: In many definitions of cognitive warfare, it is highlighted that the target is human mind, and not only the contents of it but the various cognitive processes, such as attention and decision making. The aim in cognitive warfare is often defined to be the influencing of how individuals think, not what they think. Social media is often mentioned as one of the main platforms by which these cognitive influence operations are conducted, possibly enhanced with big data analytics and artificial intelligence (AI) tools. In some definitions it is also included, that in addition to behavioral and cultural sciences, also the exploiting of neuroscience for even more effective and more precisely targeted influences on individual cognition could be considered. The intertwined cognitive, technological, and information dimension form new types of threats which call for a close evaluation of possible effects and countermeasures. The DOTMLPF-I framework (Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities, Interoperability) is used in armed forces to guide capability development. This study is a conceptual analysis within these dimensions, with the focus on Leadership and Education dimensions and how they should adapt to face these new types of threats. Military leadership is expected to be fast rational decision-making under uncertainty. However, cognitive warfare challenges this with disinformation and emotional manipulation, for example. Introducing AI functionalities to decision support systems may enhance situational awareness and decision-making speed, but the algorithms may be biased and the systems may operate in a non-transparent way, thus eroding trust towards them. Resilience against effects of cognitive warfare requires training in media literacy and critical thinking, but also in emotional skills. The forming of situational understanding is one of the main targets in cognitive warfare and it should be supported with specialized training, for example by targeting the underlying cognitive processes of forming situational understanding. For this purpose, cognitive training should be targeted to, for example, attention control, working memory, and mental flexibility. In the current manuscript the challenges posed by cognitive warfare to military leadership are reviewed with suggested solutions.

Keywords: Cognitive warfare, Military leadership, Leadership training, Information warfare, Psychological warfare

1. What is Cognitive Warfare?

Cognitive warfare has been defined as a new concept in military sciences and defence studies. Central to various definitions of this concept have been the using of human cognition and new technologies for influencing decision making and behavior (Deppe & Schaal, 2024). The term cognitive refers in the various definitions to influencing human cognitive processes, such as perception, attention, memory, and eventually, decision making. By no means, the concept of influencing adversary thinking is not a new idea and psychological operations have been part of military strategy for ages. The novelty in the concept of the cognitive warfare comes (supposedly) from utilization of recent research on cognitive science and the neurosciences, and from the new technologies. Often artificial intelligence (AI) and social media platforms are mentioned as new technologies, but some scholars have also identified connections to even neurotechnology and nanotechnology (Grigsby et al., 2023; Claverie & Du Cluzel, 2022; Morelle et al., 2023).

Cognitive warfare is presented as some kind of a paradigmatic shift in modern conflicts, targeting the human cognitive processes instead of (merely) influencing opinions. This can be seen in definitions such as the one by Claverie & Du Cluzel (2022), who write that: “The stated objective is to attack, exploit, degrade or even destroy how someone builds their own reality, their mental self-confidence, their trust in processes and the approaches required for the efficient functioning of groups, societies, or even nations.”

The field of study of cognitive warfare is still new and there are varying definitions of the phenomenon. Even if these definitions share some similarities, most of them mentioning cognitive processes and new technologies, there are still differences. This might hinder not only the academic study of the field, but also doctrinal work and preparing. Many scholars and analysts agree on the fact that there are new and developing ways to use information technologies as an attack vector for influencing both decision makers and also the public opinion. These operations are labeled as influence operations, cyber-enabled influence operations, or next-generation psychological warfare (Hoffman, 2025), for example. Advances in AI, big data analytics, and neurotechnology enable various capabilities for attacking and defensive cognitive warfare, ranging from using AI for personalized disinformation campaigns to brain-computer interfaces for monitoring stress responses and thus adapting user interfaces of future systems. Cognitive warfare raises also unprecedented ethical challenges by targeting subconscious processes and potentially violating human autonomy.

It is true that technological developments are constantly offering new and more efficient ways for influencing the decision makers and targeted populations. However, it is debatable whether these developments in technologies are such that they entitle the defining of new type of warfare. It is justified to ask what exactly "cognitive warfare" adds beyond "political warfare" (Armstrong, 2025) or some other concept. In addition, cognitive warfare should be positioned in relation to psychological warfare, information warfare, and psychological operations (Ibrahim et al., 2023). The concept of cognitive warfare should be studied critically, with a focus on forming a sound and useful definition, that is needed for both advancing the academic study of the field but also strategic and operative preparing for these new types of threats (e.g., Bebber, 2025).

An interesting direction for more tangible definition of cognitive warfare may be reached by defining the properties, actions, and operations of cognitive warfare. One such example is the set of three defining features for cognitive warfare actions, proposed by Morelle and colleagues (2023). First, the purpose of the action should be "broader than what is immediately apparent". The authors present an illustrative example where a cyberattack is actually targeted to erode trust towards the bank. Second, the action has a diffuse nature, that is, the action is part of a strategy consisting of various different actions and different means that construct a chain reaction where it is difficult to identify the origin of the attack and to estimate the long-term effects. Third, the target of the actions is cognition. This interesting approach to form a definition offers tangible aspects that can be further identified from actual events from recent history. Even if there is still no standard or a widely accepted definition for cognitive warfare, it is suggested that the different definitions share the formulation that as the methods to influence evolve from traditional propaganda to AI-enhanced influence operations, there is a significant shift in the character of these operations and new approaches and competences may be needed also from military leadership.

This study is a conceptual analysis on how military leadership is challenged by cognitive warfare.

1.1 Ways of Cognitive Warfare

Some recent events that have been labeled in the literature as representing or including elements of cognitive warfare are election manipulation in Baltic countries during 2018-2019, annexation of Crimea in 2014, Russian narrative on repressions of ethnic Russians in Georgia and Ukraine after the annexation of the Crimea, and the Chinese disinformation campaign with the narrative that Taiwan is and will be part of China (Fenstermacher et al., 2023). All these events include actions and operations on various domains, and cognitive warfare is merely a one viewpoint to these totalities. It must also be noted, that the time-line of cognitive warfare doesn't always line with the more traditional or kinetic operations. Means of cognitive warfare may be used to prepare the battlespace, for example there are notions of Russian agents intending to coordinate unrest in Crimea before the annexation (Fenstermacher et al., 2023).

Decision making is a central function in military leadership. In the research literature there have been identified groups of objectives of cognitive warfare that are related to decision-making. These include leading of the enemy into taking a certain course of action, influencing the enemy's decision-making process and thus leading to bad decisions and possibilities to exploit these, weakening the enemy's decisions so that they end up being delayed or lacking initiative, protecting of one's own decision-making from enemy influence, and enhancing one's own capability for decision making (Sattler, 2023). Cognitive warfare methods can be used to attack decision making capability directly or more indirectly by influencing the environment in which the decisions are made, by manipulating troop morale or public opinion, for example (Sattler, 2023). The shaping of the decision space prior to and during the operation has been identified as one of the key factors in modern conflicts (Reczkowski & Lis, 2022). This makes countering cognitive warfare difficult, the indirect effects may be built over longer periods of time and may become visible when it is already too late.

The various methods of cognitive warfare challenge leadership and military decision-making in many ways. For example, the Russian reflexive control, or conveying to the opponent information with a goal to incline them to voluntarily make a pre-determined decision (Thomas, 2004). These influence operations may be difficult to detect, especially if conducted utilizing new technological means, for example by automated social media bot farms to build and spread narratives with memes (e.g., Ferrara et al., 2016; Munk, 2025), possibly using false information and emotionally engineered content for more effective spreading (Brady et al., 2017; Vosoughi et al., 2018;) or using personalized attacks to identified target individuals (Matz et al., 2017), possibly even mobilizing crowds against them (Rahman, 2024). Russian propaganda is typically rapid, continuous and repetitive. This is an effective approach, since first impressions tend to be resilient, and repetition leads easily to familiarity and then to acceptance (Paul & Matthews, 2016).

One way to counter these types of actions is the increasing of training on digital media literacy and critical thinking skills of the staff, and also including to the decision-making process check points for considering alternative courses of action and wargaming their effects.

2. Effects of Cognitive Warfare and how to Mitigate Them

There are already some practices and examples that are proposed to act as defensive mechanisms against of diminish effects of cognitive warfare. These methods can be classified by the DOTMLPF-I framework, which stands for Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability, and is widely used in western militaries when planning to build capabilities (NATO, 2016). Regarding the **Doctrine**, the forthcoming NATO Cognitive Warfare Concept (NATO ACT, 2024) will likely formalize and harmonize the definition of this phenomenon across allied nations and also serve doctrinal development work. In another essay, primary lines of effort were identified for cognitive-security strategic approach (Cheatham et al., 2024). The authors suggested that the U.S. Department of Defence should, through the Joint Staff, lead the work of integrating the cognitive domain to the joint doctrine and also that cognitive warfare training should be included at every echelon.

An example of the **Organization** category is the Swedish Psychological Defence Agency, which was established to coordinate and develop the operations of agencies in psychological defence. Cognitive warfare may affect both the armed forces and also the civilian society, this leads to need for different agencies, departments and ministries to collaborate effectively on the topic and the management structures should support this. One example of building resilience towards wide range of threats, including hybrid threats, is the Finnish comprehensive national defence, a model of cooperation to secure society's vital functions mobilizing the whole society (e.g., Sederholm, Rannikko & Salo, 2025).

For **Training** there are examples of various training programs to enhance, for example, digital media literacy skills that build resilience against cognitive warfare (e.g., Nygren et al., 2021). Developments in the **Materiel** category include, for example projects to build AI capabilities in decision support systems, where safety is considered even if there might be strong desire and hurry for ready systems (Probasco et al., 2025). Another, more futuristic example is the combining of nanotechnology, biotechnology, information technology, and cognitive technology for ultimately constructing augmented human operators (Claverie & Du Cluzel, 2022). These types of augmentations may enhance resilience against effects of cognitive warfare, but also open up new types of attack vectors for targeting cognitive processes.

For **Leadership & Education** there are ongoing programs to build soldiers and leaders cognitive resilience (Andoh, 2025). Leaders should be active in informing their team members on the impacts that new technologies and social media-evoked cognitive biases could have and to facilitate training in topics such as mindfulness and cognitive reappraisal techniques. In addition, the leaders should work to increase digital and media literacy training to increase resilience against hostile influence operations (Cheatham et al., 2024).

In the model of Herlihy (2022) the direct approach to cognitive dominance includes brain education, cognitive science-based learning, and managing information overload. Technological interventions are included also. Education and learning should include topics such as metacognition and thinking skills, the author suggests that these could be fostered by offering education on the functioning of the brain and also training in mindfulness skills. For the cognitive science-based learning the author proposes intelligent tutoring and increasing of the tacit knowledge or durable knowledge in long-term memory of the soldier to support critical thinking skills. Managing information overload is suggested to be supported by a change in the culture of "always on", where real-time availability is expected from the leaders, and also by offering education on effects of multitasking, interruptions, information overload, and time-management skills. These changes would affect various levels and functions of military organizations and for a successful change to occur, a change in the culture would be needed, where the promoting of cognitive capabilities are central to achieve cognitive dominance. And it is the task of leaders in all echelons to support and coordinate the building of such a culture.

The increasing digitalization of the warfare may lead to increasing demands for human decision making. Decision making is required to be made at "post-human speed", thus leading to increased demand for AI-based solutions (Crilly, 2022). In addition, Crilly (2022) suggest that in future post-digital hyper-war leaders would increasingly need competencies such as ingenuity, intellect, media-savviness, and legal and digital competencies. Due to these requirements, the author also suggests that younger generations of leaders should be given a more prominent role in leading future wars, implying that more senior leaders may not be

experts in the new type of warfare. It is true that military leadership relies on rapid, rational decision-making under uncertainty. Cognitive warfare undermines this process by introducing misinformation, deepfakes, and emotional manipulation (Qureshi & Khan, 2024). Research demonstrates that emotional disruption significantly impairs judgment, increasing susceptibility to adversarial influence (Bakir & McStay, 2020; Bakir et al., 2024). Targeted narratives can be used to erode trust within command structures, delaying critical decisions. The psychological toll on leaders and troops further exacerbates operational risks. Practicing of decision-making is simulations with induced stress and cognitive challenges has been suggested as a one way to increase decision-making resilience against cognitive warfare (Sattler, 2023).

Situational understanding refers to the ability to perceive, comprehend, and project the status of the operational environment to support decision-making (Endsley, 1995). In military contexts, this skill is essential for mission success and operational adaptability. The concept of situational understanding builds upon Endsley's (1995) model of situation awareness, which includes perception, comprehension, and projection. Military doctrine emphasizes that situational understanding extends beyond awareness by, for example, integrating critical thinking, collaboration, and predictive analysis (U.S. Army, 2019). Teaching situational understanding requires a combination of cognitive and experiential methods. Classroom instruction can introduce theoretical models and decision-making frameworks. Case-based learning and historical scenario analysis help students recognize patterns and anticipate outcomes. Simulation-based training is one of the most effective methods for developing various managerial skills. Virtual and constructive simulations immerse trainees in complex environments, requiring real-time assessment and decision-making (Salas et al., 2009). Live exercises and wargaming further reinforce these skills by replicating uncertainty and operational stress (U.S. Army, 2019). It is suggested that to build resilience against cognitive warfare, there should be dedicated training for situational awareness and understanding, and also for decision making. The guidelines for situational awareness training and education by Endsley and Jones (2011) could be used when creating and evaluating such programs.

Cognitive training programs, such as those focusing on attention control, working memory, and mental flexibility, enhance the underlying processes that support situational understanding (Blacker et al., 2019). Techniques like red teaming and structured analytic methods encourage critical thinking and challenge assumptions. Advances in artificial intelligence and adaptive learning systems enable personalized training for situational understanding. Intelligent tutoring systems can assess learner performance and adjust scenarios dynamically to target weaknesses (Bell & Kozlowski, 2008). Overall, situational understanding is a multifaceted skill that can be taught and trained through a blend of theoretical instruction, experiential learning, and cognitive enhancement. Military organizations should invest in simulation technologies, adaptive learning platforms, and critical thinking programs to prepare leaders for complex operational environments.

For **Personnel** there are developments for continuous cognitive monitoring for every soldier (Gillis, 2024).

In an integrated approach to cognitive dominance Herlihy (2022) presents both indirect and direct approach for expanded cognitive capability and optimized cognitive performance. Indirect approach includes methods such as talent management, and physiological and pharmacological interventions. Regarding the talent management the author suggests more refined methodology for assessing the individuals' cognitive traits and capabilities during recruiting. In addition to more traditional assessment tools also neuroimaging is suggested. For the physiological interventions the author refers to previous studies that have shown the effect that physical training, nutrition, and sleep have on cognitive functions. Pharmacological interventions could be conducted using various types of stimulants, from caffeine to prescribed medicine to increase cognitive performance and alertness during long missions. Wearable devices are offered as one possible solution in supporting behavioral change, for example for better sleeping habits. Other technological interventions include neurotechnology, such as electro-magnetic stimulation to induce better sleep quality.

For **Facilities** there are synthetic training environments for various types of training (Marino, 2025).

Cheatham and colleagues (2024) suggested to develop defensive mechanisms and tools, for example AI tools that would help in identifying patterns of disinformation and to disrupt hostile attempts to influence the information environment. The integration of artificial intelligence into command and control (C2) systems introduces both opportunities and vulnerabilities. AI-driven decision-support systems promise, for example, enhanced situational awareness but raise concerns about algorithmic bias (e.g., Probasco et al., 2025). NATO's cognitive command initiatives aim to turn traditional command and control structure and systems with AI-functionality to a more predictive, adaptive, and resilient system (Großwald Systems, 2025). Finally, **Interoperability** is strengthened by multinational planning tasks and exercises. There are already, for example,

commercial software that can be used in such large multinational exercises for simulating information environment (Bergh, 2023), for more realistic training against threats of cognitive warfare.

3. Discussion

Cognitive warfare represents a transformative challenge for military leadership, shifting the locus of conflict from physical domains to the human mind. Answering to this threat requires theoretical and doctrinal clarity, technological safeguards, dedicated training and education, and also leadership and decision-making resilience. By prioritizing these areas, military organizations can preserve decision-making integrity and operational effectiveness in the era of cognitive warfare.

Cognitive warfare imposes also profound organizational, doctrinal, and psychological challenges. Applying DOTMLPF-I enables comprehensive mitigation through doctrine adaptation, organizational restructuring, training, technological safeguards, and interoperability. Whole-of-government support and continuous wargaming of possible futures are critical to maintaining military effectiveness in an era where war is fought in minds and on battlefields. Professional military education must also evolve to address cognitive threats. There are ethical dilemmas related to influence operations, particularly regarding civilian populations. Balancing operational effectiveness with international law and ethical standards remains a challenge for leadership. Integrating cognitive security modules into education and training can prepare leaders for these complexities. Cognitive warfare exploits psychological vulnerabilities, eroding trust within units and between allies. Deepfake technologies and AI-generated contents may amplify these effects and create constant uncertainty. Building cognitive resilience requires comprehensive training in media literacy, emotional regulation, and critical thinking. Leadership development programs must incorporate these competencies to build resilient decision-making. Organizational resilience also depends on fostering a culture of adaptability.

The convergence of psychological, technological, and informational dimensions in cognitive warfare demands a holistic response. Military leadership must navigate various new and emerging issues. Collaborative frameworks between allies to build cognitive resilience, and effective using of the new technologies for defensive purposes are needed to mitigate risks. Future research should explore standardized definitions, cross-cultural training programs, and ethical frameworks for cognitive operations. Failure to adapt could result in strategic paralysis and erosion of public trust in defense institutions.

State and also non-state actors use cognitive operations for their strategic objectives. In future battleground cognitive dominance can be achieved, for example, by AI-enabled influence operations, targeting both military and civilian populations. Every military leader is a target of cognitive warfare, but so are their subordinates and also the people of the civilian society, with whom the wars are fought. Cognitive warfare poses various old and also new challenges to military leadership. Situational understanding and evaluating of the future become increasingly difficult under the operations of cognitive warfare. Uncertainty of the situation and suspicion towards information slows down decision making and burdens leaders and decision makers. The uncertainty may be evoked between leaders and their subordinates, between military and the civilian society, between allies from different nations, and towards information from various sources, from allies or from own sensors and intelligence functions.

These all developments have an effect to the military leadership, as leaders are the ones leading and coordinating work for preparedness. Every leader has to be familiar with threats from social and digital media. Depending on the hierarchical level or echelon, the threats vary and so do the responsibilities of the leader, whether they are about watching for mobile phone and social media use of the subordinates or the forming and supervising of higher order communication strategies. A shared task and role for leaders in all echelons is to act as mediators of situational understanding and also as pedagogical leaders in coaching the subordinates and team members in their task of becoming more proficient in forming situational understanding to enable efficient decision-making and action.

Ethics and AI declaration: Ethical clearance was not required for the current research according to the national laws and regulations. No artificial intelligence (AI) tools were used for writing this paper.

References

Andoh, E. (2025) Building mental strength in the military. American Psychological Association. Available at: https://www.apa.org/monitor/2025/11-12/mental-strength-military. (Accessed: 26 November 2025).

Armstrong, M. (2025) "Cognitive Warfare" fails the cognitive test. Available at: https://mountainrunner.substack.com/p/cognitive-warfare-fails-the-cognitive. (Accessed: 26 November 2025).

Bakir, V., Laffer, A., McStay, A., Miranda, D., and Urquhart, L. (2024) On manipulation by emotional AI: UK adults' views and governance implications. Frontiers in Sociology, Vol 9, 1339834. https://doi.org/10.3389/fsoc.2024.1339834

Bakir, V., and McStay, A. (2020) Empathic media, emotional AI, and the optimization of disinformation. In Affective politics of digital media (pp. 263-279). Routledge.

Bebber, J. (2025) China is waging cognitive warfare. Fighting back starts by defining it. Defense One. Available at: https://www.defenseone.com/ideas/2025/03/china-waging-cognitive-warfare-fighting-back-starts-defining-it/403886/. (Accessed: 26 November 2025).

Bell, B. S., and Kozlowski, S. W. J. (2008) Active learning: Effects of core training design elements on self-regulatory processes, learning, and adaptability. Journal of Applied Psychology, Vol 93, pp 296-316.

Bergh, A. (2023). Chapter 11 – SOMULATOR: Developing cogwar resilience through social media training. Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-ET-356.

Blacker, K. J., Hamilton, J., Roush, G., Pettijohn, K. A., and Biggs, A. T. (2019) Cognitive training for military application: a review of the literature and practical guide. Journal of Cognitive Enhancement, Vol 3, No. 1, pp 30-51. https://doi.org/10.1007/s41465-018-0076-1

Brady, W. J., Wills, J. A., Jost, J. T., Tucker, J. A., and Van Bavel, J. J. (2017) Emotion shapes the diffusion of moralized content in social networks. Proceedings of the National Academy of Sciences, Vol 114, No. 28, pp 7313-7318. https://www.pnas.org/doi/pdf/10.1073/pnas.1618923114

Cheatham, M. J., Geyer, A. M., Nohle, P. A., and Vazquez, J. E. (2024) Cognitive warfare: the fight for gray matter in the digital gray zone. Joint Force Quarterly, Vol 114, No. 2, pp 83-91. https://digitalcommons.ndu.edu/joint-force-quarterly/vol114/iss2/15

Crilly, M. (2022) Prosecuting the post-digital hyper-war: Preparing for the upcoming war of decision superiority and cognitive dominance. The RUSI Journal, Vol 167, No. 4-5, pp 78-82. https://doi.org/10.1080/03071847.2022.2144431

Claverie, B. and du Cluzel, F. (2022) Cognitive warfare: The advent of the concept of cognitics in the field of warfare. In: B. Claverie et al., eds. Cognitive warfare: The future of cognitive dominance. Brussels: NATO Science and Technology Organization, pp 2-1–2-8. Available at: https://hal.science/hal-03635889/document. (Accessed: 26 November 2025).

Deppe, C., and Schaal, G. S. (2024) Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Frontiers in Big Data, Vol 7, 1452129. https://doi.org/10.3389/fdata.2024.1452129

Endsley, M. R. (1995) Toward a theory of situation awareness in dynamic systems. Human Factors, Vol 37, No. 1, pp 32–64.

Endsley, M. R., and Jones, D. G. (2025) Designing for situation awareness: An approach to user-centered design. CRC press.

Fenstermacher, L., Uzcha, D., Larson, K., Vitiello, C., and Shellman, S. (2023) New perspectives on cognitive warfare. In Signal Processing, Sensor/Information Fusion, and Target Recognition XXXII, Vol. 12547, pp 172-187. https://doi.org/10.1117/12.2666777

Ferrara, E., Varol, O., Davis, C., Menczer, F., and Flammini, A. (2016) The rise of social bots. Communications of the ACM, Vol 59, No. 7, pp 96-104. https://dl.acm.org/doi/pdf/10.1145/2818717

Gillis, W. (2024) Fort Moore launches Cognitive Monitoring Program to enhance Soldier health and readiness. U.S. Army. Available at: https://www.army.mil/article/279247/fort_moore_launches_cognitive_monitoring_program_to_enhance_soldier_health_and_readiness. (Accessed: 26 November 2025).

Grigsby, C. C., McKinley, R. A., Bridges, N. R., and Carpena-Núñez, J. (2023) Developing cognitive neuroscience technologies for defense against cognitive warfare. Mitigating and Responding to Cognitive Warfare. NATO STO Technical Report RDP STO-TR-HFM-ET-356.

Großwald Systems. (2025) Cognitive command: AI-enhanced decision-making in Multinational Battle Networks. Available at: https://www.grosswald.org/cognitive-command-ai-enhanced-decision-making-in-multinational-battle-networks/. (Accessed: 26 November 2025).

Herlihy, D. J. (2022) Cognitive performance enhancement for multi-domain operations. The US Army War College Quarterly: Parameters, Vol 52, No. 4. https://doi.org/10.55540/0031-1723.3188

Hoffman, M. (2025) Assessing "Cognitive Warfare". Small Wars Journal. Available at: https://smallwarsjournal.com/2025/11/14/assessing-cognitive-warfare/. (Accessed: 26 November 2025).

Ibrahim, F., Rhode, S., and Daseking, M. (2023) A systematic review of cognitive and psychological warfare. Available at: https://tdhj.org/blog/post/cognitive-psychological-warfare/ (Accessed: 26 November 2025).

Marino, C. (2025) Reality check. U.S. Army. Available at: https://www.army.mil/article/286728/reality_check. (Accessed: 26 November 2025).

Matz, S. C., Kosinski, M., Nave, G., and Stillwell, D. J. (2017) Psychological targeting as an effective approach to digital mass persuasion. Proceedings of the National Academy of Sciences, Vol 114, No 48, pp 12714-12719. www.pnas.org/cgi/doi/10.1073/pnas.1710966114

Morelle, M., Julien, C., Marion, D., and Jean-Marc, A. (2023) Towards a definition of cognitive warfare. In Conference on Artificial Intelligence for Defense. Available at: https://hal.science/hal-04328461/document. (Accessed: 26 November 2025).

Munk, T. (2025) Digital Defiance. Memetic Warfare and Civic Resistance. European Journal on Criminal Policy and Research, Vol 31, pp 501-528. https://doi.org/10.1007/s10610-025-09613-4

NATO Allied Command Transform. (2024) Allied Command Transformation develops the Cognitive Warfare Concept to combat disinformation. NATO Allied Command Transformation. Available at: https://www.act.nato.int/article/cogwar-concept/. (Accessed: 26 November 2025).

NATO, Joint Analysis and Lessons Learned Centre (2016). Joint Analysis Handbook. Available at: https://www.jallc.nato.int/application/files/9416/0261/6056/Joint_Analysis_Handbook_4th_edition.pdf. (Accessed: 26 November 2025).

Nygren, T., Guath, M., Axelsson, C.-A. W., and Frau-Meigs, D. (2021) Combatting visual fake news with a professional fact-checking tool in education in France, Romania, Spain and Sweden. Information, Vol 12, No. 5. https://doi.org/10.3390/info12050201

Paul, C., and Matthews, M. (2016) The Russian "Firehose of Falsehood" Propaganda Model. RAND Corporation. Available at: https://www.rand.org/pubs/perspectives/PE198.html (Accessed: 26 November 2025).

Probasco, E. S., Toner, H., Burtell, M., and Rudner, T. G. (2025) AI for Military decision-making. Center for Security and Emerging Technology. Available at: https://cset.georgetown.edu/wp-content/uploads/CSET-AI-for-Military-Decision-Making.pdf. (Accessed: 26 November 2025).

Qureshi, J., and Khan, S. (2024) Deciphering deception: The impact of AI deepfakes on human cognition and emotion. Journal of Applied Artificial Intelligence, Vol 2, No. 1, pp 101-107.

Rahman, E. A. (2024) Indirect Swarming and Its Threat to Democracies: A New Frontier in Online Harassment. New America. Available at: https://www.newamerica.org/oti/briefs/indirect-swarming-and-its-threat-to-democracies/. (Accessed: 26 November 2025).

Reczkowski, R., & Lis, A. (2022) Cognitive Warfare: what is our actual knowledge and how to build state resilience?. Bezpieczeństwo. Teoria i Praktyka, 48(3), 51-61. https://doi.org/10.48269/2451-0718-btip-2022-3-003

Salas, E., Wildman, J. L., and Piccolo, R. F. (2009) Using simulation-based training to enhance management education. Academy of Management Learning & Education, Vol 8, No. 4, pp 559-573.

Sattler, T. (2023) The impact of cognitive warfare on strategic decision making in NATO. In Pashova et al. (ed.), CMDR COE Proceedings, pp 177-205.

Sederholm, T., Rannikko, R., & Salo, M. (2025) Total defence model at the heart of Finland's national defence and resilience. In Rongved (ed.), European Total Defence (pp. 115-134). Routledge. https://doi.org/10.4324/9781003497370

Thomas, T. (2004) Russia's reflexive control theory and the military. Journal of Slavic Military Studies, Vol 17, No. 2, pp 237-256. https://doi.org/10.1080/13518040490450529

U.S. Army. (2019). Army Doctrine Publication 6-0: Mission Command. Department of the Army.

Vosoughi, S., Roy, D., and Aral, S. (2018) The spread of true and false news online. Science, 359(6380), 1146-1151. https://doi.org/10.1126/science.aap9559