

Artificial Intelligence as a Tool in Cognitive Warfare on Digital Platforms

Niina Meriläinen

Faculty of Management and Business, Tampere University, Finland

Niina.merilainen@tuni.fi

Abstract: Cognitive warfare uses selective framing, AI and ICT to manipulate cognition, exploit vulnerabilities, and influence beliefs and decisions. AI supports both offensive and defensive cognitive warfare, feeding into kinetic warfare through psychological tactics. Cognitive warfare is immersive and long-term, often unnoticed, even via trusted actors. As AI and ICT evolve, unpredictable uses will emerge, raising ethical, legal, and moral challenges that demand multidisciplinary research. Future warfare will involve complex trade-offs, while democracies must prevent adversaries from weaponizing these tools—by using them strategically themselves.

Keywords: AI, Cognitive Warfare, Vulnerabilities, Internet, Digital platforms

1. Introduction

Cognitive warfare makes use of cognitive vulnerabilities, credibility, and authority. Artificial intelligence (AI) and various information and communication technologies (ICT) are used during this process. Cognitive warfare has strengthened its place in the strategic, operational and tactical levels of warfare. By targeting cognitive elements such as attitudes, beliefs, and understandings as well as the causal relations these create, cognitive warfare aims to shape the attitudes, beliefs, values, and heritage as well as behaviour of people and compel them to the adversary's aims. Moreover, it aims to compromise, disrupt, or destroy information systems, networks, and infrastructure. It also includes a wide range of activities, including espionage, sabotage, and propaganda, conducted by state and non-state actors who act as proxies. People rely heavily on digital platforms (social media, the Internet, and gaming) as spaces for facts and fiction as well as belonging to in-groups where they find truths, causes, safety, and reasons to live. These platforms, content, and actors producing the content are believed and consumed selectively based on individuals' values, beliefs, cognitive vulnerabilities, and biases. Digital platforms are used effectively as battlefields in cognitive warfare besides kinetic warfare. Next to the traditional five operational domains—land, air, maritime, space, and cyber—the human mind can be considered a new domain of operations in warfare (Neculcea & Răpan, 2022).

RQ1: The research question is, can AI be used as a tool in cognitive warfare?1

During and in between warfare, AI and various other ICT tools are used to create content, people, profiles, images, narratives, and realities. These are also used to create, collect and analyse data in intelligence analysis and, for example, in drone warfare. The tools have limitless potential in warfare. They do not bleed or demand physical geographical locations to operate. AI-driven and algorithm-aided viral actors (influencers) and content such as deepfakes, memes, fake news, ads, mis- and disinformation offer innovative possibilities but also pose significant risks to authenticity, privacy, and national security (Babaei et al., 2025; Maik & Afridi, 2024; Samoilenko & Suvurova, 2023; Meriläinen, 2025; Collier, 2025). AI and various ICT tools can be used successfully in cognitive warfare on digital platforms across the globe in information operations. Information operations succeed on digital platforms since people are prone to regard their critical media literacy as strong, simultaneously showcasing a lack of it. People believe they cannot be targets of information operations during cognitive warfare (Meriläinen, 2024; 2025). Meanwhile, various countries struggle to hold various technology giants, from Meta and Discord to TikTok, accountable as platforms in cognitive warfare. Politicians simply pay lip service to the platforms as places for warfare due to a lack of political will or know-how about how these platforms operate as places for war. Thus, we need to look at how, if at all, cognitive warfare can benefit from AI and ICT to guide the research going forward.

2. Related Works

2.1 Cognitive Warfare

Cognitive warfare influences how a target population believes, thinks, and acts (Backes & Swab, 2019; Meriläinen, 2025). It is a strategic, non-physical form of conflict that modifies perceptions and thought processes by weaponizing the content people consume and trust (Putter, 2025). However, it can escalate into physical violence and contribute to kinetic warfare. Non-kinetic methods, such as cognitive warfare, can lead to kinetic warfare—and vice versa (Saressalo, 2025), which is why the author discusses lethal and non-lethal

warfare. Cognitive warfare involves manipulating individuals', groups', or whole populations' cognition to gain an advantage over adversaries, transforming human cognition into a critical realm of warfare. It is the art of using cognitive attributes and technology to change the cognition of human targets, who are often unaware of any such attempt, as are those entrusted with countering, minimising, or managing its results (Claverie & Du Cluzel, 2022). Both defensive and offensive counterintelligence operations are used in tandem with cognitive warfare strategies and tactics (Putter, 2025). However, Gergelewicz (2024) argues that there is a low level of understanding of information threats during the ongoing cognitive warfare. Thus, there is a lack of holistic, practical solutions in the field of building social resilience against disinformation used in cognitive warfare in the form of information operations. Information operations are a tool in cognitive warfare as cognitive warfare often takes the shape of information operations. Information operations use any attributes, vulnerabilities, values and beliefs as well as information to affect an adversary's cognition and accomplish strategic goals. Giles (2016) and Meriläinen (2025) note that, for example, digitally enabled information operations as part of cognitive warfare are not random.

Careful planning and intelligence gathering from OSINT and SOCMINT are done prior to information operations (Giles, 2016; Putter & Henrico, 2022). From military doctrines and cross-sectional influencing, information operations benefit from social and political agendas, memes, online activism, dis- and misinformation, hashtags, historical narratives, humour, AI-generated fake accounts, imagery, narratives, algorithms, and bots (Meriläinen 2024; Eleferenko 2023; Weedon et al., 2017; Mozur et al., 2021). Please see more on information operations on digital platforms and cognitive warfare (Starbird et al., 2019; Turan, 2018; Thomas, 1998; Cox, 2006; Darczewska, 2014; JCS, 2012; Chochowski, 2022; Knapp, 2024). Information operations operate within the realm of politics and society, utilising psychological tactics to achieve strategic objectives (Putter, 2025) with AI and various ICT tools. Previously, Backes & Swab (2019) argued that cognitive warfare will remain a constant threat to Western political systems. By targeting cognitive elements such as vulnerabilities, values, attitudes, beliefs, and understandings, cognitive warfare aims to shape the behaviour of adversaries and compel them to accede to one's aims.

2.2 Cognitive Vulnerabilities

Cognitive warfare takes advantage of vulnerabilities to reach the goal of military operations. Cognitive vulnerabilities and biases are faulty beliefs or structures that are hypothesised to set the stage for later psychological problems when they arise (Riskind & Black, 2005). Vulnerabilities are not static but change as time and related issues, actors and events, and the causal relationships they form change. They are subjected to selective framing and priming. They can be defined differently even in research (Parley, 2011). Previous passive cognitive vulnerability can be activated if a person encounters stressful events, such as social rejection (Abramson et al., 2002). Different sets of cognitive vulnerabilities are all aligned with the inability and unwillingness to decode new information, leading to false and inadequate understanding of current situations and new information (Trent, 2005). This serves as the exact point of entry for information operations as part of cognitive warfare.

Ryan and Deci (2017) discuss self-determination by highlighting the need for people to be able to make their own choices, decide on their lives, and experience their value in society and in their community. If, for example, due to vulnerabilities, these are prevented or impossible to fulfil, people can be targeted by cognitive warfare. This gives them reasons why their self-determination is taken away, and they are subsequently targeted by AI- and ICT-driven cognitive warfare online. During this warfare, an emphasis is made on who is to blame and how to get the determination back. Cognitive vulnerability can make people believe false information, nefarious actors, and realities. Vulnerable people can be influenced and manipulated and cannot make informed decisions (Van Dongen et al., 2011; Block & Gordon, 2019). Cognitive vulnerabilities may be as simple as being tired or otherwise having a "bad day", which directly impacts a person's ability to be alert. When a person is in a vulnerable state, they can be targeted by various cognitive attacks. Thus, detecting the vulnerabilities of individuals is a useful tool in cognitive warfare. When a person is cognitively vulnerable, they are likely to attach themselves to credible situations, truths, information, and sources of these that align with their values and beliefs in accordance with confirmation biases. Informational and psychological influence is an important tool for conducting information and psychological wars (Habro et al., 2022).

2.3 Cognitive Authorities and Credibility

Cognitive authority refers to the source or content of knowledge that credibly shapes thinking. It involves recognizing information as trustworthy and worthy of belief, emphasizing its quality, usefulness, currency, and accuracy (Wilson, 1983; Rieh, 2002). For cognitive warfare to succeed, the actor, their communication, and the

platforms they communicate, must appear credible to the receiver, exploiting cognitive vulnerabilities as tools (Meriläinen, 2025). Drawing on Aristotle, the influencer's ethos, pathos, and logos—along with the platform and message—must align with the audience's pre-existing values and beliefs. Furthermore, selective framing (Meriläinen, 2014) must present narratives as facts or embed emotional hooks to reinforce persuasive power. There must also be a connection to cognitive attributes, credibility and authority. Umeogu (2012) defines credibility as the sender's belief in the receivers' minds, emphasizing the significance of charisma. Credible actors function as authority and distributors of messages, thus holding immense power. Traditionally, credible leaders have been connected to certain traits or behaviours (Ivancevich et al., 2013). Kamau and Oginde (2022) listed attributes related to a credible, authentic leader, from honesty to values. For example, related to cognitive warfare, Kalpokas (2017) argues that so-called sofa warriors are active information spreaders or part of DDoS attacks, working in the background by making the information atmosphere favourable for the main information operation. Meanwhile, Meriläinen (2024; 2025) notes that influencers are credible actors in information operations and work as proxies between adversary states and young people, drawing people into the influence of states like Russia and China, while not doubting the purpose and aims of the influencers or even recognising the usage of AI and ICT.

2.4 Cognitive Warfare and Artificial Intelligence

While cognitive warfare is nothing new, it benefits from AI, neuroscience, and digital platforms to influence human cognition (Fenstermacher et al., 2023). The shaping of cognition relates to earlier notions of biases and selective framing by legacy media and the pictures in the heads people live in (Lippmann, 1922). Nowadays framing is done to a lesser degree by legacy media. Now it is done with the help of AI and ICT on various digital platforms by actors known and unknown. AI is used by states in a variety of ways to improve, automate, or intensify cognitive warfare strategies and modern military operations.

AI is used in cognitive warfare for:

- strategic (cyber) deception and espionage,
- social engineering of people, their values, beliefs, habits and members of their ingroups,
- in the creation of credible and legitimate actors, from influencers to sofa warriors,
- in the creation of viral online content from memes to satire,
- in the creation of deep fakes,
- (social) bots,
- mis- and disinformation, hashtags,
- algorithms, ads,
- censorship,
- mental and physical intimidation and control,
- bullying, harassment and violence.

AI also has a massive role in intelligence gathering and analysis, which is furthermore used in both cognitive and kinetic warfare. The strategic use of AI, espionage, various types on content and online communication methods, algorithms, ads, influencers, mis-disinformation and by attaching them to human emotions, this numerous threats to personal safety, corporate and national security. (Rosli, 2025; Maik & Afridi, 2024; Samoilenko & Suvurova, 2023; Meriläinen 2025; Collier, 2025; Kalpokas, 2017) The aim is to undermine shared values, by undermining trust in institutions and authority (Albert et al., 2023). AI is an effective tool for adversary states for generating fake content to use in information warfare (Lande & Danyk, 2025) as part of cognitive warfare. The new(er) content utilizes cognitive vulnerabilities and people's needs to find information and truths that help them make informed decisions and to make sense of their surroundings in the world riddled with uncertainties. AI+ICT driven cognitive warfare offers vast opportunities to manipulate and control people, to sow distrust towards democratic institutions from schools to national defense and even legitimize kinetic wars.

Indeed, the rapid development of AI and ICT has created new possibilities for malicious use as part of warfare (Samoilenko & Suvorova, 2023). These tools facilitate massive, rapid, disruptive, and subversive campaigns designed to have serious cognitive and emotional impacts on international audiences and present multiple threats to organisational safety and national security (Pashentsev, 2021). AI breaks down national borders, creating a limitless workforce and operating at superhuman speed. While moral objections exist, the alternative is allowing enemies to manipulate people's minds using advanced AI technologies. Thus, AI must be

utilised in warfare in offensive and defensive warfare. (van Diggelen et al., 2025) Indeed, there is a growing interest in harnessing AI and related tools to serve national defense and warfare (Rani et al., 2025).

Some argue that NATO does not have a ready-to-use concrete doctrine on cognitive warfare, while Russia has one (Miron & Thornton, 2024). NATO must catch up with Russia. The Russian military employs AI and deepfakes as part of their cyberpsychological and cybertechnical operations to create strategic, potentially war-winning effects, aiming to undermine state adversaries and weaken them through influence operations long-term, while NATO has no clearly defined policies to counterattack these operations (Miron & Thornton 2024). However, Bykov (2025) argues that NATO's cognitive security strategies and informational environment analysis can counter Russia's cognitive warfare and following cyber-attacks, requiring state, civil society, private sector, and international partnerships for coordinated efforts within NATO. Russia is just one example of how a state effectively uses cognitive warfare and AI to gain a strategic advantage in conflicts. Various countries use propaganda and psychological operations to divide the enemy's population, while the increased use of social media makes people vulnerable (Afridi, 2025). Examples can be found globally from China, Taiwan, and the USA (Hung & Hung, 2022; Mozur et al., 2021; Reinhold & Reuter, 2022.)

Young people showcase a lack of critical media literacy online and are especially indifferent towards the power of AI, ICT, advertising, algorithms, bots, deepfakes etc. (Meriläinen, 2024; 2025). This makes them potential targets of cognitive warfare in the form of information operations. People may not think to doubt digital platforms, influencers, AI, algorithms, bots, ICT and digital advertisements. They are something that people cannot or do not care to doubt or think twice about (Meriläinen 2025). At the same time, AI and algorithms can be viewed as tools for control and coercion, leading to the consumption of mis- and disinformation on various digital platforms. Numerous problems are associated with AI. Previous studies have shown that AI has built-in misogyny, discrimination and racism and allows doxxing, discrimination and sexism (Burak 2021; Soh & Connolly 2021; Waelen & Wieczorek 2022). The same tools can be used to disseminate war-related information and to monitor and document human rights violations during wartimes (Nemkova et al., 2023), while others claim that AI and machine learning bear no accountability for anyone and allow bullying, harassment and violence (Razmetaeva, Barabash & Lukianov, 2022; Langford, 2020). All of these can be utilised in cognitive warfare to create AI-assisted us-versus-them realities. However, we get back to the question: can and should we use AI to defend ourselves? Yes. While moral objections exist, the alternative is allowing enemies to manipulate society's minds using advanced AI technologies. Thus, AI must be utilised in warfare in offensive and defensive warfare. (van Diggelen et al., 2025)

3. Discussion and Conclusions

Relating to Lippman's seminal research (1922), people live in mental constructs. These were previously influenced and shaped by the legacy media selectively by selective framing (Meriläinen 2014). Nowadays, this phenomenon illustrated by Lippman is holding strong within cognitive warfare. The influencing occurs via digital platforms by actors not even known to people consuming the content. Cognitive warfare exploits people's need to belong, various cognitive vulnerabilities, basic needs, societal silos and political movements. The rapid development of AI and subsequent ICT tools has created new possibilities for the adversary actors to use AI in malicious ways as part of information and psychological warfare (Albert et al., 2023). AI, ICT, and cognitive vulnerabilities and biases are heavily used as tools in cognitive warfare. This critical realm of warfare is designed by adversary states to modify the perceptions of reality by nefarious means, benefiting from AI and various ICT tools. Cognitive warfare utilises various content (data, information, and knowledge) to manipulate cognition and create uncertainty, often to exploit vulnerable populations or achieve strategic gains, to influence target audiences' values, beliefs, behaviours and decisions (Putter, 2025; Bykov, 2025). Moreover, AI technologies are used to gain knowledge and further control over people in cognitive wars against their own or foreign nationals (Hung & Hung, 2022). AI enhances kinetic warfare through intelligence gathering, audience manipulation, and technologies such as drone operations (Johnson, 2020; Giles, 2016; Putter & Henrico, 2022). Moreover, cognitive warfare can escalate into kinetic warfare, revealing their intrinsic interdependence at the core of modern conflict.

Adversary states do their research to find divisions and cognitive strengths and vulnerabilities in the target societies. To exploit these divisions and vulnerabilities, AI and ICT is employed as a tool in cognitive warfare, both locally and globally. Geological restrictions and proximity are removed in cognitive warfare because AI-assisted attacks can take place and be coordinated anywhere globally (Veljković, 2024). AI serves as a tool in both defensive and offensive cognitive warfare operations on strategic, operational and tactical levels. As cognitive warfare occurs in virtual spaces and uses AI and ICT to inflict damage on opponents, potentially the

consequences of the war are not immediately apparent. This type of warfare takes time. AI-aided cognitive warfare operates within the realms of cyber, politics, and society, utilising psychological tactics to achieve strategic objectives (Putter, 2025). In this process, AI is a significant tool together with bots, deepfakes, memes, narratives, realities, and credible actors such as newer agenda setters, e.g., influencers. The influencer economy combined with various AI and ICT tools has transformed legacy media and previous gatekeepers as truth-tellers, influencing various aspects of life, including entertainment, consumerism, news, and even national security as well as warfare (Meriläinen, 2025). AI serves as a cross-national tool in cognitive warfare against states globally. With the use of AI, ICT and digital platforms, kinetic warfare seems to have an excellent partner in cognitive warfare online. Victims may not even be aware, or care, that they are under immersive, long-term attacks from multiple platforms, even via actors they trust. With its capacity to absorb, analyse and create vast volumes of data, comprehend human behaviour, and swiftly and efficiently manipulate information and create trustworthy actors and realities, AI serves a central and advancing role in cognitive warfare.

As AI develops and is used more profoundly, there will probably be new and unpredictable uses for it in cognitive warfare, which raises important ethical, legal, moral and not yet foreseeable questions regarding the future of cognitive and kinetic warfare. Rani et al. (2025) and van Diggelen et al. (2025) argue that many decisions in this realm involve complex moral trade-offs that require careful analysis and more research. AI cannot fully replicate human judgement. Thus, we should not follow AI-driven recommendations blindly amidst warfare. Because of AI, do we need to prove that we are real humans? Are we the adversaries or the defenders? Is our war offensive or defensive? These are questions that we must address in future research regarding AI and warfare.

AI creates a limitless workforce and operates at superhuman speed, yet ethical and moral objections exist. If we decline to use AI and ICT tools in warfare, the alternative is to allow enemies to manipulate people and their minds using advanced these technologies. Thus, AI must be utilised in our warfare. (Rani et al., 2025; van Diggelen et al., 2025) Informational and psychological influence is an important tool for conducting informational psychological wars and operations and is seriously detrimental to social consciousness. (Habro et al., 2022) We need more multidisciplinary research to address the ethical, defensive and human perspectives in warfare. In future research we should focus on how and why people are targeted by warfare on digital platforms. How is AI and ICT used in each case example, and how influencers are utilised in warfare? More focus must be placed on framing, confirmation biases and cognitive elements such as cognitive vulnerabilities, credibility, and authorities and how these are and can be utilised in warfare with the help of AI and ICT.

Acknowledgement

I wish to thank the reviewer of this paper.

Ethics declaration: No ethical clearance was required.

AI declaration: No AI tools were used in creation of this paper.

References

- Abramson, L., Alloy, L., Hankin, B., Haefel, G., MacCoon, D., and Gibb, B. (2002) "Cognitive vulnerability-stress models of depression in a self-regulatory and psychobiological context", In I., Gotlib and C. Hammen (Eds.), *Handbook of depression*, pp 268–294. The Guilford Press.
- Afridi, M. (2025) "Deciphering Russian information warfare: lessons from Georgia to Crimea and Ukraine", *ASSAJ*, Vol.3, No.01, pp 824-837.
- Albert, C., Mullaney, S., Huitt, J., Hunter, L., and Snider, L. (2023) "Weaponizing Words", *The Cyber Defense Review*, Vol. 8, No.3, pp 15-32.
- Babaei, R., Cheng, S., Duan, R., and Zhao, S. (2025) "Generative Artificial Intelligence and the Evolving Challenge of Deepfake Detection: A Systematic Analysis", *Journal of Sensor and Actuator Networks*, Vol. 14, No. 1, pp 1-38.
- Backes, O. and Swab, A. (2019) "Cognitive Warfare. The Russian Threat to Election Integrity in the Baltic States", *Cambridge: Belfer Center for Science and International Affairs*, pp 1-50.
- Block, J. and Gordon, B. (2019) "Populations in research requiring additional considerations and/or protections". [online] [Populations-in-Research-Requiring-Additional-Considerations-and-or-Protections-ID-16680.pdf](#)
- Burak, B. (2021) "Human Rights Violations in Cyberspace: Internet Censorship and Online Surveillance in Turkey", *Cyberpolitik Journal*, Vol. 6. No. 12, pp 202-220.
- Bykov, S. (2025) Challenges of Cognitive Warfare: The Ukrainian Case Study. *Thesis*. DOI: 10.13140/RG.2.2.10097.19045
- Chochowski, K. (2022) "Legal aspects of information operations in Poland", *Journal of Scientific Papers Social Development and Security*, Vol 12, No. 2, pp 1-11.

- Claverie, B. and Du Cluzel, F. (2022) "Cognitive warfare": The advent of the concept of "cognitics" in the field of warfare, *Cognitive Warfare: the future of cognitive dominance*, pp 1-11.
- Collier, H. (2025) "AI in Social Engineering: The Next Generation of Offensive Cyber Operations", *Proceedings of the 24th European Conference of Cyber Warfare and Security*, Vol 24, No.1, pp 80-83.
- Cox, J. L. (2006) "Information Operations in Operations Enduring Freedom and Iraqi Freedom: What Went Wrong?", *School of Advanced Military Studies, United States Army Command and General Staff College*.
- Darczewska, J. (2014) "The anatomy of Russian information warfare. The Crimean operation, a case study", *POINT OF VIEW* 2014-05-22. Centre for Eastern Studies.
- Eleferenko, A. (2023) "How can digital diplomacy reconcile Russia and the West?", *International Policy Review*, Vol. 4, No. 1, pp 1-20.
- Gergelewicz, T. (2024) "Countering Disinformation Concept for building social resilience in times of cognitive warfare", *Przegląd Nauk o Obronności*, Vol. 9, pp 23-36.
- 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.
- Giles, K. (2016) "Handbook of Russian information warfare", NATO Defence College Research Division.
- Habro, I., Vovchuk, L. and Shevchuk, O. (2020) "Informational and Psychological Influence on Student Youth in the Conditions of the Information-Psychological War", *Journal of Educational and Social Research*, Vol. 10, No. 1, pp 56-61
- Hung, T. C., & Hung, T. W. (2022) "How China's cognitive warfare works: a frontline perspective of Taiwan's anti-disinformation wars", *Journal of Global Security Studies*, Vol 7, No. 4, pp 1-18.
- Ivancevich, J., Konopaske, R., and Matteson, M. (2013) "Organizational behavior and management". McGraw-Hill Irwin.
- JCS (2012) Joint Chiefs of Staff, Joint Publication 3-13. Doctrine for Information Operations. Washington DC.
- Johnson, J. (2020) "Artificial intelligence, drone swarming and escalation risks in future warfare", *The RUSI Journal*, Vol. 165, No. 2, pp 26-36.
- Kalpokas, I. (2017) "Information warfare on social media: A brand management perspective", *Baltic Journal of Law & Politics*, Vol. 10, No. 1, pp 35-62.
- Kamau, J. and Oginde, D. (2022) "Making of a Credible, Authentic Leader", *Journal of Human Resource & Leadership*, Vol. 6, No. 3, pp 47 - 61.
- Knapp, M. (2024) Arms and Influencers: Leveraging the Social Media Stars in the US Military's Ranks. [online] <https://mwi.westpoint.edu/arms-and-influencers-leveraging-the-social-media-stars-in-the-us-militarys-ranks/>
- Lande, D. and Danyk, Y. (2025) "Competitive Artificial Intelligence in Information and Cyber Warfare", *Available at SSRN* 5084698.
- Langford, M. (2020) "Taming the digital leviathan: Automated decision-making and international human rights", *American Journal of International Law*, Vol 114, pp 141-146.
- Lippmann, W. (1922) *Public Opinion*, New York, USA. Macmillan.
- Maik, H. and Afridi, S. (2024) "The Role of Artificial Intelligence in Modern Warfare and International Security". DOI: 10.13140/RG.2.2.24155.89129
- Meriläinen, N. (2025) "Influencers as Tools in Hybrid Operations Online", *Proceedings of the 20th International Conference on Cyber Warfare and Security*, Vol. 20, No. 1, pp 256-272.
- Meriläinen, N. (2014) "Understanding the Framing of Issues in Multi-Actor Arenas Power Relations in the Human Rights Debate," *Dissertation*. University of Jyväskylä. Finland.
- Meriläinen, N. (2024) "The possible role of digital platforms in information operations", *Proceedings of the 11th European Conference on Social Media - ECSM 2024*, Vol 11, No. 1, pp 137-143
- Miron, M. and Thornton, R. (2024) "The Use of Cyber Tools by the Russian Military: Lessons from the War against Ukraine and a Warning for NATO?", *Applied Cybersecurity & Internet Governance*, 3.
- Mozur, P., Zhong, R., Kroluk, A. Aufrichtig, A. & Nailah Morgan N. (2021) INSIDE A CHINESE PROPAGANDA CAMPAIGN, [online] The New York Times, <https://www.nytimes.com/interactive/2021/12/13/technology/china-propaganda-youtube-influencers.html>
- Neculcea, C. A., & Răpan, F. (2022) "Information operations—comparative doctrinal analysis", *Strategic Impact*, Vol. 85, No. 3-4, pp 68-79.
- Nemkova, P., Ubani, S., Polat, S., Kim, N. and Nielsen, R. (2023) "Detecting Human Rights Violations on Social Media during Russia-Ukraine War". *arXiv preprint arXiv:2306.05370*.
- Parley, F. (2011) "What does vulnerability mean?", *British Journal of Learning Disabilities*, Vol. 39, No 4, pp 266-276.
- Pashentsev, E. (2021) "The malicious use of artificial intelligence through agenda setting: Challenges to political stability", In *Proceedings of the 3rd European Conference on the Impact of Artificial Intelligence and Robotics ECIAIR*, pp 138-144.
- Putter, D. (2025) "Navigating the interplay of cognitive warfare and counterintelligence in African security strategies: insights and case studies", *Journal of Policing, Intelligence and Counter Terrorism*, Vol 20, No. 2, pp 173-192.
- Putter, D. and Henrico, S. (2022) "Social media intelligence: The national security-privacy nexus", *Scientia Militaria - South African Journal of Military Studies*, Vol. 50, No.1 , pp 19-44.
- Rani, N., Jindal, K., Chikkara, R., & Malik, N. (2025) "Empowering Defense: Harnessing AI for Next-Generation Warfare", *Artificial Intelligence-Enabled Businesses: How to Develop Strategies for Innovation*, pp 289-310.
- Razmetaeva, Y., Barabash, Y., and Lukianov, D. (2022) "The Concept of Human Rights in the Digital Era: Changes and Consequences for Judicial Practice", *Access to Justice in Eastern Europe*, Vol 3, No. 15, pp 41-56.

- Reinhold, T., & Reuter, C. (2022) *Artificial Intelligence and The Future of Warfare, The USA China and Strategic Stability*. Manchester. Manchester University Press.
- Rieh, S. Y. (2002) "Judgment of information quality and cognitive authority in the Web", *Journal of the American society for information science and technology*, Vol. 53 No. 2, pp 145-161.
- Riskind, J. and Black, D. (2005) "Cognitive vulnerability", *Encyclopedia of cognitive behavior therapy*, pp 122-126.
- Rosli, W. R. W. (2025) "Waging warfare against states: the deployment of artificial intelligence in cyber espionage" *AI and Ethics*, No. 1, Vol. 7, pp 47-53.
- Ryan, R. & Deci, E. (2017) *"Self-determination theory: Basic psychological needs in motivation, development, and wellness"*. Guilford publications.
- Samoilenko, S. and Suvorova, I. (2023) "Artificial intelligence and deepfakes in strategic deception campaigns: The US and Russian experiences", In *The Palgrave handbook of malicious use of AI and psychological security*, pp 507-529. Cham: Springer International Publishing.
- Saessalo, T. (2025) "Information influencing in wars and conflicts in the early 21st century", National Defence University Series 1, Research Publications, 67.
- Soh, C. and Connolly, D. (2021) "New frontiers of profit and risk: The Fourth Industrial Revolution's impact on business and human rights", *New Political Economy*, Vol. 26, No. 1, pp 168-185.
- Starbird, K., Arif, A and Wilson, T. (2019) "Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations", *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), pp 1-26.
- Thomas, T. L. (1998) "Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations", *The Journal of Slavic Military Studies*, Vol 11, No. 1, pp 40-62.
- Trent, S. (2005) "A study of the cognitive challenges and vulnerabilities of intelligence analysis, *Master's thesis*, The Ohio State University.
- Turan, S. (2018) "The Internet and social media as Information Operations and Public Relations Tools for the Turkish Armed Forces. Doctoral dissertation, Monterey, CA; Naval Postgraduate School.
- van Diggelen, J., Aidman, E., Rowa, J., and Vince, J. (2025) "Designing AI-Enabled Countermeasures to Cognitive Warfare". *arXiv preprint arXiv:2504.11486*.
- Van Dongen, H., Caldwell Jr, J., and Caldwell, J. (2011) "Individual differences in cognitive vulnerability to fatigue in the laboratory and in the workplace", *Progress in brain research*, Vol. 190, pp 145-153.
- Waelen, R., and Wiczorek, M. (2022) "The struggle for AI's recognition: understanding the normative implications of gender bias in AI with Honneth's theory of recognition", *Philosophy & Technology*, Vol. 35, No. 2, 53.
- Weedon, J., Nuland, W. and Stamos, A. (2017) Information operations and Facebook. [Online] <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>
- Wilson, P. (1983) Second-hand knowledge: An inquiry into cognitive authority.
- Umeogu, B. (2012) "Source Credibility: A Philosophical Analysis", *Open Journal of Philosophy*, Vol. 2, pp 112-115.