Human Cognition is a Tool in Warfare in the Cyber Domain

Niina Meriläinen
Faculty of Management and Business, Tampere University, Finland

Niina.merilainen@tuni.fi

Abstract: Warfare in cyber domains has evolved into a battleground for both defensive and offensive geopolitical objectives, exploiting cognitive vulnerabilities, credibility, and authority. Artificial intelligence (AI), information communication technologies (ICT), digital platforms and gaming are increasingly used to influence cognitive elements such as attitudes, biases, beliefs, perceptions, and psychological susceptibilities. Cognitive warfare is now an integral part of international relations, posing serious threats to individuals, critical infrastructure, and national security. Human cognition serves as a powerful instrument in this domain. As AI, ICT tools and digital platforms continue to advance, cyber warfare is becoming more complex, with diverse threat vectors and networks of adversarial actors. Tactics such as psychosensory warfare and white noise jamming are proving effective in cognitive operations, where fear and the loss of hope play a central role in digital battlefield strategies.

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

1. Introduction

The cyber domain and various digital platforms have become arenas for both defensive and offensive geopolitical activities, including warfare. Cyber warfare exploits cognitive vulnerabilities such as biases, values, beliefs, credibility, and authority. In this process, artificial intelligence (AI), information and communication technologies (ICT), the Internet, social media, and gaming are actively employed. By targeting cognitive elements, such as biases, beliefs, attitudes, and understanding, cyber warfare seeks to shape individual and collective perceptions. Consequently, human behavior can be influenced, enabling adversaries to steer populations toward their strategic objectives. Human cognition is a central asset in cognitive warfare within the cyber domain. This form of warfare constitutes an integral part of modern conflict, posing serious threats to personal, organizational, military, and national security, and is conducted alongside kinetic warfare. The purpose of this article is to examine existing research and the thematic variations it presents, and to reflect on how future studies should approach this complex and evolving phenomenon through various threat vectors.

This theoretical paper draws on existing literature to explore the question:

How can human cognition be harnessed in cognitive warfare?

It provides a theoretical outlook and offers recommendations on why cognitive security should be considered a critical concern for:

- personal (tactical),
- municipality/organizational (operational) and
- state/military leadership (strategic) levels.

Warfare in the cyber domain involves manipulating the cognition of individuals, groups, or entire populations to gain strategic advantage over adversaries. It elevates human cognition into a critical dimension of modern warfare. The cyber domain provides an ideal environment for persistent and continuously evolving attacks. In this context, cognitive warfare integrates processes, knowledge, technologies, and cognitive capabilities related to threat awareness at personal, organizational, and state or military levels. Communication and cognitive attributes play a central role in these operations. While success in kinetic warfare can, at best, be measured in seconds, the strategic, operational, and tactical outcomes of cognitive warfare unfold gradually over time. Therefore, understanding human cognition—and how it can be harnessed as a tool alongside kinetic operations—is essential.

2. Related Works

2.1 Human Cognition and Warfare

Human cognition, while resilient, contains exploitable vulnerabilities. Cognitive warfare targets fundamental human needs, such as the need to belong and to feel loved and safe. It also leverages political and social silos, as well as mistrust toward leaders, legacy media, the military, police, politicians, and educators. People live within mental constructs (Lippmann, 1922). In the past, these were shaped by legacy media; today, they are influenced by actors from newer media, including influencers and keyboard warriors (Meriläinen, 2025;

Kalpokas, 2017). These influencers actively create, sustain, and exploit cognitive vulnerabilities for strategic gains in personal brand building as well as in cyber-based cognitive warfare. Cognitive warfare significantly overlaps with other forms of non-kinetic warfare. It serves as an umbrella concept encompassing psychological operations, information, political, cyber, and electronic warfare (Rhode, 2024). As Crawford (1999) notes, research on these topics is too important to be left solely to the military.

Human cognition, as it relates to warfare in the cyber domain, refers to the processes through which individuals learn, assess, and process information—encompassing perception, attention, language use, memory, and creative problem-solving (Ahmed et al., 2025). Cognitive warfare involves manipulating the cognition of individuals, groups, or entire populations—from everyday citizens to policymakers, military officers, and high-ranking officials. Its goal is to gain strategic advantage over adversaries by turning human cognition into a critical battleground. This form of warfare employs technologies such as AI, ICT, bots, advertisements, gaming, deepfakes, trolls, the Internet, and social media to alter the cognition of human targets—many of whom remain unaware of these manipulative efforts, as do those responsible for countering, mitigating, or managing their effects (Claverie & Du Cluzel, 2022; Meriläinen, 2025). Russia and China are recognized experts in leveraging cognitive elements in warfare (Fang, 2024). China has learned from Russia, with a key distinction: Russia disregards its international reputation, whereas China seeks to preserve it (Sobchuk, 2025). Other nations are following these two expert countries. Yet, Russia is a pioneer in psychological warfare, particularly in its methods of creating confusion and destabilization—not by offering alternative truths, but by undermining the very concept of truth itself (Sobchuk, 2025).

Beznosov (2025) explores how Russian psychosensory warfare targets human senses to influence emotions and, consequently, behavior. This strategy affects individuals and groups by manipulating sensory modalities—sight, touch, sound, taste, and smell—to provoke emotional responses. As Beznosov notes, such tactics foster a pervasive atmosphere of fear, with fear itself being the primary objective of psychosensory warfare. Continuous cognitive attacks by adversarial actors reinforce and sustain this climate, with the key being the absence of pauses between assaults. These attacks involve persistent messaging across multiple cyber and offline channels. To maximize impact, hostile actors conduct target group research to identify the most effective ways to amplify fear and hopelessness. Existing societal concerns—such as climate change, immigration, unemployment, and general uncertainty—are exploited as emotional triggers. Simultaneously, influencers are deployed to repeatedly disseminate these messages, ensuring constant exposure to a "wind of fear" (Meriläinen, 2025). Psychosensory warfare (Beznosov, 2025) operates in tandem with cognitive-level white noise jamming (Gatov, 2018), where external criticism is dismissed as Russophobia—echoing earlier Kremlin censorship of foreign broadcasts.

2.2 Cognitive Warfare and Societies Levels

The human mind is the battleground in cognitive warfare (Marjanović & Smiljanić, 2025). Not everything that happens in cyberspace stays there (Marsilii, 2023). In the cyber world, individuals navigate across multiple platforms and are influenced by a variety of actors and groups. There is no clear boundary between the analog and cyber spheres—they are deeply interconnected. Therefore, the connection between cognition and behavior must be understood in the context of warfare.

2.2.1 Personal level

Cognitive warfare targets the human mind by influencing values, biases, beliefs, and behavior, while eroding trust in governments, official actors, those around us, and the convictions people hold. Digital platforms, such as social media and Internet is used to undermine state interests, discredit institutions, and sow domestic discord (Prier, 2020; Meriläinen 2025). Individuals engage across various cyber arenas, receiving information, news, and even cognitive authority from alternative media sources, influencers, and actors outside traditional structures (Meriläinen, 2025). Many believe their media literacy is strong and assume immunity to tactics such as disinformation, AI- and ICT-generated content, deepfakes, and information operations (Meriläinen, 2024). ICT tools and disinformation play a central role in both defensive and offensive cognitive warfare (Lande & Danyk, 2025). In cyber domains, individuals are easily targeted (Meriläinen, 2025).

For instance, Russia's psychosensory warfare aims to influence foreign decision-making by supplying polluted information and fear (Beznosov, 2025). When disinformation becomes embedded in decision-making processes, Moscow achieves a key element of reflexive control (Beznosov, 2025). Even without direct policy impact, its spread through various digital platforms—such as social media—can create a permissive public opinion environment in which Russian narratives are perceived as factual (Kanet, 2024; Bykov, 2025;

Meriläinen, 2025). Kibeom (2025) argues that the proliferation of digital platforms has made disinformation a powerful tool. Due to cognitive biases and the effects of mis- and disinformation, countering fake news with accurate information is not always possible (Meriläinen, 2025; Lysenko et al., 2023). Manipulated information can reshape public perceptions (Lysenko et al., 2023). Moreover, ICT and global connectivity have enabled new and evolving threats from cyber domains—marked by unprecedented speed, scale, and unconventional tactics (Marsili, 2023).

Effective operations in cyber domains require strong situational awareness of events in both the physical and informational spheres, as well as an understanding of how these influence the cognitive domain (Ponangi et al., 2012). Cognitive warfare is a strategic approach to conflict that seeks to alter how target populations think and behave (Backes & Swab, 2019), leveraging content consumption and belief systems to shape individual thought processes. It is often deployed alongside both defensive and offensive kinetic warfare. Information operations are a central tool in cognitive warfare, designed to influence adversaries' cognition and achieve strategic objectives. These operations draw on a wide range of sources, including military doctrines, memes, online activism, disinformation, hashtags, historical narratives, humor, AI-generated fake accounts, imagery, algorithms, and bots (Meriläinen, 2024; Eleferenko, 2023; Weedon et al., 2017; Mozur et al., 2021).

The adversarial aspect of cyber-domain warfare frequently relies on government-funded networks and covert channels to disseminate disinformation, often through state actors or influencers (Meriläinen, 2025; Lysenko et al., 2023). For example, cognitive and information warfare, propaganda, and cyberattacks targeting Ukrainian infrastructure are designed to break the population's will to resist (Lysenko et al., 2023). As Kanet (2024) observes, cognitive warfare in cyber domains can alter perception to the point where disinformation is accepted as fact. The Russian military, for instance, employs AI and deepfakes in cyber-psychological and cyber-technical operations to achieve strategic, potentially war-winning effects. These influence operations aim to gradually undermine and weaken adversaries. Meanwhile, NATO lacks comprehensive policies to counter such tactics (Miron & Thornton, 2024). However, Bykov (2025) argues that NATO's cognitive security strategies and analysis of the informational environment can help counter Russia's cognitive warfare and related cyberattacks. This requires coordinated efforts across state institutions, civil society, the private sector, and international partnerships. Russia has effectively used information warfare to gain strategic advantages in conflicts, employing propaganda and psychological operations to divide enemy populations. Its leadership understands the power of information in shaping and manipulating audiences, and the rise of social media has made netizens increasingly vulnerable (Afridi, 2025). The individual human mind is connected to municipal, organizational, and military/state levels of society. When trust in societal structures and the actors within them begins to erode, and fear takes hold, the human mind becomes vulnerable to warfare. In such conditions, the mind itself becomes part of conflicts, sometimes even a soldier, a keyboard warrior.

2.2.2 Municipality and organizational levels

Warfare that leverages cognitive attributes as tools is a core element of modern international relations, posing serious threats to organizations and critical infrastructure, including banking, energy, transportation, national security, elections, economics, and politics (Musakhanov, 2023). Assets requiring protection include power plants, energy distribution networks, water treatment and supply facilities, transportation systems, radio and satellite communication networks, military communication channels, weapons systems, command and control centers, and surveillance and reconnaissance systems (Kumar & Nagar, 2024). Palletti et al. (2021) emphasize the interconnected nature of these systems and the cascading effects that cyberattacks can trigger. Attackers must understand how infrastructures are linked, which highlights the need for a global approach to strengthening cyber defense resilience in the face of increasingly frequent and sophisticated attacks on cyber domains—particularly those targeting cognition.

Executing cyberattacks against critical infrastructure requires the ability to modify malware and target specific industrial protocols—skills that are not widely available (Izycki & Vianna, 2021). Cognitive warfare encompasses a wide range of constantly evolving attacks targeting both physical systems and human cognition. Because these attacks can occur anywhere within cyber domains, they are not bound by geography and can be organized globally (Veljković, 2024). Targets include not only states and armed forces but also individuals, communities, and organizations. According to Veljković (2024), digital conflict is designed to harm adversaries, often with unintended consequences. It uses digital technologies to compromise, disrupt, or destroy cognition, information systems, networks, and infrastructure. Activities include espionage, sabotage, and propaganda, carried out by both state and non-state actors (Kumar & Nagar, 2024; Meriläinen, 2025; Veljković, 2024).

To carry out these attacks, adversaries must identify cognitive vulnerabilities. Hostile third parties may use computers for cybercrime and cyberwarfare, threatening the safety and security of individuals, their cognition, companies, and governments in ways that are difficult to counter using traditional methods (Dalton, 2017). The assets requiring protection remain the same: critical infrastructure and communication systems (Kumar & Nagar, 2024). Given the risks cyber warfare poses to both organizations and employees, it is essential to consider the cognitive impacts on staff, who may experience harassment and psychological strain from malicious attacks (Rafi & Imtiaz, 2023). Employees may feel disconnected from their workplace or colleagues. They may perceive decisions affecting them as being made elsewhere and feel unappreciated or distrusted by employers, politicians, and public officials—from healthcare to education and law enforcement. This alienation can lead individuals to identify with actors who promote distrust, finding common ground in the cyber domain. Everyday pressures may further erode their sense of belonging to their work, community, or society.

This dynamic is shaped by the constant priming and framing of cognitive vulnerabilities, values, biases, beliefs, emotions, and behaviors—factors linked to espionage, information warfare, cyberattacks, and influence operations. These processes threaten not only critical infrastructure but also societal cohesion. During information operations and warfare, cognitive attacks pose significant risks to global security, economic stability, and individual rights. Companies must adopt a holistic approach to address these threats (Sharma & Vandra, 2024), while hostile states exploit employee alienation. When individuals become disconnected from their organizations, their cognition can be manipulated in ways that turn them against their workplace—and even against their society and state. Notably, cognitive vulnerabilities, credibility, and authority are closely linked to social engineering. Social engineering involves manipulating human cognition to gain access to information and knowledge held by individuals during cyber-domain warfare. In this context, cognitive authority and perceived credibility are key tools for infiltrating targets—regardless of their social status or employment. Social engineering poses a serious security threat to infrastructure, users, data, and operations in cyberspace by exploiting vulnerabilities within cyber domains (Wang et al., 2020), spanning personal, organizational, state, and military levels.

2.2.3 State and military leadership levels

When states carry out cyberattacks, they may provoke counterattacks—highlighting both the defensive and offensive dimensions of warfare in cyber domains (Izycki & Vianna, 2021). Cognitive warfare in the cyber domain is invisible and insidious, creeping into its targets, and often, by the time its effects are recognized, it is too late for a state or military to respond effectively (Kibeom, 2025). It elevates traditional warfare by targeting how humans think, react, and make decisions, affecting civilians, decision-makers, and military personnel alike (Masakowski & Blatny, 2023). Scholars have examined whether military doctrines and counter-doctrines for cognitive warfare exist in countries such as Russia, China, Taiwan, and within NATO (Miron & Thornton, 2024; Bykov, 2025; Hung & Hung, 2022; Mozur et al., 2021; Reinhold & Reuter, 2022).

In offensive cognitive warfare, militaries may attempt to influence adversaries' perceptions of targets, troop movements, and future battle scenarios. In defensive operations, military leadership must train personnel to maintain trust in command structures, as adversaries aim to erode this trust through communication across both cyber and analog domains. Russia views ICT as a decisive factor in warfare, capable of influencing outcomes at multiple levels. The war in Ukraine has reshaped understandings of warfare on cyber domain, with superpower dynamics defining the nature and purpose of cyber operations. The relationship between ICT and cognitive methods continues to evolve (Kukkola, 2024). New techniques, simultaneous attacks, and asymmetric strategies are common in information warfare and related cyber operations (Hamilton et al., 2002). Cognitive attacks can bypass conventional defenses (Nikoula & McMahon, 2024). To effectively navigate cognitive warfare, military leaders must integrate traditional doctrine with modern digital tools and psychological strategies, ensuring resilience and strategic clarity in today's complex cyber battlespace. For example, resilience training should be incorporated into military education to counter cognitive warfare efforts (Rusu, 2025). Moreover, military leaders must prioritize the threat of disinformation and recognize that personnel often lack the skills and awareness needed to resist cognitive manipulation.

It is essential to recognize that military leaders and soldiers do not operate in a vacuum—they are influenced online like everyone else and are not immune to cognitive attacks. Even subtle cognitive manipulation can impair decision-making and challenge core values. To protect military personnel, leaders must implement proactive strategies, including training programs that enhance individual competencies in identifying and resisting disinformation (Cheatham et al., 2024). Operational, tactical, and strategic levels all face significant disadvantages in the cyber domain. As algorithmic manipulation and disinformation continue to spread,

greater emphasis must be placed on the strategic value of psychological operations and narrative control (Gombar, 2025). Some argue that national defense strategies must evolve to address not only technical vulnerabilities but also the social, psychological, and cognitive dimensions exploited by cognitive warfare. Both aspects are essential for protecting critical systems and the minds of individuals under attack (Meghraoui & Belkhamza, 2025).

3. Discussion and Conclusions

This theoretical study draws on existing literature and the themes it presents to explore the question: How can human cognition be harnessed in cognitive warfare within cyber domains? Human cognition is a powerful asset in cognitive warfare, which involves a wide range of continuous and ever-evolving attacks targeting both physical systems and the human mind. Because cognitive warfare can occur anywhere within both analog and cyber domains, it can be organized globally, removing geographical constraints and proximity requirements (Veljković, 2024). Furthermore, existing research indicates that cognitive warfare attacks are not limited to states and their armed forces, they also target individuals, communities, and organizations. Non-kinetic warfare can escalate into kinetic warfare and vice versa (Saressalo, 2025). Therefore, in future research we should focus on how these two forms of warfare interact, highlighting the harm caused by cognitive warfare—even when bloodshed is not immediately visible.

According to Veljković (2024) and Meriläinen (2025), conflict in digital environments is designed to harm adversaries, often with both intended and unintended consequences. It employs digital technologies to compromise, disrupt, or destroy cognition, information systems, networks, and infrastructure. Activities include various forms of AI, ICT, espionage, sabotage, and propaganda, conducted by both state and non-state actors (Kumar & Nagar, 2024; Meriläinen, 2025; Veljković, 2024). Personal (tactical), municipal/organizational (operational), and state/military leadership (strategic) levels must be viewed as a unified whole. We cannot protect just one part, as people form the foundation of all these societal levels. Moreover, individuals are influenced across all these levels through multiple vectors online and offline. These threat vectors permeate all levels and are constantly evolving, making it impossible to define any single, concrete, and lasting vector. This reality calls for continuous training across all levels of society we are seemingly unprepared to meet.

Individuals can be psychologically fragmented and repurposed as tools in cyber-domain warfare. Psychosensory warfare (Beznosov, 2025) and white noise jamming (Gatov, 2018) are effective instruments in this context. Fear and hopelessness play a central role in how cognitive warfare is operationalized and executed across digital arenas. Cyber resilience is essential for countering the effects of cognitive warfare, which exploits vulnerabilities in both digital systems and human cognition (Radu, 2025). Strategic, operational, and tactical levels must adopt vector-like procedures to defend against such threats. However, resilience is deeply tied to cognition—values, biases, and beliefs, making it difficult to build and sustain.

Because people have different understandings of reality, varying values, beliefs, and cognitive biases, how can we build awareness and protect ourselves, our organizations, armed forces, and states from hostile actors? For example, shortly after Russia's full-scale invasion of Ukraine, the Russian news agency TASS published disinformation claiming that "Zelensky hastily fled Kyiv" (TASS, 2022). This message was simultaneously spread on internet and social media by actors and accounts affiliated with Russia. Although legacy media outlets fact-checked and disproved the claim (DW, 2022; Reuters, 2022), many individuals no longer consume legacy media, leaving them vulnerable to distorted perceptions (Meriläinen, 2025). Cognitive warfare has continued since the invasion. Russian-affiliated social media accounts have blamed Zelensky for the lack of peace, portraying Russia as the party seeking resolution. Influencers use various cyber platforms, framings, and hashtags to push narratives suggesting Zelensky refused peace talks, labeling him a war criminal, and calling Ukraine supporters "people profiting from the war" and "retards" (Levinsz, 2025; Anna, 2025). These messages—spread by bots, deepfakes, and real accounts—are part of Russia's psychosensory and cognitive warfare strategy, aiming to instill fear and erode trust in national leadership, making surrender appear as the only viable option.

The core objectives of cognitive warfare in cyber domains are to instill and sustain fear, and to break trust: trust in one's environment, community, institutions, and leadership, including both civil, state and military authorities. The cyber domain offers an ideal platform for this, providing flexible and shifting threat vectors unconstrained by geography or time. By targeting values, biases, and beliefs—and by leveraging newer actors such as influencers, as well as the human need for hope and a vision of the future—adversaries can reshape cognition and influence behavior. Cyber domains thus serve as powerful arenas for cognitive warfare, where

human cognition is one of many tools that can be exploited at any time, cost-effectively and without restriction, to serve adversarial aims. As people increasingly use various digital platforms and are exposed to ICT- and AI-driven content, it is natural that warfare and influence operations have become a new frontier of war. Mastery in cognitive warfare lies in the fact that it is not always recognized as warfare, as its effects may be invisible or take a long time to manifest—unlike kinetic warfare, where outcomes can be seen within seconds. If the cyber environment and cognition are not acknowledged as arenas of warfare and properly prepared for, we risk enabling direct hostile operations against us.

Acknowledgements

I wish to thank the reviewer of this paper.

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

Ethics declaration: No ethical clearance was required.

References

Afridi, M. (2025) "Deciphering Russian information warfare: Lessons from Georgia to Crimea and Ukraine", *ASSAJ*, Vol *3*, No. 1, pp 824-837.

Ahmed, S. S., Nisar, H., & Lo, P. K. (2025) "Introduction to human-machine interaction" In *Artificial Intelligence and Multimodal Signal Processing in Human-Machine Interaction*, Academic Press, pp 1-18.

Backes, O., & Swab, A. (2019) "Cognitive Warfare. The Russian Threat to Election Integrity in the Baltic States", Cambridge: Belfer Center for Science and International Affairs.

Beznosov D. S. (2025) "Social and psychological technologies of information warfare and means of counteracting them", Bulletin of the Saratov University, Series: Philosophy. Psychology, Vol 25, No. 2, pp 120-125.

Brittain-Hale, A. (2023). Clausewitzian Theory Of War in The Age of Cognitive Warfare. *The Defense Horizon Journal*, pp 1-4.

Bykov, S. (2025) "Challenges of Cognitive Warfare: The Ukrainian Case Study". *Thesis.*

Cheatham, M. J., Geyer, A. M., Nohle, P. A., & 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.

Claverie, B. & 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.

Crawford, B. C. H. (1999) "Information warfare: Its application in military and civilian contexts", *The Information Society*, Vol 15, No. 4, pp 257-263.

Dalton, W. (2017) "The silicon hat hacker: using reinforcement learning in hybrid warfare. Conference: Hybrid Threats and Asymmetric Warfare: What to do?", Swedish Defence University (SEDU) – Stockholm.

DW (2022) "Zelenskyy rejects rumors he has fled Kyiv — as it happened" (online) https://www.dw.com/en/ukraine-zelenskyy-rejects-rumors-he-has-fled-country-as-it-happened/a-60908297

Eleferenko, A. (2023) "How can digital diplomacy reconcile Russia and the West?", *International Policy Review,* Vol. 4, No. 1, pp 1-20.

Fang, K. (2024) "Wangbao (Cyberbullying) and Jubao (Reporting): Collaborative State-Society Online Influence Operations in China" *Journal of Online Trust and Safety*, *2*(3).

Gatov, V. (2018) How to Talk with Russia. Public diplomacy for the 21st century, [online] https://www.lse.ac.uk/iga/assets/documents/research-and-publications/How-to-talk-with-Russia-Public-Diplomacy-for-the-21st-Century-3.pdf

Gray, G. P. (2025) "The Political Expediency of Counter-Disinformation: An Analysis of the Response to Russian Information Warfare", (online) https://tsuda.repo.nii.ac.jp/record/2000108/files/%E5%9B%BD%E9%9A%9B%E9%96%A2%E4%BF%82%E5%AD%A6%E7%A0%94%E7%A9%B651_01-16_Gray.pdf

Gombar, M. (2025) "Algorithmic Manipulation and Information Science: Media Theories and Cognitive Warfare in Strategic Communication", *European Journal of Communication and Media Studies*, Vol *4, No.* 2, pp 1-11.

Hamilton, S. N., Miller, W. L., Ott, A., & Saydjari, O. S. (2002) "Challenges in applying game theory to the domain of information warfare", In Information Survivability Workshop (ISW).

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.

Izycki, E., & Vianna, E. W. (2021) "Critical infrastructure: A battlefield for cyber warfare". In *ICCWS 2021 16th international conference on cyber warfare and security*, pp 454-462.

Kalpokas, I. (2017) "Information warfare on social media: A brand management perspective", *Baltic Journal of Law & Politics*, Vol 10, No. 1, pp 35-62.

Kanet, R. E. (2024) "Moscow and the World: From Soviet Active Measures to Russian Information Warfare", *Applied Cybersecurity & Internet Governance*, Vol 3, No.1, pp 34-57.

Kibeom, K. (2025) "A Study on the Concept of Cyber Cognitive Warfare and Case Study Methodology From a Psychological Perspective", In *European Conference on Cyber Warfare and Security*, pp 241-249.

Kukkola, J. (2024) “Suvereenit hiekkamadot: Venäjän kybertoiminta osana valtioiden välistä kamppailua 2000-luvulla” (online) https://www.doria.fi/handle/10024/188804

Kumar, S., & Nagar, G. (2024) ”Threat Modeling for Cyber Warfare Against Less Cyber-Dependent Adversaries”, In *European Conference on Cyber Warfare and Security*, Vol 23, No. 1, pp 257-264.

Lande, D., & Danyk, Y. (2025) ”Competitive Artificial Intelligence in Information and Cyber Warfare”, (online) *SSRN 5084698*.

Lippmann, W. (1922) Public Opinion, New York, USA. Macmillan.

Lysenko, S., Marukhovskyi, O., Krap, A., Illiuschenko, S., & Pochapska, O. (2023) “The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War”, *Studies in media and communication*, Vol 11, No. 7, pp 150-158.

Marjanović, A., & Smiljanić, D. (2025) “Cognitive warfare–the human mind as the new battlefield”, In *Proceedings of the Defense and Security Conference,* pp. 84-114.

Marsili, M. (2023) “Guerre à la Carte: Cyber, information, cognitive warfare and the metaverse“ *Applied Cybersecurity & Internet Governance*, Vol 2, No. 1, pp 1-11.

Meghraoui, L., & Belkhamza, Z. (2025) “Cognitive Warfare and Cybersecurity: Strategic Implications for Global Security”, In *Proceedings of the 19th International Conference on Cyber Warfare and Security*”, pp 257-264.

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. (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

Meriläinen, N., Hiljanen, M., & Rautiainen, M. (2023) Archetypes of youth as vectors in power relations From praises to information operations. Frontiers in Political Science, 5, 1228838.

Miron, M. & 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*, Vol *3*.

Mozur, P., Zhong. R., Krolik, 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

Musakhanov, D. (2023) “The international consequences of cyber warfare: A study of the" Stuxnet" case”, *Acta of Turin Polytechnic University in Tashkent*, Vol *13, No.*3, pp 47-50.

Nikoula, D., & McMahon, D. (2024). Cognitive warfare: Securing hearts and minds. *Information Integrity Lab. JULY*. pp 1-16.

Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021) ”Cascading effects of cyber-attacks on interconnected critical infrastructure”, *Cybersecurity*, Vol *4*, pp 1-19.

Ponangi, P., Kidambi, P., Rao, D., Fendley, M., Haas, M., & Narayanan, S. (2012) “On the Offense: Using Cyber Weapons to Influence Cognitive Behavior”, *International Journal of Cyber Society and Education,* Vol 5, No. 2, pp 127-150.

Prier, J. (2020) “Commanding the trend: Social media as information warfare”, In *Information warfare in the age of cyber conflict*, Routledge, pp 88-113.

Rafi, S., & Imtiaz, N. (2023) “Cyberwar: Its Psychological Impact on Employees and Consequences for Organizations”, In *Handbook of Research on War Policies, Strategies, and Cyber Wars,* IGI Global, pp 108-127.

Radu, R. (2025) “Building Cyber Resilience to Face the Challenges of Cognitive Warfare”, In *European Conference on Cyber Warfare and Security*, pp 803-810.

Reinhold, T., & Reuter, C. (2022) Artificial Intelligence and The Future of Warfare, The USA China and Strategic Stability. Manchester. Manchester University Press.

Reuters (2022) “Fact Check: President Volodymyr Zelenskiy still in Ukraine as of Oct. 25, contrary to online claims” (online) https://www.reuters.com/article/fact-check/president-volodymyr-zelenskiy-still-in-ukraine-as-of-oct-25-contrary-to-online-idUSL1N31Q1NU/

Rhode, S. (2024) “A Systematic Review of Psychological Warfare, Cognitive Warfare, Associated Terminology and Techniques” Master Thesis. der Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg.

Rusu, A. (2025) “Military Ethics in the Light of Cognitive Warfare”, *Redefining Community in Intercultural Context*, Vol *12*, No. 1, pp 45-50.

Saressalo, T. (2025) “Information influencing in wars and conflicts in the early 21st century”, National Defence University Series 1, Research Publications, 67.

Sobchuk, M. (2025) ”To understand the nature of modern Chinese influence operations, study Russia first”, Cyfluence Research Center, pp 1-7.

Tass (2022) “Zelensky hastily fled Kiev, Russian State Duma Speaker claims” (online) https://tass.com/politics/1411855

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. pd

Veljković, S. (2024) “Possibility of applying the rules of international humanitarian law to cyber warfare”, *Pravo teorija i praksa*, Vol 41, No.3, pp 17-28.

Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEe Access*, *8*, 85094-85115.