Cyber Domain as an Arena in Cognitive Warfare

Niina Meriläinen
Tampere University, Finland

Niina.merilainen@tuni.fi

Abstract: Modern warfare increasingly targets the mind and national heritage through AI-driven cognitive and cyber operations. Various heritages are weaponized as both a physical and symbolic asset, with disinformation campaigns framing its destruction or protection to justify military actions. Cyber platforms amplify these tactics, enabling large-scale manipulation of narratives, identities, and emotions via influencers, bots, virtual reality, deepfakes, and algorithmic amplification. These operations work in tandem with kinetic warfare. This hybridization of cognitive, cyber, information and kinetic warfare create fragmented information ecosystems where sustaining narratives can be as decisive as controlling territory. It engenders profound risks to individuals, critical infrastructure, and national security, while concurrently transforming cultural, historical, territorial, and natural resource heritage. Defending various heritage now demands integrated strategies at strategic, operational, and tactical levels, combining technological safeguards and cultural resilience to counter adversarial uses of AI and preserve democratic continuity. Yet societies remain largely unprepared—and hostile actors are already gaining the upper hand.

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

1. Introduction

The purpose of this theoretical research paper is to review relevant published studies on cognitive warfare and cyberspace and reflect on their findings, to identify new directions for future research in relation to cognitive warfare and heritage. Alongside the traditional five operational domains—land, air, maritime, space, and cyber—the human mind is increasingly recognized as a new domain in warfare (Neculcea & Răpan, 2022). Cyber environments, including social media and the internet, have become arenas for information and cognitive warfare, often complementing kinetic operations. Cognitive warfare poses significant risks to individuals, infrastructure, and national security, while reshaping cultural and historical heritage. Unlike kinetic warfare, where heritage suffers as collateral damage, cognitive warfare deliberately targets values, beliefs, and identities through digital means. This theoretical paper examines this phenomenon based on existing research and outlines future research directions, focusing on three key mechanisms.

1. AI (artificial intelligence), ICT (information and communication technologies) tools, and disinformation campaigns that distort historical and factual information,
2. Influencer-driven narratives that undermine resilience, unity, and trust in national media, education, leadership and state institutions from parliament to police and military,
3. Psychosensory warfare that fosters fear and hopelessness, to achieve adversary's strategic military goals.

Cognitive warfare in the cyber domains involves manipulating the cognition of individuals, groups, or entire populations to gain strategic advantage. It transforms human cognition into a contested space. While cognitive and information warfare strips away hope and a sense of future, it simultaneously offers alternatives—false beliefs and fabricated visions—through social media, internet and gaming. The cyber domain provides an ideal arena for long-lasting, adaptive attacks executed by diverse adversary actors, from states to proxies. Cognitive warfare connects processes, knowledge, technology, and cognitive capabilities, influencing awareness and threat perception at personal, organizational, and state levels. Communication and cognitive attributes play a central role in these operations. Whereas success in kinetic warfare can be measured in seconds, the strategic, operational, and tactical impact of cognitive warfare in the cyber domain unfolds gradually over time.

2. Related Works

2.1 Key Themes

In modern conflicts, AI and diverse ICT systems are deployed to fabricate and amplify content and its creators, construct identities, form in-groups and enemies, and shape narratives and perceived realities. These technologies also enable large-scale data collection and analysis for intelligence purposes, supporting operations both on the ground and across cyber platforms. Their potential is virtually limitless, operating without physical presence or geographical constraints. The objective is to engage people emotionally—evoking feelings from love

to anger—and to keep them actively involved in both information and cognitive warfare within cyber domains, while influencing developments in the physical world. A defining feature of cognitive warfare today is the integration of AI-driven content, influencers, and algorithmically amplified actors into information operations. Influencers, once confined to entertainment and consumer culture, now function as strategic assets in shaping perceptions and legitimizing narratives. Their perceived authenticity and trustworthiness make them powerful conduits for propaganda, disinformation, and psychological manipulation. Combined with AI-generated content—bots, deepfakes, memes, fake news, virtual reality, and targeted ads—these actors create immersive realities that blur the line between truth and fiction, posing severe risks to authenticity, privacy, and national security. The influencer economy, amplified by AI and ICT, has dismantled traditional gatekeeping by legacy media, creating fragmented information ecosystems where numerous actors can dominate narratives of warfare and heritage. Cognitive warfare thrives on cyber platforms because individuals often overestimate their media literacy while remaining highly vulnerable to manipulation. Many believe they are immune to influence operations, which paradoxically increases susceptibility. Meanwhile, elected officials struggle—or lack the will—to hold major technology companies such as Meta, Discord, and TikTok accountable for their role as enablers of cognitive warfare. Political responses often amount to symbolic gestures, reflecting insufficient understanding of how these platforms function as arenas of warfare.

2.2 Cognitive Warfare, ICT, and Heritage

Operating across personal, political, military, and societal spheres, cognitive warfare employs psychological tactics to achieve its objectives. It challenges traditional notions of warfare and national identity by shifting the battlefield from physical territories to digital and psychological spaces, where heritage—values, beliefs, and collective memory—becomes both a target and a weapon. Multiple realities coexist in these spaces (Lippmann, 1922; Meriläinen, 2014). Cognitive warfare threatens not only national security but also organizational, personal, and societal stability. Closely related to information warfare, it involves manipulating the cognition of individuals, groups, or entire populations to gain strategic advantage. Its aim is to create, alter, and sustain fear, stripping individuals and nations of their sense of future. Cognitive warfare represents a strategic approach to conflict without physical violence, focusing instead on modifying perceptions and influencing thought processes by weaponizing the content people consume (Putter, 2025). By targeting cognitive elements such as attitudes, beliefs, values, and understandings, adversaries seek to shape behavior and compel military targets to comply with their objectives—ultimately influencing heritage according to their own agenda. With the development of digital society and advances in AI and ICT, cyber platforms have emerged as key arenas for information sharing and interaction. However, insufficient online supervision and user anonymity have created favorable conditions for the dissemination of false information, rumors, and fake news, particularly during emergencies (Ball & Maxmen, 2020; Iasiello, 2017) and warfare (Meriläinen, 2025; Maschmeyer et al., 2025).

2.3 Cognitive Warfare and Heritage

Cognitive warfare destroys heritage by targeting the common bonds that ensure national continuity—our culture and history. It strikes at the very place where heritage resides: the human mind. Cognitive warfare is a form of conflict that targets human cognition—beliefs, emotions, values, and decision-making—without physical violence (Backes & Swab, 2019; Claverie & Du Cluzel, 2022). However, it can escalate into physical violence, linking kinetic and non-kinetic warfare. Saressalo (2025) therefore refers to these as lethal and non-lethal forms of warfare. Non-kinetic or non-lethal warfare can escalate into kinetic or lethal warfare, and vice versa. AI-driven cognitive warfare threatens heritage by distorting historical narratives (Mozur et al., 2021), exploiting divisions (Hung & Hung, 2022), and weakening democratic continuity (Albert et al., 2023). Cyber platforms have become repositories of heritage, and their manipulation risks rewriting history and eroding shared values. Defending against cognitive warfare is not only a security issue, but also a cultural imperative. By manipulating individual and collective understanding, distorting facts, and eroding trust, adversaries aim to reshape memory and identity, erasing them and replacing them with new constructs through cyber platforms. The erosion of trust fragments heritage, leaving individuals disconnected from their national or cultural identity. Instead, they may align with alternative narratives that serve adversarial interests. For example, during Russia's invasion of Ukraine, disinformation campaigns falsely claimed that President Zelensky had fled Kyiv (TASS, 2022). Although legacy media disproved these claims (DW, 2022; Reuters, 2022), many individuals—disconnected from traditional media or platforms publishing corrections—may have accepted them as truth. This illustrates how cognitive warfare can rewrite facts in real time, later shaping historical narratives and undermining democratic and national heritage. Importantly, Russia is not the only actor employing such tactics. History shows how majority cultures have waged internal wars, committed human rights violations, and systematically suppressed

First Nations and minorities—erasing collective memories and, in some cases, entire existences through practices such as eugenics. These actions targeted indigenous peoples and minorities, including deaf communities, often leading to calls for national apologies and restitution for those oppressed or their descendants (Katsui et al., 2024; Weyeneth, 2001).

2.4 War, Heritage, and Cyber Platforms

Cyber platforms (social media, the Internet, and gaming) serve as platforms for information, news, entertainment, and belonging to in-groups. Content and actors on these platforms are trusted and consumed selectively, based on individuals' values, beliefs, cognitive vulnerabilities, strengths, and biases. Increasingly, these platforms have become spaces for war. Adversarial actors exploit cognitive vulnerabilities to reframe historical narratives and cultural values (Kalpokas, 2017; Mozur et al., 2021). Cyber platforms are used effectively as battlefields in cognitive warfare alongside kinetic warfare. They are particularly suited to manipulating cognition. Not only to influence behavior but to reshape collective beliefs, identity, and memory, and thus heritage. Platforms that once enabled connection and information exchange have become battlegrounds where heritage is contested and replaced. These platforms and their actor's 1) host content that trivialize or distort historical and current events, 2) simulate as credible sources, 3) act as alternative media to hated legacy media. This shift undermines traditional defenders of heritage, such as journalists, educators, historians, and replaces them with algorithmically amplified voices that often lack accountability, transparency of funding and networks. The result is a pluralization of truth, where heritage ceases to be a shared foundation and becomes contested terrain.

With ICT and AI tools, bots, deepfakes, virtual reality and influencers pushing narratives that delegitimize heritage, disinformation and fabricated heritage are framed as real, demanding surrender as a rational act. These tactics exploit the human need for hope and belonging, turning heritage itself into a weapon on cyber platforms. Defending against cognitive warfare is not only a strategic necessity. It is a cultural imperative and a matter of national survival. Societies must protect their values, beliefs, and historical narratives from manipulation and exploitation. This requires renewed acts against cognitive and information warfare on cyber platforms. However, national heritage is not a monolith. Within one nation there exist multiple groups, each with its own understanding of identity, culture, and heritage. Cognitive warfare can therefore originate from within, especially when heritage is simplified into a singular narrative of "one nation, one heritage." Cyber platforms can simultaneously host multiple overlapping wars, each driven by different actors, agendas, and objectives. These conflicts unfold in parallel, involving diverse soldiers such as influencers, bots, and algorithmic amplifiers, all operating within fragmented information ecosystems to pursue competing or converging strategic goals.

Heritage is inherently diverse and layered, reflecting multiple histories, identities, and traditions. This complexity, however, can be exploited by adversary actors through cognitive warfare strategies. Their approach often involves:

- Mapping and profiling: Identifying and analyzing different heritage narratives to locate vulnerabilities and identity-based tensions
- Narrative manipulation: Amplifying differences and constructing divisive stories that pit groups against one another
- Fragmentation of social cohesion: Encouraging national and ethnic communities to turn inward and compete, ultimately fostering internal conflict within states.

This is the essence of cognitive warfare: parallel attacks on perception, identity, and trust, alongside physical infrastructure. When cultural heritage is framed as singular and fragile, it becomes more susceptible to manipulation.

3. AI and Disinformation

Disinformation and propaganda have long been staples of conventional warfare (Crawford, 1999). Disinformation has long been a weapon of war, used to manipulate perceptions and weaken adversaries without direct confrontation. In the cyber arenas, these tactics have evolved into large-scale information operations that complement kinetic warfare by eroding trust, destabilizing societies, and shaping strategic narratives of the enemy. While the battle for hearts and minds remains unchanged, it has shifted decisively to digital platforms (Crawford, 1999). Today, the strategic use of artificial intelligence (AI) for disinformation, misinformation, and

subversion represents a critical global security challenge (Meriläinen, 2025). AI enables rapid creation of persuasive disinformation, deepfakes, virtual reality and algorithmically amplified content, making information operations faster, scalable, and harder to detect. These capabilities allow adversarial actors to manipulate identities, historical narratives, and cultural heritage as part of cognitive warfare (Fenstermacher et al., 2023). By shaping representations of history, language, and tradition, AI influences what is preserved or marginalized within heritage with the help of disinformation. It is not a neutral tool but a transformative "actor" in negotiating collective memory. AI-driven operations include strategic deception (Rosli, 2025), social engineering (Putter, 2025), influencer creation (Meriläinen, 2025), and algorithmic manipulation (Babaei et al., 2025). Disinformation campaigns undermine democratic institutions, erode trust, and legitimize kinetic warfare (Albert et al., 2023; Lande & Danyk, 2025), while adversary states like Russia and China advance AI-based doctrines as NATO struggles to respond (Miron & Thornton, 2024; Bykov, 2025).

4. Influence-Driven Narratives in Cyber Warfare

Influencers who are active on cyber platforms, have authority among their followers. Cognitive authority refers to the source or content that credibly influences thinking, emphasizing qualities such as accuracy, relevance, and trustworthiness (Wilson, 1983; Rieh, 2002). For cognitive warfare to succeed, the actor, the content and the platform must appear credible, exploiting cognitive vulnerabilities to shape perceptions (Meriläinen, 2025). Influencers have become key instruments in this process, functioning as proxies between adversarial states and target audiences, often without users recognizing the role of AI or psychosensory tactics behind their messaging (Kalpokas, 2017; Meriläinen, 2024). Their perceived authenticity and alignment with audience values make them powerful tools for disinformation and manipulation. Influencers have shifted from being figures of entertainment and consumer culture to becoming potent tools of cognitive warfare. Their perceived authenticity and trustworthiness make them highly effective conduits for adversarial narratives, particularly in shaping perceptions of heritage. Unlike traditional propaganda channels, influencers operate within familiar social ecosystems, often blurring the line between personal opinion and state-driven messaging. This creates a sense of intimacy and credibility that legacy media cannot replicate (Meriläinen, 2025; Kalpokas, 2017). Influencers often serve as proxies between hostile states and target audiences, especially younger demographics who consume most of their information through social media platforms (Meriläinen, 2024; Mozur et al., 2021). By leveraging AI-driven analytics, adversaries can identify influencers with high engagement potential and tailor content to resonate with specific cognitive vulnerabilities, such as identity-based insecurities or political grievances (Hung & Hung, 2022).

AI and ICT tools enhance this process by generating deepfakes, virtual reality memes, and algorithmically optimized content that influencers disseminate to their followers. These tactics create immersive realities where truth becomes contested, and heritage—values, beliefs, and historical narratives—is reframed to serve adversarial interests (Babaei et al., 2025; Samoilenko & Suvorova, 2023). The influencer economy, combined with AI-driven personalization, dismantles traditional gatekeeping by legacy media, replacing it with fragmented ecosystems where alternative and competition, parallel narratives thrive (Meriläinen, 2025).This dynamic is particularly dangerous because individuals often overestimate their media literacy, believing they are immune to manipulation while remaining highly susceptible to influence operations (Meriläinen, 2024). As a result, influencers become central actors in psychosensory warfare, repeatedly exposing audiences to fear-inducing messages and divisive frames that foster hopelessness and compliance (Beznosov, 2025). The strategic use of influencers in cognitive warfare raises critical ethical and security questions. Should democratic states counter these tactics by deploying their own influencer networks? How can societies regulate platforms like TikTok, Instagram, and Discord, which serve as battlegrounds for cognitive manipulation? Current political responses remain largely symbolic, reflecting a lack of will or understanding of how these platforms function as platforms of war (Maik & Afridi, 2024; Collier, 2025). Ultimately, influencers are not merely cultural figures. They are operational tools in modern warfare on cyber platforms. They are soldiers. Their integration with AI and ICT technologies enables states to wage cognitive battles that transcend geography, operate at superhuman speed, and target the very foundations of heritage and identity. Defending against this requires multidisciplinary research, robust platform accountability, and strategies that reinforce cognitive resilience across all societal levels (Rani et al., 2025; van Diggelen et al., 2025).

4.1 Heritage and Psychosensory Warfare on Cyber Platforms

In addition to the points discussed above, it is essential to address psychosensory warfare and its connection to conflicts on cyber platforms. This form of warfare exploits human senses to provoke fear and hopelessness,

reinforcing cognitive attacks through continuous exposure to targeted messaging. When combined with cyber operations, psychosensory tactics amplify the psychological impact of digital information warfare, making them a critical component of modern warfare. The aim and purpose of psychosensory warfare is fear. Beznosov (2025) explores how this form of warfare targets human senses to influence emotions and, consequently, behavior. By manipulating sensory modalities—sight, touch, sound, taste, and smell—psychosensory warfare provokes emotional responses that foster a pervasive atmosphere of fear. Fear itself becomes the primary objective. Continuous cognitive attacks by adversarial actors reinforce and sustain this climate, with no pauses between assaults. These attacks involve persistent messaging across multiple cyber and offline channels, utilizing mis- and disinformation. To maximize impact, hostile actors conduct target group research to identify the most effective ways to amplify fear and hopelessness via senses selectively framed information. 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. When heritage is deliberately influenced and destroyed through psychosensory warfare, the goal is not only physical erasure but psychological domination. What remains is fear—an emotion strategically amplified via digital platforms to control narratives and shape perceptions. Psychosensory warfare manipulates human senses to provoke emotional responses, creating a climate of despair reinforced by continuous exposure to targeted messaging online (Beznosov, 2025).

5. Discussion and Conclusions

This theoretical paper discussed existing literature on cognitive warfare and relevant topics. What is evident is that AI and ICT tools evolve, so must our understanding of warfare, one that recognizes the mind as a battlefield and heritage as a strategic target. Heritages play a comprehensive role in warfare, functioning not only as a physical target but also as a symbolic and cognitive asset as well as additional target in modern conflicts. Modern cognitive and information warfare employs information operations to manipulate narratives surrounding heritages, framing their destruction or protection as evidence of defensive or offensive warfare. Disinformation campaigns often circulate claims about various heritage to mobilize emotional responses, justify military actions, or delegitimize adversaries. These strategies extend into the digital domain, where heritage becomes vulnerable through kinetic and cyberattacks on archives, language, nature, museums, and historical databases, threatening both tangible and intangible cultural memory. Moreover, actors exploit historical narratives and identity-based heritage claims to reinforce propaganda, creating a powerful link between cultural continuity and strategic objectives. This convergence of kinetic, cognitive, and cyber dimensions illustrates how heritage is transformed into a battlefield of meaning, where controlling narratives can be as influential as controlling territory. Moreover, the legitimacy of diverse forms of heritage: cultural, political, historical, natural, and territorial, is actively undermined and eroded as part of warfare. Future research will demand empirical case examples to test the theories and connect heritages to cognitive warfare on cyber arenas.

Cognitive warfare redefines identity, language, historical and cultural continuity, seeking not only to influence but to erase and reconstruct heritage through digital means. Unlike kinetic warfare, its attacks are subtle, persistent, and global. Their effects may be invisible in the short term, yet they are profound and long-lasting. The cyber environment is no longer a secondary arena but a primary domain of war. Social media and internet platforms, with gaming, and digital ecosystems enable adversaries to deploy AI and ICT tools to amplify disinformation, create alternative realities, and weaponize influencers as credible actors. These platforms allow information operations to be scaled rapidly, exploiting cognitive vulnerabilities and societal divisions through algorithmic amplification. This hybridization of warfare demands integrated defense strategies that combine technical security with psychological resilience.

Cyber platforms do not host a single war but multiple, overlapping conflicts occurring simultaneously. These parallel battles involve diverse actors—state-sponsored operatives, influencers, bots, and algorithmic amplifiers—each pursuing distinct or converging objectives. Social media, Internet and gaming environments, with streaming platforms function as fragmented arenas where cognitive and information warfare tactics exploit different audiences through tailored narratives, disinformation, and psychosensory triggers. This multiplicity creates a complex, multidimensional battlespace that is difficult to monitor or counter, as attacks evolve in real time across interconnected ecosystems. Recognizing this parallelism is essential for developing integrated defence strategies that address not only technical vulnerabilities but also psychological and cultural dimensions of modern warfare. Influencers play a pivotal role in legitimizing propaganda and shaping perceptions,

particularly among audiences who overestimate their media literacy. Their integration with AI-driven personalization dismantles traditional gatekeeping by legacy media, creating fragmented information environments where authoritarian narratives thrive. Psychosensory warfare further amplifies these attacks by exploiting human senses to provoke fear and hopelessness, reinforced by continuous exposure to targeted messaging on cyber platforms. This tactic is further supported by white noise jamming, which neutralizes external criticism and fosters confusion (Gatov, 2018). Such practices demand urgent multidisciplinary research, ethical scrutiny, and coordinated strategies to counter adversarial uses of AI. Modern conflict is no longer confined to geography; it is a battle for truth, trust, and the human mind.

Heritage is an active front of warfare—attacked, reshaped, and weaponized through digital means. Defending against this requires societies to recognize heritages as a strategic domain, invest in cognitive resilience across all societal levels, and reassert control over digital narratives and historical truth. In the age of AI-driven warfare, the battle for heritage is fought not with drones, missiles but with for example FYP on social media, music, videos, memes, algorithms, and emotions. Societies that fail to prepare risk losing control over their values, identity, and future. Historical, territorial, cultural and identity heritage has long been entangled with warfare, not only as a physical casualty of armed conflict but also as a symbolic asset in the battle for narratives. In contemporary conflicts, heritage and historical narratives are increasingly exploited in information operations to influence opinions, legitimize territorial claims, and undermine targets' identity. For example, actors may circulate disinformation about the destruction or preservation of heritage to frame themselves as protectors of civilization while portraying opponents as aggressors. Similarly, selective use of historical memory, such as emphasizing ancient ties to contested regions, serves as a powerful tool in propaganda campaigns. These strategies amplify emotional resonance, mobilize support, and justify military actions under the guise of cultural defence. Thus, heritage becomes not only a victim of kinetic warfare but also a weapon in the cognitive domain, where controlling narratives can be as decisive as controlling territory.

The evolving role of information operations in digital environments emphasizes how digital platforms and influencers shape perceptions of credibility and truth. People often trust these platforms and influencers without critically assessing their agendas, leaving them vulnerable to subtle forms of manipulation by hostile actors (Meriläinen, 2023; 2024). In ever-changing and simultaneous digital ecosystems, cultural heritage becomes intertwined with information warfare when narratives about identity, history, and national symbols are weaponized online to legitimize territorial claims or erode societal cohesion. By framing heritage as part of strategic communication, information operations can transform cultural assets into cognitive battlegrounds, illustrating how cyber-enabled propaganda targets not only infrastructure but also the intangible heritage of communities. Meriläinen's work underscores the urgent need for resilience strategies that combine technological safeguards with critical media literacy to protect both democratic values and cultural continuity in times of conflict (Meriläinen, 2023; 2024; 2025). Future research must address algorithmic amplification, cross-platform coordination, influencers, and ethical frameworks for AI deployment in defensive operations. Heritage, despite being a target, can also serve as a tool of resistance. By reinforcing collective memory and cultural identity—while ensuring that diverse heritages can coexist safely—we can resist cognitive fragmentation and maintain cohesion in the face of adversarial attacks. In the age of AI-driven warfare, the battle for truth and identity is fought with memes, algorithms, and emotions—not only with drones and missiles. Societies that fail to prepare risk losing control over their values and future.

Acknowledgements

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

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.

Ball, P., & Maxmen, A. (2020) "The epic battle against coronavirus misinformation and conspiracy theories", Nature, Vol. 581, No. 7809, ´pp 371-375.

Bykov, S. (2025) Challenges of Cognitive Warfare: The Ukrainian Case Study. *Thesis.* DOI: 10.13140/RG.2.2.10097.19045

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 Wafare and Security, Vol 24, No.1, pp 80-83.

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

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.

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.

Iasiello, E. J. (2017) "Russia's improved information operations: from Georgia to Crimea," The US Army War College Quarterly: Parameters, Vol 47, No. 2, pp 7.

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.

Katsui, H., Koivisto, M., Rautiainen, P., Meriläinen, N., Tepora-Niemi, M., Tarvainen, M., Rainò, P., and Hiilamo H. (2024) Deaf people, injustices, and reconciliation: Signed memories. Taylor & Francis. London: United Kingdom.

Lande, D. and Danyk, Y. (2025) "Competitive Artificial Intelligence in Information and Cyber Warfare", *Available at SSRN 5084698*.

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

Maschmeyer, L., Abrahams, A., Pomerantsev, P., & Yermolenko, V. (2025) "Donetsk don't tell–'hybrid war'in Ukraine and the limits of social media influence operations", *Journal of Information Technology & Politics*, Vol. *22, No.* 1, 49-64.

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., 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

Neculcea, C. A., & Răpan, F. (2022) "Information operations–comparative doctrinal analysis", *Strategic Impact*, Vol. 85, No. 3-4, pp 68-79.

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.

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.

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.

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.

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.

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

van Diggelen, J., Aidman, E., Rowa, J., and Vince, J. (2025) “Designing AI-Enabled Countermeasures to Cognitive Warfare”. *arXiv preprint arXiv:2504.11486*.

Weyeneth, R. R. (2001) “The power of apology and the process of historical reconciliation”, The Public Historian, Vol. 23 No. 3, pp 9-38.

Wilson, P. (1983) Second-hand knowledge: An inquiry into cognitive authority.