Cognitive Warfare and Cybersecurity: Strategic Implications for Global Security

Loukmane Meghraoui[1] and Zakariya Belkhamza[2]
[1]The Higher National School of Political Sciences, Romania
[2]Ahmed Bin Mohammed Military College, Doha, Qatar

meghraoui.loukmane@enssp.dz
zbelkhamza@abmmc.edu.qa

Abstract: This conceptual paper explores the emerging domain of cognitive warfare, focusing on its strategic dimensions and the approaches of some state actors. Cognitive warfare transcends traditional psychological and information warfare by targeting the perceptions, emotions, and cognitive functions of adversaries, ultimately disrupting decision-making processes. Through a detailed analysis of Chinese and Russian tactics, this study explores how cognitive warfare is used to destabilize democratic institutions, manipulate public opinion, and create social fragmentation. The paper further investigates how these strategies challenge established concepts of warfare and security. It concludes by offering insights into the broader implications for national and global security, presenting defense frameworks and strategies to mitigate the growing threat of cognitive warfare.

Keywords: Cognitive war, Cybersecurity, Attack incidents, Incident detection, Data breaches

1. Introduction

Cognitive warfare is a multifaceted strategy that targets the human mind to influence decision-making processes, perceptions, and social structures (Nikoula & McMahon, 2024). Unlike conventional warfare, which focuses on physical destruction, cognitive warfare operates in the realm of ideas, emotions, and beliefs (Claverie and du Cluzel, 2022). The goal is to manipulate the adversary's cognitive functions, slowing down or distorting their decision-making processes to create confusion, demoralization, or self-destruction. By disrupting this process, cognitive warfare weakens individuals' and societies' ability to respond effectively to crises or challenges (Clarke and Kanke, 2019; Bernal et al., 2020).

In the contemporary context, cognitive warfare has become a cornerstone of strategies employed by some states, which blend traditional psychological operations with advanced technologies like artificial intelligence (AI), social media, and neuroscience. For instance, Russia's disinformation campaigns during the 2016 US presidential election sowed division and distrust, while China has used AI-driven tools to tailor propaganda and manipulate public perception globally (Dahl, 1996; Claverie and du Cluzel, 2022).

1.1 Research Problem

The growing sophistication of cognitive warfare presents a new dimension of threat to national security. Unlike traditional cyberattacks or military confrontations, cognitive warfare operates subtly, influencing public opinion, political decision-making, and social stability without the use of overt force or physical combat (Golovchenko, Hartmann and Adler-Nissen, 2018; Tashev, Purcell and McLaughlin, 2019). This form of warfare manipulates perceptions and emotions, embedding within the societal fabric to create confusion, division, and mistrust.

The rise of cognitive warfare marks a significant evolution in the nature of conflict, introducing challenges distinct from traditional forms of warfare. Its ability to operate silently and exploit the psychological and informational domains makes it particularly insidious. The implications are especially profound for democratic societies, where freedom of information and open communication channels are fundamental but can be weaponized to destabilize public trust and societal cohesion (Siboni, 2016). This subtle yet far-reaching form of warfare has profound implications for national security, public trust, and societal stability, particularly in democratic societies (Gregor and Mlejnková, 2021).

2. Complexity of Detection and Attribution

One of the key challenges of combating cognitive warfare lies in the invisible nature of its operations. Cognitive warfare occurs within the informational and psychological realms (Bernal et al., 2020). It manipulates the perceptions and thought processes of entire populations, often without them being aware that they are being attacked.

Cognitive warfare has the ability to seamlessly blend into everyday information flows. Disinformation, propaganda, and fake news are disseminated through platforms that people use daily, such as social media,

news outlets, and online forums (Le Guyader, 2022). This makes it difficult for governments, institutions, and individuals to distinguish between genuine information and manipulated content designed to influence public opinion or decision-making.

Furthermore, the attribution problem complicates efforts to defend against cognitive warfare. Since these operations are often executed through non-state actors, covert channels, or proxy organizations, identifying the exact source of the manipulation is difficult (Aukia and Kubica, 2023).

3. Targeting Democratic Institutions and Civilian Sectors

Another critical issue in cognitive warfare is its focus on civilian populations and democratic institutions. In democratic societies, where freedom of expression and open information flow are fundamental, cognitive warfare can exploit these very freedoms to undermine public trust in key institutions (Siboni, 2016). By spreading disinformation, cognitive warfare can destabilize elections, fuel political polarization, and erode public confidence in government and media (Claverie and du Cluzel, 2022).

China and Russia have used cognitive warfare to target civilian sectors, particularly during periods of social or political vulnerability. For example, Russia's interference in the 2016 US presidential election involved extensive social media manipulation to polarize voters and sow discord. By targeting civil discourse, cognitive warfare threatens the social cohesion of democratic states, making it difficult for governments to maintain, control, and effectively govern their populations militarily.

The targeting of education systems, media outlets, and administrative bodies further exacerbates the problem. These sectors are fundamental to a functioning democracy, and when they are manipulated through cognitive warfare, the impact is profound (Aukia and Kubica, 2023). In education, for example, students can be exposed to manipulated narratives or distorted information, influencing their understanding of history, politics, and social issues (Wu, Chang and Pan, 2017; Claverie and du Cluzel, 2022). In the media, biased or fabricated stories can shape public perception and steer societal discourse in ways that align with the objectives of foreign actors.

4. Psychological Vulnerability and Emotional Manipulation

Cognitive warfare uses the psychological vulnerabilities of individuals and groups to achieve strategic goals. Human beings are naturally inclined to seek out information that confirms their existing beliefs, a phenomenon known as confirmation bias (Le Guyader, 2022). Cognitive warfare exploits this tendency by disseminating customized disinformation that reinforces biases or stimulates emotional reactions, such as fear, anger, or distrust. These emotional triggers can lead to irrational decision-making at both the individual and collective levels (Le Guyader, 2022).

For example, during the COVID-19 pandemic, both China and Russia engaged in disinformation campaigns based on public fears about the disease's origin, treatment, and vaccines (Siboni, 2016). By manipulating emotions such as fear and uncertainty, these campaigns sowed confusion, undermined public trust in health authorities, and hindered effective responses to the pandemic (Gregor and Mlejnková, 2021). The long-term consequence of such emotional manipulation is the erosion of social cohesion, as populations become divided along ideological lines, making it difficult to build consensus or trust in public institutions (Khan, 2024).

5. Lack of Effective Countermeasures

Despite the increasing prevalence of cognitive warfare, many countries still lack effective countermeasures for these types of threats. Traditional defense mechanisms, such as cybersecurity protocols and information control systems, are designed to protect against more tangible forms of attack, such as cyberattacks on critical infrastructure or military targets. However, they do little to combat the psychological and informational manipulation that lies at the heart of cognitive warfare (Claverie and du Cluzel, 2022).

There is a growing recognition that defending against cognitive warfare requires a new set of tools and strategies, particularly in the realms of public education, media literacy, and psychological resilience (Miller, 2016; Aukia and Kubica, 2023). Governments and institutions must invest in educating the public about the dangers of disinformation and the ways in which cognitive warfare operates (Deppe, 2023). However, many nations have been slow to develop comprehensive strategies to deal with these types of threats, leaving their populations vulnerable to manipulation (Newman et al., 2021).

Furthermore, the globalization of information has made it easier for cognitive warfare tactics to cross borders and affect multiple societies simultaneously. Platforms like Facebook, Twitter, and YouTube provide convenient

channels for the dissemination of disinformation, and their global reach makes it difficult for individual countries to control the flow of harmful content (Vision of Humanity, 2022).

6. The Strategic Importance of Cognitive Warfare in Modern Conflict

Cognitive warfare is now recognized as a strategic pillar in modern conflict, particularly by authoritarian regimes seeking to expand their influence on the global stage. The goal of cognitive warfare is not simply to win battles or achieve short-term victories; rather, it aims to reshape society, undermine trust, and destabilize governments over the long term. This makes it a particularly potent tool for asymmetric warfare, where smaller powers or non-state actors can exert significant influence without the need for military superiority (Golovchenko, Hartmann and Adler-Nissen, 2018).

By focusing on influencing the perceptions and beliefs of adversaries, cognitive warfare allows state and non-state actors to achieve strategic objectives without engaging in direct confrontation. This makes it an attractive option for certain countries, which seek to weaken democratic states and enhance their geopolitical influence without risking military escalation (Bernal et al., 2020; Claverie and du Cluzel, 2022).

7. Research Objectives

The objective of this paper is to address the various complexities and challenges of cognitive warfare, and provide insight into how cognitive warfare operates in the psychological and informational realms. Specifically, this paper analyzes the principles of cognitive warfare, as conceptualized by major power nations such as China and Russia, to understand the foundations of cognitive warfare that these two leading state actors that have invested heavily in the development of cognitive warfare tactics. Both countries have adopted sophisticated methods to manipulate perceptions and influence decision-making within target populations, using advanced technologies and traditional psychological warfare techniques (Le Guyader, 2022). Second, this paper explores how cognitive warfare tactics, such as disinformation campaigns, media manipulation, and psyops, have been employed to manipulate public perception and destabilize key societal structures in democratic and non-democratic nations. In particular, this paper examines how these tactics have been used to provoke political polarization, social unrest, and loss of trust in institutions (Wu, Chang and Pan, 2017). Third, this paper assesses the implications of cognitive warfare for global security and provides future insights for defense**.** It analyzes the broader implications of cognitive warfare for national and global security, highlighting the need for new strategies to counteract its effects, and proposes innovative approaches to the detection, prevention, and mitigation of cognitive warfare attacks, particularly in democratic states that face unique challenges in defending against these tactics (Bernal et al., 2020).

8. Conceptual Framework

Cognitive warfare's nonlinear and asymmetric nature demands a multidimensional approach to understand its strategies and implications. It is imperative therefore, to study it from a perspective that integrates psychological operations, information warfare, and advanced technologies. These strategies highlight key elements of cognitive warfare, such as manipulating perceptions, disrupting decision-making, and exploiting emotional vulnerabilities across military and civilian domains.

As part of the broader literature on scalable and adaptable solutions to security challenges, frameworks like the Serenity framework (Gallego-Nicasio et al., 2009, Serrano et al., 2009), offer valuable insights. These frameworks focus on dynamic adaptation at runtime and the reusability of security patterns to address evolving threats in complex environments. It is a comprehensive system designed to address security and dependability (S&D) challenges such as Ambient Intelligence (AmI), ubiquitous computing, and other adaptive systems.

The following sections provides a comprehensive understanding of cognitive warfare, its strategic foundations, and its implications for global security, based on the strategic models of China and Russia. Cognitive warfare merges psyops, information warfare, and technological advancements, creating a sophisticated strategy to manipulate public perception, emotions, and decision-making processes.

8.1 Cognitive Warfare as a Multidimensional Threat

Cognitive warfare is an advanced form of conflict that targets the human mind and the informational environment. Unlike conventional warfare, which focuses on destroying physical assets, cognitive warfare aims to manipulate the cognitive processes of individuals and societies, thereby disrupting decision-making and undermining social cohesion (Dahl, 1996).

- **Information as a weapon:** Information is manipulated to influence perceptions and emotions, making cognitive warfare a nonlinear, asymmetric strategy. Instead of direct military confrontation, the objective is to weaken an adversary from within, exploiting psychological vulnerabilities and information networks (Siboni, 2016).
- **Targeting decision-making:** Cognitive warfare focuses on disrupting the OODA loop, which is traditionally a military framework but is now applied to civilian decision-making processes. The goal is to slow, distort, or disrupt decision-making at both the individual and societal levels (Claverie and du Cluzel, 2022).

8.2 China's Cognitive Warfare Strategy: Emphasis on the Cognitive Domain

China has long recognized the power of cognitive warfare in modern conflicts, integrating AI, neuroscience, and the manipulation of social networks into its military and strategic doctrines. Chinese strategists emphasize that the future of warfare will occur in three domains: physical, informational, and cognitive. Among these, the cognitive domain is becoming the most critical, as it focuses on influencing perception and controlling narrative.

- **AI and neuroscience**: China has invested heavily in AI and neuroscience to enhance its cognitive warfare capabilities. These technologies are used to manipulate emotions, influence decision-making, and create psyops that target both domestic and foreign populations. AI tools are designed to analyze human behavior and predict psychological vulnerabilities, enabling the creation of customized narratives that resonate with specific target audiences (Claverie and du Cluzel, 2022).
- **Social media and information control**: Chinese cognitive warfare also relies on controlling information flow, especially through social media platforms. During the COVID-19 pandemic, for example, Chinese state actors used social networks to spread disinformation and misleading narratives regarding the disease's origins and safety (Le Guyader, 2022). The goal was to cultivate distrust in global health institutions and exploit social divisions (Siboni, 2016).

8.3 Russia's Hybrid Warfare: Cognitive Warfare as a key Component

Russia's cognitive warfare strategy is deeply embedded in its broader hybrid warfare doctrine, which combines conventional military operations with cyberattacks, information warfare, and psychological manipulation. It uses disinformation, historical revisionism, and perception management to achieve its strategic objectives (Siboni, 2016).

- **Disinformation campaigns**: Russia has mastered the art of disinformation as part of its cognitive warfare operations. During the 2016 US presidential election, Its actors used social media platforms to manipulate public perception by creating false narratives, deepening political polarization, and weakening democratic processes (Singer and Brooking, 2018).
- **Historical narrative manipulation**: Russia often engages in historical revisionism as a tactic to control the narratives around its actions. By distorting history, Russia aims to justify its military intervention and gain domestic and international support (Parker, 2022). This tactic was evident in the Ukraine conflict, in which Russia used historical arguments to legitimize its invasion while simultaneously spreading disinformation to weaken Ukraine's international alliances.
- **Media and information warfare**: Russian cognitive warfare tactics also include targeting media outlets, hacking news organizations, and spreading false information through state-controlled media. By manipulating the informational environment, Russia seeks to create confusion, division, and societal unrest in target countries (Tashev, Purcell and McLaughlin, 2019).

9. Cognitive Warfare in Civilian Sectors: Targeting Democracy and Civil Society

Cognitive warfare does not confine itself to military targets; it extensively influences civilian sectors and democratic institutions. China and Russia have strategically focused their cognitive warfare efforts on exploiting the openness of democratic societies (Siboni, 2016).

- **Targeting media and political institutions**: Both countries use disinformation to manipulate elections, polarize political landscapes, and erode trust in democratic processes (Tashev, Purcell and McLaughlin, 2019). The Russian interference in the US serves as a notable example in which social media manipulation undermined public confidence in the electoral process.
- **Education and public opinion**: Cognitive warfare also targets education systems by influencing what is taught and believed about history, politics, and society (Tangredi and Galdorisi, 2020). Manipulated

information can distort how young populations understand global events, making them more susceptible to propaganda (Gregor and Mlejnková, 2021).

- **Emotional manipulation in crises**: During crises such as the COVID-19 pandemic, cognitive warfare intensifies as state actors exploit fear and uncertainty. Disinformation about vaccine safety, virus origin, and public health measures deepened societal divisions, leading to weakened public trust in health authorities (Newman et al., 2021).

10. Psychological Vulnerability and Emotional Manipulation: Key Tools of Cognitive Warfare

Cognitive warfare uses the psychological vulnerabilities of individuals and groups to exploit emotional biases to achieve strategic goals. Cognitive warfare tactics often capitalize on confirmation bias, the tendency of individuals to seek information that confirms their preexisting beliefs (Dahl, 1996; Bernal et al., 2020).

- **Emotional triggers**: Both countries use disinformation campaigns to exploit emotional triggers such as fear, anger, and distrust. For example, by playing with fears during the COVID-19 pandemic, these campaigns caused confusion about vaccine efficacy, leading to public distrust in governments and health systems (Aukia and Kubica, 2023; Vision of Humanity, 2022).
- **Misinformation and collective decision-making**: Disinformation, particularly on social media, spreads misleading narratives that reinforce social divisions, which make it difficult to build consensus on important issues, such as public health measures or political reforms, which, in turn, leads to instability (Le Guyader, 2022).

11. Technological Enhancements in Cognitive Warfare: The Role of AI and Neuroscience

Technological advancements, especially in AI, neuroscience, and social media algorithms, have revolutionized cognitive warfare tactics. These technologies can be used to scale operations and target specific demographics with precision (Claverie and du Cluzel, 2022).

- **AI**: AI enables cognitive warfare campaigns to analyze large amounts of data to identify psychological patterns and behavioral trends. For example, China's use of AI-driven tools allows it to tailor propaganda to specific populations based on their psychological profiles, making disinformation more effective and targeted (Wu Chi-hsun, 2018).
- **Social media algorithms**: Algorithms that shape content on platforms like Facebook and Twitter are increasingly used to push disinformation to specific groups, creating echo chambers where false information is reinforced and dissenting views are suppressed. This technology-driven manipulation is a key component of modern cognitive warfare (Le Guyader, 2022).

12. The Non-Linear Nature of Cognitive Warfare: Asymmetric and Globalized Conflict

One of the defining features of cognitive warfare is its non-linear nature. Unlike traditional warfare, which is constrained by geography and clear battlefronts, cognitive warfare operates across the psychological, informational, and cyber domains, affecting military and civilian targets globally (Bernal et al., 2020).

- **Global information flows**: The globalization of information has made cognitive warfare more prevalent. Platforms like YouTube, Twitter, and Facebook allow for real-time manipulation of public discourse across borders. China and Russia have used these platforms to spread disinformation to millions of people worldwide, destabilizing multiple nations simultaneously (Vision of Humanity, 2022).

13. Implications for Global Security: A new Dimension of Warfare

Cognitive warfare introduces a new dimension to global security, blurring the lines between war and peace. It challenges traditional defense mechanisms by targeting the psychological fabric of society, undermining trust, and destabilizing democratic processes (Bernal et al., 2020).

- **National security threats**: Cognitive warfare represents a significant threat to national security, particularly for democracies that value freedom of speech and open information systems (Claverie and du Cluzel, 2022). Unlike traditional warfare, cognitive warfare operates subtly within society, attacking the psychological foundation of a nation. The impact is far-reaching, destabilizing democratic institutions, elections, and even public health responses (Siboni, 2016).

14. Cognitive Warfare as a Nonlinear Strategy: Challenges in Detection and Defense

The non-linear and diffusive nature of cognitive warfare presents significant challenges for detection and defense. Cognitive attacks are covert, often invisible, and intertwined with the normal flow of information in society, making it difficult to detect malicious intent (Bernal et al., 2020).

- **Challenges of detection**: Since cognitive warfare operates within the psychological and informational domains, traditional military radars, designed to detect physical attacks, fail to detect these subtler threats (Aukia and Kubica, 2023). Attacks may appear as ordinary news posts on social networks or even as public opinion.
- **Attribution difficulty**: Another challenge is attribution. Cognitive warfare campaigns are often carried out by non-state actors, proxy organizations, or covert state-sponsored entities, making it difficult to determine the source of the attack (Tashev, Purcell and McLaughlin, 2019). This is evident in both China's and Russia's use of troll farms and state-controlled media, in which plausible deniability is built into their cognitive warfare strategies.
- **Blurring of war and peace**: Cognitive warfare further complicates the traditional notions of war and peace. Although conventional warfare is clearly defined, cognitive warfare exists in a gray zone, where the boundaries between peacetime and conflict are unclear (Siboni, 2016). This makes it difficult for governments to respond, as they must navigate the legal, political, and moral challenges of engaging in counteroperations during what may be perceived as "peacetime" (Bernal et al., 2020).

15. Countermeasures and Defense Mechanisms: Building Cognitive Resilience

Despite the growing threat of cognitive warfare, many countries lack effective measures to combat these attacks. Conventional defense mechanisms, such as cybersecurity protocols and military defenses, offer little protection against the psychological manipulation that lies at the heart of cognitive warfare (Claverie and du Cluzel, 2022).

- **Public education and media literacy**: One of the most effective ways to counter cognitive warfare is to invest in public education and media literacy. By educating the public about disinformation tactics, fake news, and propaganda, governments can build resilience against these attacks (Le Guyader, 2022). This includes developing critical thinking skills, fact-checking abilities, and understanding how emotional manipulation is used to influence decisions (Aukia and Kubica, 2023).
- **Psycho-social defense strategies**: Beyond public education, governments should also focus on building psychological resilience within their populations. Psychosocial defense strategies include mental health support, community building, and social cohesion efforts (Siboni, 2016). These are crucial in preventing social fragmentation during times of increased cognitive warfare (Newman et al., 2021).
- **Collaboration with technology platforms**: Social media platforms such as Facebook, Twitter, and YouTube play a central role in disinformation dissemination. Governments must work closely with these platforms to develop algorithmic solutions that detect and mitigate disinformation, including the use of AI-driven detection systems, real-time content monitoring, and partnerships with fact-checking organizations (Vision of Humanity, 2020).

16. The Future of Cognitive Warfare: Expanding Conflict Frontiers

As cognitive warfare evolves, advanced technologies such as AI, neuroscience, biotechnology, and improved human capabilities will be increasingly integrated. These innovations will further blur the lines between psyops and direct conflict, expanding the battlefield into social networks, neurological processes, and individual cognition (Claverie and du Cluzel, 2022).

- **Integration of AI and machine learning**: AI and machine-learning technologies will be at the forefront of future cognitive warfare, allowing state actors to predict human behavior, analyze cognitive vulnerabilities, and tailor disinformation campaigns more precisely than ever before (Wu Chi-hsun, 2018). China has already begun using AI to identify behavioral patterns in populations, which allows for more personalized psychological attacks (Le Guyader, 2022).
- **Biotechnology and neuroscience**: Advances in biotechnology and neuroscience also play a role in cognitive warfare, allowing more sophisticated methods of manipulating human cognition. This includes technologies that directly target the brain, manipulating emotions, perceptions, and memory to control human behavior on an unprecedented level.

Cross-domain operations: Future cognitive warfare will not only target the cognitive domain but will also operate in multiple fields of conflict, including the cyber domain, space, air, and land. The cross-domain nature of cognitive warfare will make it difficult to be counteracted, as attacks could come from multiple directions at once, targeting the mind, information networks, and physical infrastructure.

17. Conclusion

Cognitive warfare demonstrates a profound shift in the nature of modern conflict, moving away from traditional physical engagement and instead focusing on manipulating the human mind. The complexity of this new form of warfare lies in its subtlety and pervasiveness, targeting not just military systems but entire societies. By manipulating perceptions, emotions, and decision-making processes, cognitive warfare undermines social trust, polarizes populations, and weakens democratic institutions.

The strategies discussed in this paper illustrate how cognitive warfare can destabilize societies by exploiting systemic vulnerabilities. Through the use of advanced technologies such as AI, big-data analytics, and social media platforms, state actors can manipulate public perception and create long-term strategic advantages without resorting to conventional military means (Siboni, 2016). China's AI-driven cognitive manipulation and Russia's disinformation campaigns show the adaptability and power of cognitive warfare in contemporary geopolitical struggles (Tashev, Purcell and McLaughlin, 2019).

Traditional security measures, such as cybersecurity protocols and military defenses, are no longer sufficient for addressing the multifaceted threats that cognitive warfare poses. These measures typically focus on protecting physical infrastructure or critical systems, but cognitive warfare targets the psychological and social foundations of society (Claverie and du Cluzel, 2022). The implications for national security are profound: Since cognitive warfare operates in the information and psychological realms, it presents an existential threat to the integrity and stability of democratic institutions (Vision of Humanity, 2022).

Government and national defense strategies must evolve to face this emerging form of conflict. Rather than focus solely on the technical aspects of defense, there is a pressing need to address the social, psychological, and cognitive vulnerabilities that cognitive warfare exploits. Building resilience within populations, increasing awareness of disinformation tactics, and improving psychological defenses are crucial steps toward mitigating the impact of cognitive warfare (Newman et al., 2021). The future of national security will depend not only on protecting critical systems but also on protecting the minds and perceptions of people.

18. Recommendations

Educating the public about cognitive warfare and its impact is one of the most critical measures to defend against this form of conflict. Public awareness campaigns should focus on explaining how cognitive warfare works, the techniques used to spread disinformation, and the ways in which emotions and perceptions are manipulated. These campaigns should also promote media literacy and critical thinking skills, which are essential in a digital age where misinformation is easily spread. Schools, universities, and public institutions must implement media literacy programs to teach citizens how to discern credible information from false narratives. Governments must develop a comprehensive cyber-psychological defense strategy that integrates technological and psychological defenses. This approach should combine traditional cybersecurity measures with a greater focus on protecting against psychological manipulation. By monitoring online platforms for coordinated disinformation campaigns and identifying attempts to sow discord and polarize societies, governments can mitigate the impact of cognitive warfare.

References

Aukia, J. and Kubica, L., 2023. *Russia and China as hybrid threat actors: The shared self-other dynamics*. Hybrid CoE Research Report 8. The European Centre of Excellence for Countering Hybrid Threats. Available at: https://www.hybridcoe.fi [Accessed 16 October 2024].

Bernal, A., Carter, C., Singh, I., Cao, K. and Madreperla, O., 2020. *Cognitive Warfare: An Attack on Truth and Thought*. NATO & Johns Hopkins University, Baltimore, MD, USA. Available at: https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf [Accessed 16 October 2024].

Clarke, R.A. and Knake, R.K., 2019. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press, New York.

Claverie, B. and du Cluzel, F. (2022). "Cognitive warfare: The advent of the concept of 'cognitics' in the field of warfare," in B. Claverie, B. Prébot, N. Buchler, and F. du Cluzel (eds.) *Cognitive warfare: The future of cognitive dominance*. NATO STO CSO.

Dahl, A.B., 1996. *Command Dysfunction: Minding the Cognitive War*. Master's thesis. School of Advanced Air and Space Studies, Air University. Maxwell Air Force Base, AL: Air University Press. Available at: https://permanent.fdlp.gov/websites/dodandmilitaryejournals/www.maxwell.af.mil/au/aul/aupress/SAAS_Theses/SAASS_Out/dahl/dahl.pdf [Accessed 16 October 2024].

Deppe, C., 2023. *Disinformation in Cognitive Warfare: Hybrid Threats and Information Disorder*. The Defence Horizon Journal, Available at: https://tdhj.org/blog/post/disinformation-cognitive-warfare-hybrid/ [Accessed 16 October 2024].

Gallego-Nicasio, B., Muñoz, A., Maña, A., & Serrano, D. (2009). Security patterns, towards a further level. Proceedings *of the International Conference on Security and Cryptography*, 349–356. https://doi.org/10.5220/0002230303490356

Golovchenko, Y, Hartmann, M & Adler-Nissen, R 2018, 'State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation', *International Affairs*, vol. 95, no. 5, pp. 975-994. https://doi.org/10.1093/ia/iiy148

Gregor, M. and Mlejnková, P., 2021. *Facing disinformation: Narratives and manipulative techniques deployed in the Czech Republic*. *Politics in Central Europe*, 17(3), pp.541-564.

Khan, D.S., 2024. *The Khan Review: Threats to Social Cohesion and Democratic Resilience: A New Strategic Approach*. UK Government. Available at: https://assets.publishing.service.gov.uk/media/65fdbfd265ca2ffef17da79c/The_Khan_review.pdf [Accessed 16 October 2024].

Le Guyader, H., 2022. *Cognitive Domain: A Sixth Domain of Operations*. In: B. Claverie, B. Prébot, N. Buchler, and F. du Cluzel, eds. *Cognitive Warfare: The Future of Cognitive Dominance*. NATO Collaboration Support Office, pp.1-5. ISBN: 978-92-837-2392-9. Available at: https://hal.archives-ouvertes.fr/hal-03635898 [Accessed 16 October 2024].

Miller, S., 2016. *Shooting to kill: The ethics of police and military use of lethal force*. Oxford University Press.

Newman, N., Fletcher, R., Schulz, A., Andı, S., Robertson, C.T. and Nielsen, R.K., 2021. *Digital News Report 2021*. 10th ed. Reuters Institute for the Study of Journalism. DOI: 10.60625/risj-7khr-zj06.

Nikoula, D., & McMahon, D. (2024). *Cognitive warfare: Securing hearts and minds*. Information Integrity Lab, University of Ottawa

Parker, C., 2022. *Russia and Syria conducted dozens of illegal 'double tap' strikes, the report says*. *The Washington Post*, 21 July. Available at: https://www.washingtonpost.com/world/2022/07/21/syria-russia-double-tap-airstrikes-report-war-crimes/ [Accessed 16 October 2024].

Serrano, D., Ruíz, J. F., Maña, A., & Armenteros, A. (2009). Development of applications based on security patterns 2009 *Second International Conference on Dependability*, 111–116. https://doi.org/10.1109/DEPEND.2009.23.

Siboni, G., 2016. *The first cognitive war*. In: A. Kurz and S. Brom, eds. *Strategic survey for Israel 2016–2017*. The Institute for National Security Studies, pp. 215–223.

Singer, P.W. and Brooking, E.T., 2018. *Likewar: The weaponization of social media*. Eamon Dolan/Houghton Mifflin Harcourt.

Tangredi, S.J. and Galdorisi, G., 2020. *AI at War: How Big Data, Artificial Intelligence, and Machine Learning Are Changing Naval Warfare*. Naval Institute Press.

Tashev, B., Purcell, M. and McLaughlin, B., 2019. *Russia's information warfare: Exploring the cognitive dimension*. *MCU Journal*, 10(2), pp. 129–147.

Vision of Humanity, 2022. *The unfolding cyberwar in Ukraine*. Available at: https://www.visionofhumanity.org/ukraine-cyberattacks-2022/ [Accessed 16 October 2024].

Wu, Q., 2018. *China's cyber forces back online: Eight hacker groups resume operations*. Available at: https://www.ithome.com.tw/news/126295 [Accessed 16 October 2024].

Wu, W.-C., Chang, Y.-T. and Pan, H.-H. 2017 'Does China's middle class prefer (liberal) democracy?', Democratization, 24(2), pp. 347–366. doi: 10.1080/13510347.2016.1192607.