 DOI: 10.3849/2336-2995.33.2024.01.063-083

Peer-reviewed

Cognitive Warfare as a New Dimension of Security A fictional concept or a real silent threat?

Kognitivní válčení jako nová dimenze bezpečnosti Fiktivní koncept či reálná tichá hrozba?

Kristýna Drmotová, Libor Kutěj

Abstract: Cognitive warfare is a new phenomenon that differs from any forms of action previously used in the information space aiming to affect the thinking of target groups. The main difference consists in the targeted and sophisticated use of scientific knowledge from neuroscience, with special attention on consciousness and perception of reality. This deeper understanding of how the human mind works has impacted distributed narratives and the choice of the most suitable technological platforms for their distribution to the target audience. This article presents a conceptual classification of cognitive warfare and defines its three core segments: neuroscience, technology and aspects of social science.

Abstrakt: Kognitivní válčení představuje nový fenomén, jenž se liší od dříve využívaných forem působení ovlivňujících myšlení cílových skupin v informačním prostoru. Hlavní rozdíl spočívá v cíleném a sofistikovaném využití vědeckých poznatků, které vychází z neurovědní oblasti a kladou zvláštní zřetel na vědomí a vnímání reality. Hlubší poznání způsobu fungování mysli ovlivňuje šířené společenské a kulturní narativy a volbu nejvhodnějších technologických platforem využívaných pro jejich distribuci mezi cílenou populací. Článek předkládá konceptuální zařazení kognitivního válčení a vymezuje jeho tři základní segmenty: neurovědu, technologie a společenskovědní aspekty.

Keywords: Cognitive Warfare; Neuroscience Segment; Social Science Segment; Technological Segment.

Klíčová slova: Kognitivní válčení; neurovědní segment; společenskovědní segment; technologický segment.

INTRODUCTION

For centuries, military commanders and their staff have striven to find ways and methods to demoralise both the military forces and civilians of their enemy, to deteriorate their ability to successfully resist aggression or, conversely, conduct offensive operations. Over time, all manners of means have been used for this purpose and level of their employment depended on the objectives of a particular operation and the capacity of the respective instruments.

Of course, rapid, massive and unprecedent technological development has contributed to the increasing sophistication of methods used to influence the morale of armed forces and the mood of the population in a targeted way. The previous range of individual forms of warfare has been expanding, with synergistic use of knowledge from scientific disciplines that were not previously directly involved in the conduct of conflict operations.

The mass development of communication technologies has also created an entirely new environment for developing capabilities that are enormously effective in terms of meeting information warfare goals, much more so than before the spread of the Internet and social media as sources of uncensored and professionally uncorrected information. Technological development has thus enabled the creation of an uncontrolled information flow "into every household", to every individual and to all social groups.

At the same time, advancements in neuroscience have made it possible to get an ever deeper understanding of the processes of receiving and processing information in the human brain. The bringing together of knowledge from the biological and technological sciences have given rise to new forms of "addressing" the target population with a high degree of probability that the disseminated narrative will affect thought processes and opinion formation in accordance with the intention of the creator and distributor of the information activities, which are usually implemented within a framework of long-term information campaigns.

By exploiting the potential of neuroscientific knowledge and highly advanced technological instruments, a new environment has been created where battles for "hearts and minds" can take place. Currently, this environment can be described as an uncharted area of the human mind that is unconsciously influenced and controlled, above all, by modern technology.

The previously known environment, in which psychological operations were conducted as part of information warfare, the dissemination of disinformation, cyber infiltration, and other forms of hybrid warfare, has thus been fundamentally expanded to include a very effective domain. It increases the probability of the success of an opponent's action on the individual and is characterised by the breadth of its potential in this action. On the other hand, this process is not limited to military forces and population groups at the stages of preparing and conducting conflicts between states or other entities; rather it tends to be used for deeply latent operations in peacetime, without making the long-term efforts of a potential enemy to manipulate whole nations obvious.

Unlike traditional methods of employing information, this process creates a "silent threat", which, due to its focus on the human mind, can be referred to as cognitive

warfare. While this threat may seem less graspable and obvious to some traditional warriors compared to conventional military instruments, i.e. less visible and destructive on the traditional battlefield, in fact, in terms of effectiveness and potential it is much more powerful than the effect of traditional military tools, not to mention its impact on civilians.

The means of cognitive warfare have an inherent and fundamental potential to undermine entire social units and state formations, ruin their institutions, to transform value systems and the established social order. The statement that cognitive warfare is actually a genocide of the thinking of selected targets groups is by no means an exaggeration.

New strategic conceptual and doctrinal documents[1] that have been approved in relation to future warfare and building the capabilities of the Czech Army already assume the building of abilities, capacities and resilience against cognitive influence of the enemy against all target groups in the information environment. The use of cognitive warfare is thus assumed both by one's own forces against the adversary and simultaneously it requires building the resilience of the society and protecting one's own forces against the cognitive activities of the enemy.

The aim of this article is therefore to present the multidisciplinary and complex nature of this issue, to provide its conceptual classification and to introduce the different segments and factors that need to be taken into account when discussing and addressing this highly challenging phenomenon.

1 CONCEPTUAL CLASSIFICATION OF COGNITIVE WARFARE

Terms such as "disinformation", "hybrid warfare", "cyberattacks", "psychological influence", "information warfare", "conspiracy theory", "electoral manipulation", "polarisation of society" and numerous others dominate both the contemporary military world and fields dealing with the security of the civilian environment, crisis management, maintaining social stability, as well as other trends that have become apparent in the context of the multiple crises[2] faced by global civilisation over the past two decades. Unlike earlier decades, when these terms were generally only coined between specialised experts, they have now become the everyday topics of news broadcasts, social media, and discussion platforms, so that today these concepts have become an entrenched part of our worldviews. That said, in fact only very few people can imagine what these terms actually mean, and what are their real consequences.

1 For example: *Koncepce výstavby Armády České republiky 2035 (KVAČR 2035)*. Ministerstvo obrany České republiky – VHÚ Praha, 2024. Available at: https://mocr.army.cz/assets/informacni-servis/zpravodajstvi/kvacr_2035_final.pdf.

2 We can list at random the financial crisis and the consequent socio-economic instability in 2008 and beyond, the wave of illegal migration into the European area since 2015, the COVID-19 pandemic caused by the SARS-CoV-2 coronavirus, the Russian aggression in Georgia in 2008 and Ukraine in 2022, or the energy crisis in 2022.

Moreover, within this conceptually confusing situation a completely new collocation has emerged – adjectivally implicated in actions related to the human mind, it is anchored in the complex system of diverse instruments of modern warfare. This is new, and does not represent an established or generally accepted definition of this phenomenon. It has often been confused with informational or cyber warfare or other terms referring to the asymmetric, non-kinetic, unconventional actions of the new era.[3]

At the same time, it has been discussed whether cognitive warfare itself can be regarded as a sixth global domain. In practice, however, there is currently a consensus that it should be considered "only" as a security dimension of specific actions intended to bring more benefits to one's own side and to deteriorate the potential of a competing opponent through specific actions.

1.1 Terminological Definition

An attempt to conceptually anchor the phenomenon of cognitive warfare must be based on the tools it applies and goals it pursues. This article does not provide a definition that would be definitively adopted by NATO, nor does it constitute a recognised national definition. This is due to the absence of a generally accepted concept. This is partly a consequence of different starting points, and partly the very perception of the principles and objectives of cognitive warfare by its various participants. Here it is based on evaluating the activities and trends for the use of cognitive warfare that we experience in practice.

The Middle English term *cognicioun* refers to all the conscious or unconscious activities and processes of an individual relating to the acquisition, storage, reduction, processing, development, retrieval, recovery and use of information. It combines various mental and mind-related processes such as thinking, perception, understanding, cognition, learning, memorising, reasoning, remembering, attention, motivation, imagining, and decision-making.[4] Essentially, this is the ultimate function of the mind.[5]

3 DU CLUZEL, Francois. *Cognitive Warfare, a Battle for the Brain*. Norfolk, Va.: NATO Allied Command Transformation, 2021, p. 1-12.

4 BAYNE, Tim, BRAINARD, David, BYRNE, Richard W., CHITTKA, Lars, CLAYTON, Nicky, HEYES, Cecilia, MATHER, Jennifer, ÖLVECZKY, Bence, SHADLEN, Michael, SUDDENDORF, Thomas, and WEBB, Barbara. What is cognition? *Current Biology*. July 8, 2019, Vol. 29., Is. 13, pp. 608–615. LAWLOR, Peter G. The Panorama of Opioid-Related Cognitive Dysfunction in Patients with Cancer. *American Cancer Society*. March 15, 2002, 94(6), pp. 1836–1853. Available at: doi:10.1002/cncr.10389.

5 ROBBINS, Trevor W. Cognition: The Ultimate Brain Function. *Neuropsychopharmacology Reviews*. 2011, 36, pp. 1–2. Available at: doi:10.1038/npp.2010.171.

The statement that "the mind has become a battlefield"[6] is the most common definitional shortcut related to cognitive warfare. The meaning of the word cognitive is thus linked to the mental process of understanding, which encompasses all aspects of intellectual functions, including the subconscious aspects governing all human decision--making. The words "cognitive" and "warfare" are joined to refer to activities carried out in a synchronised way with other instruments of power in order to influence the attitudes and behaviours, or disrupt the cognitive abilities of individuals or groups in order to gain an advantage over a rival party. In terms of the instruments used, it involves the integration of informational, psychological, cyber and other technological capabilities with a potential for social engineering. The applied accompanying disciplines include game theory, social psychology, and ethics. Cognitive warfare activities are not necessarily accompanied by a kinetic component and may not have directly tangible outcomes (such as the acquisition of resources or territory). As with other instruments of hybrid warfare, they are conducted in synergy with other activities that remain in a notional "grey area", i.e. below the threshold of armed conflict.[7]

To achieve a broader concept of cognitive warfare, we must include information influence operations, a crucial part of which involves disrupting the process of self-correcting inaccurate information by professional journalists or representatives of publicly engaged groups and organisations. Broad-based influence operations are characterised by the use of deception techniques and the mass use of these techniques renders the social system no longer capable of deliberately correcting inaccurate information.[8]

The relationship between information operations and cognitive warfare therefore requires a more detailed definition. For example, the definition established within the US armed forces environment says that "the information environment is the aggregate of individuals, organisations and systems that collect, process, disseminate or act on information[9]". The information environment consists of three dimensions: the physical dimension, the informational dimension, and the cognitive dimension. In this model, the mind (cognitive) is within the information flow separated from the body (physical)

6 CAO, Kathy, GLAISTER, Sean, PENA, Adriana, et al. Countering cognitive warfare: awareness and resilience. *NATO Review* [online]. Brussels: Atlantic Council, February 20, 2021 [cit. 2023-07-14]. Available at: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html#:~:text=In%20cognitive%20warfare%2C%20the%20human%20mind%20becomes%20the,to%20favour%20an%20aggressor%E2%80%99s%20tactical%20or%20strategic%20objectives.

7 Cognitive Warfare: Strengthening and Defending the Mind. *NATO ACT* [online]. Norfolk, Va.: NATO Allied Command Transformation, Strategic Warfare Development Command, April 5, 2023 [cit. 2023-07-14]. Available at: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

8 *Combating information influence activities: A Handbook for communicators* [online]. Prague: The Ministry of the Interior of the Czech Republic [cit. 2023-07-14]. Available at: https://www.mvcr.cz/chh/article/combating-information-influence-activities-prirucka-pro-komunikatory.aspx.

9 *Joint Publication 3–13: Information Operations* [online]. Washington, D.C.: Department of Defense, Joint Chiefs of Staff, 2012, pp. iii. [cit. 2023-07-16]. Available at: https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf.

and from the thoughts (informational).[10] This understanding emphasizes the differences and interconnectedness of the dimensions presented and therefore the importance of cognitive dimension itself. However, the exploration of the concept of cognitive security is at the very beginning. The relation is thus not properly described or analysed.

When evaluating the process of acquiring knowledge and understanding the individual person in the context of cognitive warfare, we encounter yet another concept. This is the concept of "psychological operations" – characterised as planned activities using communication methods and other means to influence the perception attitudes, and behaviour of the target audience in pursuit of political and military objectives. Psychological operations are one of the instruments used for implementing information operations.[11] Clearly, in this sense, activities realised as "cognitive warfare" and "psychological operations" cannot be confused.

1.2 Classification within the Spectrum of Hybrid Warfare

The tools of cognitive warfare can be classified as part of the broad concept of hybrid warfare which can be understood as an "…interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion. These instruments or tools are blended in a synchronised manner to exploit the vulnerabilities of an antagonist and achieve synergistic effects"[12]. In this type of conflict, the line between war and peace blurs. Kinetic and non-kinetic tools of hybrid activities therefore usually operate below the threshold of war. Their use is also cheaper, easier and less risky than kinetic operations, although their damage is real. Hybrid attacks are also difficult to attribute, making response to them challenging.[13] Cognitive warfare is therefore an integral part of hybrid warfare.

For mutual links, relationships and interactions between selected forms of warfare see Figure 1.

10 *Joint Concept for Operating in the Information Environment (JCOIE)* [online]. Washington, D.C.: Department of Defense, Joint Chiefs of Staff, 2018, pp. 47. [cit. 2023-10-16]. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.

11 *AJP-3.10.1: Allied Joint Doctrine for Psychological Operations, Edition B Version 1, with UK National Elements* [online]. London: Ministry of Defence, 2014, pp. 89 [cit. 2023-07-16]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf.

12 BILAL, Arsalan Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. *NATO Review* [online]. November 30, 2021 [cit. 2023-10-14]. Available at: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

13 BILAL, Arsalan Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. *NATO Review* [online]. November 30, 2021 [cit. 2023-10-14]. Available at: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

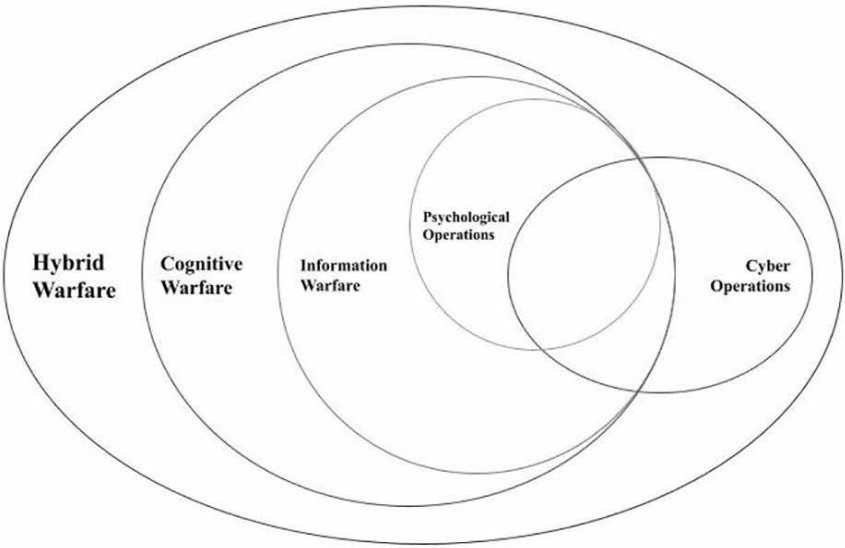

Figure 1: Classification of cognitive warfare within the spectrum of hybrid warfare
Source: HUNG, Tzu-Chieh and HUNG, Tzu-Wei. How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies*, Vol. 7, Is. 4, December 2022. Amended by authors (supplemented by psychological operations)

The above mentioned context, as well as other known ones, obviously indicate that cognitive warfare encompasses information warfare, including media, brain control and influence operations.[14] Even though they are ongoing in the information environment which is more complex (physical, informational and cognitive dimensions), information operations are always targeted at the human mind. At the same time, psychological operations are an essential part of it. They cannot be conceived outside of cognitive warfare, as it is impossible to influence the psyche and mentality of an individual outside of his cognition and nervous system.

Furthermore, the cyber domain is a part of the information environment and consists of an interconnected network of information technology infrastructures[15]. Cyber

14 HUNG, Tzu-Chieh and HUNG, Tzu-Wei. How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies*, Vol. 7, Is. 4, December 2022.

15 *Joint Publication 3–13: Information Operations* [online]. Washington, D.C.: Department of Defense, Joint Chiefs of Staff, 2012, pp. II–9. [cit. 2023-07-16]. Available at: https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf

warfare consists of physical attacks on infrastructure, selected individuals, and the individual stages of decision-making processes. It therefore contains aspects outside the cognition.

Simultaneously, cognitive warfare, which can be conceived in a very simplistic way as "mind control", is thus not an independently applied tool. It operates instead in a broad-based process of hybrid warfare that subsumes the above-mentioned tools while accepting the effects of economic warfare activities, military and other operations that do not directly affect the cognition of the individual.[16]

2 FORMS OF COGNITIVE WARFARE

Like any form of military and non-military action in the context of hybrid action, cognitive warfare has its offensive and defensive components.

Obviously, the offensive concept of cognitive warfare is the primary subject of natural interest. Offensive use by an adversary aims to modify the way reality is accepted, influence behaviour, and create social and military challenges to disrupt the political and socio-economic system and institutions, without the need for direct armed confrontation using traditional military instruments.

Defending against the consequences of its use tends to be much less discussed and is usually assessed only through the prism of defence against disinformation. However, considering the sophistication of cognitive warfare, it is essential that this phenomenon be examined in a way that allows its principles to be understood and the means it uses, in order to prepare an effective defence strategy against it.

At present the dangers of cognitive action are not being sufficiently reflected upon. However, the protection of one's own forces and sufficient resilience of the population should be a decisive priority in the defence and security efforts of any country.

3 NATURE OF TOOLS USED WITHIN COGNITIVE WARFARE

The goal of cognitive attacks is to use information and manipulate the surrounding environment to activate subconscious processes in the human mind in a way that makes it difficult for it to reflect on an existing cognitive threat. The modern concept of cognitive warfare primarily reflects developments made in the field of neuroscience in the last few decades. It is also based on the technological development of modern communication tools that allow the transfer of information to a human target. The social sciences represent a very important part of the process of cognitive action. They define and influence the operation of an individual in a particular group and their way of thinking.

16 See: HUNG, Tzu-Chieh and HUNG, Tzu-Wei. How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies*, Vol. 7, Is. 4, December 2022.

4 SEGMENT 1: THE NEUROSCIENCES

Generally speaking, we can assume the general public considers the "mind" to be actually the brain, i.e. an anatomical organ, and the thought process as an activity in which the brain is the decisive element. However, in order to better grasp cognitive warfare, it is necessary to see the thought process in a broader context, also because the mind and brain represent the environment where this form of warfare takes place.

4.1 Mind and Brain

In modern terms, the mind is a broad term covering all areas of subjective experience. It describes mental acts and senses, such as thoughts, ideas, emotions, perceptions, decisions, imagination, sensory memory, instinct and other factors which are concentrated in the central nervous system.[17] A basic orientation in environment, i.e. in the current situation, is then enabled by subjective reflections of objective reality.[18] The brain thus acts as an inference machine.[19]

Human consciousness, through observation and comparison with already acquired experience, selectively arranges details of our surroundings into "maps", thus creating our own adaptation of reality. Its form, its evaluation of events, and its efforts to meet basic human needs subsequently influence thinking, choices, attitudes, and values, etc.[20] It also navigates behaviour itself, i.e. by looking at the aforementioned "maps" enriched with emotions. Given schemes are tested constantly with the expectation of what will happen. If the prediction matches reality, the individual experiences a sort of harmony. However, when the brain reports a discrepancy between the experience and the expectation, one experiences discrepancy and surprise, called a "prediction error".[21]

17 PEROUTKA, David. *Tomistická filosofická antropologie (Thomistic philosophical anthropology)*. Prague: Krystal OP, 2012. ISBN 978-80-87183-42-7, pp. 11, 19–20, 36 and 47.

18 ŠTĚPÁNOVÁ, Klára. *Cognitive Systems: Perception: Vision. Human vs. AI (Computer Vision)* [online]. Prague: Czech Technical University, Faculty of Electrical Engineering, Czech Institute of Informatics, Robotics and Cybernetics, October 21, 2020 [cit. 2023-07-20]. Available at: https://cw.fel.cvut.cz/b221/_media/courses/a6m33ksy/2022_cognitive_systems_vision_lec3_cns_ks.pdf.

19 HORÁČEK, Jiří. The synergistic effect of the current digital ecosystem and cognitive warfare operations on the human mind, and the possibilities of defence. *Lecture at the conference Mysl jako bitevní pole (Mind as a Battlefield)*, April 12, 2023. Prague: Evropský dům.

20 DRTINOVÁ, Daniela, HORÁČEK, Jiří. *O mozku, duševní nemoci a společnosti (About the brain, mental illness, and society)*. Prague: Vyšehrad, 2021, pp. 18, 24–28, 49, 56–58, 110–118.

21 ZLÁMALOVÁ, Lenka. Nejistota a sociální sítě rozkládají mozky (Uncertainty and social media break down brains). Interview with the neuroscientist Horáček [online]. *Echo24.cz,* February 23, 2023. [cit. 2023-08-20]. Available at: https://echo24.cz/a/Hxjw9/tydenik-echo-rozhovor-psychiatr-neurovedec-horacek-vymyvani-mozku-konspiracni-teorie.

[22] [23] Due to the accompanying uncertainty and stress, the adaptation process begins by rewriting "maps", whereby one is more prone to accept any would-be explanatory information (potentially fraudulent or altered content) that seemingly offers a solution to the stressful situation. This may lead to a greater level of rigidity and polarisation of opinions, where the offered explanation contradicts the world view of a particular individual or group.

Cognitive operations take advantage of these processes, especially of the uncertainty and low resilience of targeted individuals and populations.[24] They purposefully alter or slowly and gradually shift the surrounding reality, environment, and pooled information of the person who is the target of cognitive operations and who interacts with and accepts the planted content. The outcome of this process is the manipulation of the resulting "maps" and consequently of the entire experience, thinking, and actions of the individual, who at the same time is influencing the shape of the reality of their surroundings. Consequently, one can begin to question one's prior understanding of reality and begin to separate oneself from socially accepted consensus, values and rules. Negative or alarming messages with a strong emotional charge are a particularly effective means. Such messages cause people to experience more insecurity and stress. The ability to resist this particular action requires a high degree of critical thinking, an appreciation and understanding of how consciousness works, and that not all available explanations are true.[25]

4.2 Use of the Neurosciences

Neuroscience is a discipline dedicated to the nervous system, investigating the operation of the brain, the process of receiving and sorting information, and modelling the cognitive dimension (i.e. explaining, "reading", and changing the cognitive functions). It requires the collaboration between various disciplines such as biology, psychology,

[22] HORÁČEK, Jiří. The synergistic effect of the current digital ecosystem and cognitive warfare operations on the human mind, and the possibilities of defence. *Lecture at the conference Mysl jako bitevní pole (Mind as a Battlefield)*, April 12, 2023. Prague: Evropský dům.

[23] DRTINOVÁ, Daniela, HORÁČEK, Jiří. *O mozku, duševní nemoci a společnosti (About the brain, mental illness, and society)*. Prague: Vyšehrad, 2021, pp. 25–28, 34, 49, 56, 58, 70–71, 110–118.

[24] HORÁČEK, Jiří. The synergistic effect of the current digital ecosystem and cognitive warfare operations on the human mind, and the possibilities of defence. *Lecture at the conference Mysl jako bitevní pole (Mind as a Battlefield)*, April 12, 2023. Prague: Evropský dům.

[25] DRTINOVÁ, Daniela, HORÁČEK, Jiří. *O mozku, duševní nemoci a společnosti (The brain, mental illness and society)*. Prague: Vyšehrad, 2021, pp. 162–163.

medicine, physics, mathematics, and chemistry.[26] [27] [28] The artificial Intelligence (AI), big--data mining and other new advanced methods and experiments based on machine learning, massive databases, and specific algorithms are therefore widely used in neuroscience. The main aim is to ensure two-way communication between the computer and the brain, to create its full simulation and its operation in relation to human behaviour. Neuroscience is thus revolutionary in terms of the close proximity we find ourselves to an individual's brain and their cognitive abilities. [29] [30]

However, a number of potential benefits of the neuroscience, such as personalised and regenerative medicine, entail significant risks and raise a number of ethical questions. Currently, for example, neuroscience data sets have been undergoing the process of industrialisation. Without adequate regulatory mechanisms their content is prone to be misused for undesirable political and economic purposes.[31] [32]

5 SEGMENT 2: TECHNOLOGY

The new era has offered up a new environment, scope and ways of manipulating an opponent and its population in a particular, deliberate direction. Technologies and information-psychological tools, i.e. neurotechnology, AI, virtual reality, cyberspace and hacking[33], social media, networks, and many other means[34] have consequently made it possible to carry out cognitive warfare operations quickly, efficiently, and in masse. The

26 GROSTAD, Paul. CyCon 2022 DAY 3 Panel: Cognitive Warfare – Hacking the OODA Loop. *YouTube video* [online], July 13, 2022. [cit. 2023-08-20]. Available at: https://www.youtube.com/watch?v=H3RqF5PiqXM.

27 AKIL, Huda, MARTONE, Maryann E., and ESSEN, David C. Van. Challenges and Opportunitiens in Mining Neuroscience Data. *Science*, February 11, 2011, Vol. 331, pp. 708–711.

28 ALBRIGHT, Thomas D., KANDEL, Eric R., POSNER, Michael I. Cognitive neuroscience. *Current Opinion in Neurobiology*, 2000, Vol. 10, pp. 612–624.

29 NØRGAARD, Katrine, LINDEN-VØRNLE, Michael. Cyborgs, Neuroweapons, and Network Command. *Scandinavian Journal of Military Studies*, 2021, 4(1), pp. 94–107. DOI: https://doi.org/10.31374/sjms.86.

30 FRÉGNAC, Yves. Big data and the industrialization of neuroscience: A safe roadmap for understanding the brain? *Science*, October 27, 2017, Vol. 358, pp. 470–477.

31 MALANOWSKI, Norbert. Combining ICT and Cognitive Science: Opportunities and Risks. *The European Foresight Monitor Network.* Foresight Brief No. 152, August 2008, pp. 1–4.

32 FRÉGNAC, Yves. Big data and the industrialization of neuroscience: A safe roadmap for understanding the brain? *Science*, October 27, 2017, Vol. 358, pp. 470–477.

33 A commonly used definition of hacking is the act of compromising digital devices and networks through an unauthorised access to an account or computer system. Hacking is not always necessarily a malicious act, yet most often it is associated with illegal activity and data theft by cyber criminals.

34 STOIANOV, Nikolai. Cognitive Warfare and Its Implications for the NATO STO IST Panel. *NATO Science and Technology Organization* [online], June 21, 2021. [cit. 2023-08-23]. Available at: https://hal.science/hal-03635960/document.

current paradigm is thus being changed through many kinds of modern technologies that have the potential to push the boundaries of human functioning.[35] [36]

We are talking about factors that carry the potential for progress and significant benefits, as well as for destruction and fraud, and for bringing new, as yet uncharted risks[37]. Security has therefore become a matter not only for the traditional security actors of times gone by, but also for the private sector, academia, and every individual.[38] Nevertheless, assigning responsibility, authority, and ensuring transparency for the issue, as well as defining its boundaries through international law, is a fundamental problem.[39] The possible activation of Article 5 of the North Atlantic Treaty also poses a challenge, since cognitive activities traverse below the threshold of traditionally perceived conflict and in a so-called grey area of legitimacy.[40]

To understand cognitive warfare, it is important to introduce a technological platform that, in its present form, makes it possible to get the required manipulation techniques into the minds of targeted population groups more easily and directly than ever before, as well as to collect data about them.[41]

5.1 Neurotechnology as an "Inverter" of an Individual's Cognitive Abilities

Neurotechnology and neuroweapons are created to detect, degrade, enhance, or otherwise alter the functions of an individual's brain, their cognitive and other executive abilities.[42] [43] The output might thus be the creation of a "better" individual or a hybrid

35 KADTKE, James, WELLS, Linton II. Technology Is a Strategic National Security Component. *SIGNAL Magazine*, Jan 1, 2015, pp. 1–3.

36 FLORIDI, Luciano. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality.* Karolinum: New media studies. 2019.

37 KADTKE, James, WELLS, Linton II. Technology Is a Strategic National Security Component. *SIGNAL Magazine*, Jan 1, 2015, pp. 1–3.

38 *NATO*. Emerging and disruptive technologies. *NATO* [online]. Last updated June 22, 2023. [cit. 2023-08-23]. Available at: https://www.nato.int/cps/en/natohq/topics_184303.htm.

39 NØRGAARD, Katrine, LINDEN-VØRNLE, Michael. Cyborgs, Neuroweapons, and Network Command. *Scandinavian Journal of Military Studies*, 2021, 4(1), pp. 94–107. DOI: https://doi.org/10.31374/sjms.86.

40 BROSE, Robert. Cyber War, Netwar, and the Future of Cyberdefense. *IEEE Xplore* [online], 2015, [cit. 2023-08-22]. DOI:10.1109/CYCON.2015.7158466

41 WELLS, Linton II. Cognitive-Emotional Conflict: Adversary Will and Social Resilience. *Prism*, 2017, Vol. 7, No. 2, pp. 5–17.

42 GARDEN, Hermann, WINICKOFF, David. Issues in neurotechnology governance. *OECD Science, Technology and Industry Working Papers*, November 2018, pp. 1–24.

43 WURZMAN, Rachel, GIORDANO, James. 'NEURINT' and Neuroweapons: Neurotechnologies in National Intelligence and Defense. In GIOVANO James (Ed.), *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns*. Boca Raton: CRC Press. pp. 79–113, 2015. DOI: https://doi.org/10.1201/ b17454.

system integrating the benefits of machine and human cognitive capabilities[44]. Neurotechnology includes prosthetics, neuromodules, modern weapons systems linked to AI, and medical preparations affecting cognitive abilities. The increase in the sophistication and ability to read brain activities and use of lie detectors is also being matched by improvements in interrogation methods and machines assist people in logistics and military decision-making.

A number of ethical issues necessarily arise in relation to these processes. Misuse of these technologies might lead to the serious vulnerability both of the individual and the protected population. At the same time, their nature causes confusion as to who will bear legal and ethical responsibility for the output and use of neurotechnology.[45] [46]

5.2 Information and Communication Technologies (ICT) as the Main Tool of Cognitive Operations

ICT have changed the character of contemporary human society, which has become completely dependent on them. With greater frequency they are influencing our self-perception and how we interpret the world around us. [47] It provides humans with communication and entertainment applications, where information is transmitted in previously unimaginable volumes.[48] Attackers make good use of the hyper-connectivity[49] provided by cyberspace, the Internet, social media, and other channels. Cyber operations and cyberattacks make it possible to influence targeted audiences over long distances at a relatively small cost, and in a short time. These are an apposite means for performing information and psychological operations, which may disrupt cohesion and polarise society as a whole.[50] Threats arising from ICT also include invasion of privacy,

44 Cyborg refers to the hybrid of a biological organism and a machine. This term is mostly used to describe people whose bodies are permanently supplemented with artificial components.

45 NØRGAARD, Katrine, LINDEN-VØRNLE, Michael. Cyborgs, Neuroweapons, and Network Command. *Scandinavian Journal of Military Studies*, 2021, 4(1), pp. 94–107. DOI: https://doi.org/10.31374/sjms.86.

46 TENNISON, Michael el N, MORENO, Jonathan D. Neuroscience, Ethics, and National Security: The State of the Art. *PLoS Biology*, 2012, Vol. 10, Iss. 3, pp. 1–4.

47 FLORIDI, Luciano. *The Fourth Revolution: How the Infosphere is Reshaping Human Reality.* Karolinum: New media studies. 2019.

48 ARQUILLA, John, RONFELDT, David. Cyberwar is Coming! *Comparative Strategy*, 1993, Vol. 12, No. 2, pp. 23–60.

49 DRTINOVÁ, Daniela, HORÁČEK, Jiří. *O mozku, duševní nemoci a společnosti (About the brain, mental illness, and society)*. Prague: Vyšehrad, 2021, pp. 160–163.

50 KADTKE, James, WELLS, Linton II. Technology Is a Strategic National Security Component. *SIGNAL Magazine*, Jan 1, 2015, pp. 1–3.

data theft, etc., their disruption poses a risk of the functioning of the administrations of individual countries.[51] [52]

5.3 Artificial Intelligence (AI)

The influence of ICT is strongly augmented by AI. Its so-called "deep learning" ability has been inspired by the functions and structure of the brain. Together with other analytical tools, it performs detailed data collection and analysis in the information environment.[53] [54] AI offers the possibilities of learning, searching, and the easier operation of critical infrastructure, etc.[55] [56]

However, its abilities can be relatively easily misused for learning about the psychology and internal settings, for the targeted manipulation of cognitive abilities of a selected population and individuals,[57] for fraud, political infiltration, and for conducting cyberattacks and crimes.[58] AI's algorithms also directly influence the content people see online, leading to rigidity and to selective access to information by citizens.[59] With all these risks comes a potential to jeopardise political, economic and social security and system itself.[60]

51 SINGER, Peter W., FRIEDMAN, Allan. *Cybersecurity: What Everyone Needs to Know.* Oxford University Press. 2014.

52 JEONG, Doowon. Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues. *IEEE Access*, 2020, Vol. 8, pp. 184560–184574.

53 ARMY CAPABILITIES INTEGRATION CENTER – FUTURE WARFARE DIVISION. *Operationalizing Robotic and Autonomous Systems in Support of Multi-Domain Operations* [White Paper] [online], 2018, [cit. 2023-08-22]. Available at: https://info.publicintelligence.net/USArmy-RoboticAutonomousMultiDomainOps.pdf.

54 JEONG, Doowon. Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues. *IEEE Access*, 2020, Vol. 8, pp. 184560–184574.

55 ZENG, Yingjie. AI Empowers Security Threats and Strategies for Cyber Attacks. *Procedia Computer Science*, 2022, 208, pp. 170–175.

56 KADTKE, James, WELLS, Linton II. Technology Is a Strategic National Security Component. *SIGNAL Magazine*, Jan 1, 2015, pp. 1–3.

57 GROSTAD, Paul. CyCon 2022 DAY 3 Panel: Cognitive Warfare – Hacking the OODA Loop. *YouTube video* [online], July 13, 2022. [cit. 2023-08-20]. Available at: https://www.youtube.com/watch?v=H3RqF5PiqXM.

58 JEONG, Doowon. Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues. *IEEE Access*, 2020, Vol. 8, pp. 184560–184574.

59 HORÁČEK, Jiří. The synergistic effect of the current digital ecosystem and cognitive warfare operations on the human mind, and the possibilities of defence. *Lecture at the conference Mysl jako bitevní pole (Mind as a Battlefield)*, April 12, 2023. Prague: Evropský dům.

60 ZENG, Yingjie. AI Empowers Security Threats and Strategies for Cyber Attacks. *Procedia Computer Science* 2022, 208, pp. 170–175

5.4 Wearables

Wearables (e.g. smartwatches and chips) is an object connecting people to the Internet. It actively collects physiological data from devices worn directly on the body.[61] That can be used in healthcare, i.e. for disease monitoring, detection deterioration in health, promoton of a healthy lifestyle.[62]

However, due to the openness of protocols and other security imperfections, they are highly vulnerable to various cyberthreats, the collection or modification of personal data, and the surroundings in which we operate, or to a general breach of trust, to the availability, credibility and integrity of data. This opens up the possibility not only to obtain accurate data on the targeted population on a massive scale, alter its content, control the device, but also to manipulate individuals at times when they are most vulnerable.Similar threats apply to other commonly used devices and objects that are connected to the Internet (so-called Internet of Things), or to nanotechnologies and nano-weapons that are expected to start a new industrial revolution and have the potential to disrupt the entire immune system.[63] [64] [65] [66] [67] .

5.5 Virtual Reality (VR), Augmented Reality (AR), Gaming, and Cinema

The prospect of escaping to alternative experiences, whether in the unreal environment of virtual and augmented reality, games or movies, represents an attractive opportunity for an interactive experience. Thanks to involving a great number of sensations, it is a way of providing information and entertainment for lots of individuals. We must increasingly anticipate ever more extensive possibilities for influencing the cognitive abilities of an individual in a given area as characterising the next generation of social media. This would bring enormous risks not only in relation to obtaining information

61 GAO, Yiwen, LI, He, LUO, Yan. An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, 2015, Vol. 115, No. 9, pp. 1704–1723.

62 ZAMAN, Shakila, ALHAZMI, Khaled, ASEERI, Mohammad, et. al. Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey. *IEEE Access*, 2021, Vol. 9, pp. 94668–94690.

63 TSENG, Tzu Wei, WU, Chia Tung, LAI, Feipei. Threat Analysis for Wearable Health Devices and Environment Monitoring Internet of Things Integration System. *IEEE Access*, 2019, Vol. 7, pp. 144983–144994.

64 GROSTAD, Paul. CyCon 2022 DAY 3 Panel: Cognitive Warfare – Hacking the OODA Loop. *YouTube video* [online], July 13, 2022. [cit. 2023-08-20]. Available at: https://www.youtube.com/watch?v=H3RqF5PiqXM.

65 DRESSLER, Falko, KARGL, Frank. Towards security in nano-communication: Challenges and opportunities. *Nano Communication Networks,* 2012, Vol. 3, pp. 151–160.

66 KOSAL, Margaret E. The security implications of nanotechnology. *Bulletin of the Atomic Scientists* [online], July/August 2010, [cit. 2023-08-22]. DOI: 10.2968/066004006.

67 IONESCU, Adrian M. Nanotechnology and Global Security. *Connections,* 2016, Vol. 15, No. 2, pp. 31–47.

through seemingly natural conversations or other communication flows and, e.g., deep fake technologies, but also in manipulating human emotions, an individual's imagination, and the way they view reality itself.[68] [69] [70]

Virtual and augmented reality also pose a threat to user privacy and user data preservation. Likewise, it is easy to modify the content that is transferred in them. With their help, it is possible to determine the location of the player, their biometrics as well as behavioural patterns, or to acquire other personal data. Of course, VR and AR also fully influence an individual's emotional state by manipulating and creating an illusion of the surrounding "environment" and the situations the player finds themselves in.[71]

An additional media having impact on individuals and forming their opinions, attitudes, emotions, and desires is cinematography, which presents and conveys the idea of a "perfect" world or other targeted structural, opinion-forming, value-forming, and social patterns. Opponents can misuse cinema not only to plant certain ideas, information and views, but also to distract audiences from reality or to render individuals and societies ineffective.[72]

6 SEGMENT 3: THE SOCIAL SCIENCES

For cognitive warfare to succeed, it is essential to know how the mind works and how information-processing works, as well as the technological platform by which the required information reaches the mind of the target population. The form and content of the disseminated narrative is also an integral part of this process, so that it reflects the target group as much as possible across the spectrum of characteristics that will increase the likelihood that the disseminated discourse will succeed in achieving the intended effect of the cognitive operation.

In the case of offensive cognitive operations, a deep knowledge of the target audience of the opponent is essential. With defence against the effects of cognitive operations, knowledge of one's own nation is essential to the extent that is possible to prepare measures that will allow the negative impact of the enemy's actions against one's own population to be minimised. In both cases, it is essential that the knowledge of the target or one's own population is deep enough to enable the long-term preparation of active

68 PATEL, Parth D., TRIVEDI, Prem. A systematic literature review on Virtual Reality and Augmented Reality in terms of privacy, authorization and data-leaks. *Cornell University,* December 9, 2022.

69 GROSTAD, Paul. CyCon 2022 DAY 3 Panel: Cognitive Warfare – Hacking the OODA Loop. *YouTube video* [online], July 13, 2022. [cit. 2023-08-20]. Available at: https://www.youtube.com/watch?v=H3RqF5PiqXM.

70 PATEL, Parth D., TRIVEDI, Prem. A systematic literature review on Virtual Reality and Augmented Reality in terms of privacy, authorization and data-leaks. *Cornell University,* December 9, 2022.

71 BAKER, Christopher, PAWLING, Ralph, FAIRCLOUGH, Stephen. Assessment of threat and negativity bias in virtual reality. *Scientific Reports*, 2020, Vol. 10, pp. 1–10.

72 DEPPO, Serge da. Mind Like a Battlefield. *Greetings at the Mind Like a Battlefield Conference*, April 12, 2023, Prague: Evropský dům.

measures, whether offensive or defensive. This issue can be considered broadly interdisciplinary, and it is the domain of the social sciences and humanities, which are used for building a picture of the target audience.

There is a wide range of criteria that shape the characteristics of a nation or its chosen social group. Alongside these will be a number of factors that make the target group more vulnerable to the effects of cognitive warfare tools, or, on the contrary, more resilient than others.

6.1 Political Context

The political context at all levels of the target state is of fundamental interest in the process of cognitive warfare. In particular, internal politics at the regional and national level, reflecting the political preferences of voters, is highly indicative of the opinion spectrum of the population and individual groups.

Understanding the political system and institutional order allows one to target the effect of cognitive warfare tools on the creation or support of narratives questioning the fairness of the political order, the erosion of trust in the institutions of state administration and public self-government, the credibility of political representatives, or the un-fairness of the electoral system, and to induce a sense of the erosion of the existing political order and to support efforts to change it both by legal and illegal means.

6.2 Economy

Actions aimed at the civilian population include attempts to create the desired image for foreign investors, especially in contracts of strategic importance and with key infrastructure. An important element of these activities is forming conditions for the exercise of financial influence and material dependence. Targeted and skillfully disseminated narratives may relate to problems of non-transparent deal-making, environmental degradation, industrial pollution, lack of transparency in lending, and corruption. Cognitive tools can be used to hide existing problems of this nature or vice versa to discredit a selected target by creating an impression that such negative facts exist without this actually being the case. A poor socio-economic situation is a breeding ground for distrust of government, state institutions, and for the overall questioning of political mechanisms and processes.

6.3 Societal Area

In the context of cognitive warfare, characteristics that are shaped in society over the long term, which have a low probability of being changed rapidly, and that can be

influenced by external action, i.e. from outside the society itself, only very little or not at all, can be considered crucial.

The primary goal of cognitive tools is not to completely change these characteristics, but rather to make the most of them instead – adapting the content of disseminated narratives and the form of their distribution to the target group. A deep knowledge of these characteristics is a prerequisite for successful action on the opponent's mind, or, in the case of a defence against cognitive warfare, to protect one's population. The complexity and the interdependence of these parameters shape the complexity of this segment.

At the practical level, the experience of one environment is not transferable to another. What works in one country will certainly not work in the conditions of another, and what works in relation to a certain social group will certainly not work in relation to another.

6.4 Psychology of the Nation

This characteristic is also sometimes referred to as national character or national mentality, and is an umbrella term for a more stable psychological characteristic of a particular nation. Such psychology is derived from various factors, e.g. the nature of the landscape, historical experience, or linguistic peculiarities and it relates to the typical conditions of life of a particular national population.

It includes, for example, the application of certain procedures in relation to raising children and subsequent generations. Certain political, cultural, and other events can be derived from the supposed or observed characteristics of particular nations.[73]

In the narrower meaning of psychology, it is a comparative discipline examining psychological phenomena and traits that distinguish one ethnicity from another. Nowadays, it can be equated to ethnopsychology.[74]

6.5 Religion, Faith, History

Hásová et al. state: "Religious belief and historical consciousness are indicators that refer to a particular kind of memory. We understand memory as a means of maintaining certain patterns of behaviour, actions, and thinking across generations. Relation to history and historical consciousness refers to historical memory, which is defined as a shared understanding of historical events and individuals' own attitude towards knowledge of

[73] NEŠPOR, Zdeněk at al. Charakter národní (National character). *The Sociological Encyclopedia* [online]. Prague: Institute of Sociology of the Czech Academy of Sciences [cit. 2023-07-25]. Available at: https://encyklopedie.soc.cas.cz/w/Charakter_n%C3%A1rodn%C3%AD.

[74] NEŠPOR, Zdeněk et al. Völkerpsychologie. *The Sociological Encyclopedia* [online]. Prague: Institute of Sociology of the Czech Academy of Sciences [cit. 2023-07-25]. Available at: https://encyklopedie.soc.cas.cz/w/V%C3%B6lkerpsychologie.

history and history itself. In our era, which is driven by modernisation and rising individualism, memory is threatened and yet at the same time it is a key source of identity."[75]

The link between the historical development of a nation and its religious identity is one of the most important characteristics, if not the most important. Nations playing an important role in world history which have a strong institutionalised religious identity undoubtedly have different collective characteristics than nations with marginal historical significance, without a firm anchor in the system of the world's major religions, and with built-up historical skepticism. From a cognitive perspective, each of these categories will require a completely different approach and the use of different tools.

6.6 Social Relations in Society

In this area, we may include a variety of social characteristics that are of particular importance in the process of understanding the target group. These include, in particular, ethnic composition, age groups, social stratification, mobility, social classes, social inequalities, occupational and labour market structure, consumption, leisure, mass and individual culture, deviant behaviour, the structure of social institutions, arrangement of urban and rural settlements, and everyday life in the particular society.[76]

6.7 Value System

We can refer to the order and priority that an individual or society assigns to certain values as a value system. Even if an individual or society shares a common set of values, this does not mean that they will respectively assign equal weight to its individual elements. A value system is evolutionary, reflecting social development, as well as the existential status of a person or segment of a population. In practice, there are differences between an idealised and realised value system, i.e. one that is looked up to as an ideal and one that is used in everyday life. The difference between individualism and collectivism is an important aspect, with a direct impact on the value system.[77]

In the context of cognitive warfare, it is also necessary to monitor value orientation. This manifests itself in the situational, short-term, or long-term degree of importance

75 HÁSOVÁ, Veronika, Jan VÁNĚ, Jiří VINOPAL et. al. Religious Faith and Relationship to History – Analysis of Interconnection. *Acta FF,* 2019, **11**(1), 1–18, p. 2. ISSN 23366346. Available at: doi:10.24132/actaff.2019.11.1.1

76 NEŠPOR, Zdeněk et al. Sociology. *The Sociological Encyclopedia* [online]. Prague: Institute of Sociology of the Czech Academy of Sciences [cit. 2023-07-25]. Available at: https://encyklopedie.soc.cas.cz/w/Sociologie

77 Value systems. *Psychotherapeutic database: Encyklopedie* [online]. [cit. 2023-07-25]. Available at: https://dbterapie.cz/encyklopedie/hodnotove-systemy/.

that an individual or part of society attaches to certain ideals, characteristics, and phenomena affecting their practical behaviour.[78]

6.8 Legal System and the Rule of Law

Belief in the stability and functionality of the legal system and the rule of law represent basic attributes of the trust a population has in the basic arrangements of state power and its credibility. This parameter has a significant impact especially in democratic countries, where it occupies the position of natural target for the action of cognitive warfare tools. The creation of distrust in the legal system and law enforcement is therefore a strong motive for acting on social stability, in particular if an impression can be created that the law only applies to a certain group of the population, while for another group it is unenforceable.

CONCLUSION

Cognitive warfare is a term that has been used more in recent years. Given the term "warfare", we might think that this phenomenon would relate exclusively to the military field and to the broader conduct of military operations under the conditions of the technologically advanced battlefield of the 21st century. However, from brief practical experience with the issue, we can learn it actually refers to forms of influencing the mental processes of target groups, i.e. psychological, information, influence operations. In the context of reflections on the nature of cognitive warfare, the issue of disinformation spread by modern communication platforms is often discussed, noting that this is the problem at the heart of presented phenomenon.

Nevertheless, cognitive warfare differs from previously used forms of action in the information space with an impact on the thinking of target groups thanks to its targeted and sophisticated use of scientific knowledge from the neurosciences. Disseminated narratives and the choice of the most suitable technological platforms for their distribution to the target audience are adapted to this deeper understanding of how the human mind operates. It is through the use of neuroscience that earlier forms of informational and psychological activity have reached a new level.

In defining cognitive warfare, the manner and degree of involvement of neuroscientific knowledge has not yet been determined, however. Nowhere is it specified what form the new quality should take compared to the traditionally used forms of information activity. In this respect, further focused research on the phenomenon of cognitive warfare is required, fully respecting the differences of the subject of research of all three described segments. At the same time, conceptual ambiguity and a lack of conceptual and

78 PRUNNER, Pavel. *Výzkum hodnot (Value research)*. Plzeň: Euroverlag, 2002, pp. 27–28, ISBN 80-7177-710-2.

doctrinal anchoring prevent a deeper understanding of individual segments of cognitive warfare and their interdependence.

This article therefore introduced a conceptual classification of cognitive warfare, its forms, its tools and the three main segments it connects: neurosciences, technology, and social sciences. Only further research on these core disciplines together will enable an understanding of the phenomenon and provide insights into how to address it. The importance of cognitive warfare in the near future is already sufficiently evident and poses a new fundamental challenge not only to the armed forces and security authorities, but to the defence and security community in general.

Authors: ***Kristýna Drmotová****, born 1997. She is a graduate of Security and Strategic Studies at the Faculty of Social Studies of Masaryk University in Brno (2022). Since 2022, she has been working as an academic at the Institute of Intelligence Studies at the University of Defence in Brno, where she is also pursuing her PhD studies. Her research, lecturing and publishing activities focus on cognitive warfare and regional security in the Indo-Pacific, particularly in East and Southeast Asia.*

Colonel Assoc. Prof. Libor Kutěj, Ph.D., *born 1967. Since 1992, he has worked in the security forces, first within the Ministry of the Interior and then within the Ministry of Defence. From 1996-2019 he was assigned to the Military Intelligence; from 2009-2012 he was the Defence Attaché of the Embassy of the Czech Republic in Israel, from 2012-2015 Director of the Military Diplomacy, from 2015-2019 Defence Attaché of the Embassy of the Czech Republic in Jordan. Since 2019, he has been active in academia, from 2019-2022 as Head of the Department of Intelligence Support at the Faculty of Military Leadership at the University of Defence. Since 2022, he is the Director of the Institute of Intelligence Studies at the same university, where he has also held the position of Vice-Rector for External Relations and Internationalisation since September 2020. His lecturing, research and publication activities focus on intelligence issues, cognitive warfare and the political-military and security context in the Middle East and East and Southeast Asia regions.*

How to cite: DRMOTOVÁ, Kristýna and Libor KUTĚJ. Cognitive Warfare as a New Dimension of Security. A fictional concept or a real silent threat? *Vojenské rozhledy*. 2024, 33 (1), 063-083. ISSN 1210-3292 (print), 2336-2995 (online). Available at: www.vojenskerozhledy.cz