ACIG APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse

Received: 24.04.2023
Accepted: 10.07.2023
Published: 13.07.2023

Marco Marsili Department of Philosophy and Cultural Heritage, Cà Foscari University of Venice, Italy; Centre for Research and Development, Military University Institute, Portugal, ORCID: 0000-0003-1848-9775

Abstract

Hybrid warfare is currently among the most trending topics. Hybrid threats arise in digital, cybernetic, and virtual environments and materialise in the real world. Despite being a somewhat vague term, hybrid activities include cyberwarfare, information warfare, and the emerging and evolving concept of cognitive warfare which appears from their intersection. These buzzwords gained popular attention in the context of the Russo--Ukrainian conflict and such terms are now in vogue. Even though these topics are in the spotlight, there is also widespread confusion about what exactly these usages mean and what the implications are in branding them as "warfare". Indeed, all these concepts are fluid, nebulous, and lack an undisputed legal definition. This article aims to clarify their meaning and to shed light on the characteristics of such terms – differences, similarities and overlaps – in the context of hybrid warfare and show the faulty reasoning upon which misunderstandings are based. The paper concludes with a glimpse into the future, closing with a reflection on multi-domain operations facilitated by a fully integrated human--computer interaction in the metaverse, where physical reality is merged and interacts with digital virtuality.

Keywords

cognitive, cyber, information, international humanitarian law, metaverse, warfare

Cite this article as:
M. Marsili, "Guerre à la Carte: Cyber, Information, Cognitive Warfare and the Metaverse," ACIG, vol. 2, no. 1, 2023, DOI: 10.5604/01.3001.0053.7402

Corresponding author:
Marco Marsili, Department of Philosophy and Cultural Heritage, Cà Foscari University of Venice, Italy; Centre for Research and Development, Military University Institute, Portugal; E-mail: marco_marsili@iscte-iul.pt

1. Introduction – The Nature of War

The nature of war has remained unchanged over time. Despite the popular quote attributed to Sun Tzŭ – "The nature of war is constant change" – the Chinese general never actually wrote this. On the contrary, in *The Art of War*, a tactical treatise for which he is traditionally credited as the author, Sun Tzŭ, concludes that "in warfare, there are no constant conditions" [1, p. 53, § 32], which means, in the context of the text, that the battle is affected by ground, weather, and other contingent factors. In another overquoted classic book, *On War*, Clausewitz defines war as "an act of force to compel our enemy to do our will" [2, p. 75]. In his masterpiece, the Prussian general emphasises the use of "physical force" as an essential feature of war [2, p. 75]. As one of the most important treatises on political-military analysis and strategy ever written, even two centuries after its publication *On War* still influences strategic thinking. However, the core tenet of the book is undermined by misunderstandings and misleading interpretations [3, p. 90].

Kaldor [4, p. 221] argues that Clausewitz understood war as "the use of military means to defeat another state" and rejects this approach to warfare as no longer applicable in today's conflicts. She believes that current and future conflicts will not be ended through military victory, although violence remains a key feature. But the nature of war is always the same: defeat the enemy [1, p. 26–27]. A perfect summary of the nature of war is provided by Clausewitz himself: "[w]ar is more than a mere chameleon that slightly adapts its characteristics to the given case. As a total phenomenon, its dominant tendencies always make war a paradoxical trinity – composed of primordial violence, hatred, and enmity" [2, p. 89]. While the war on the battlefield is subject to specific conditions, which may change due to multiple factors, the nature of war is characterised by extreme violence and the use of weapons to overcome the enemy [2, p. 101, 3, p. 99, 5, p. 85, 6, pp. 68–69, 71–72].

Despite far too much rhetoric on the extension of the term "war" or "warfare", armed conflict is regulated by the legal framework provided by the Geneva Conventions, which define the perimeter of international humanitarian law (IHL), i.e., the "law of war" – IHL regulates the conditions for initiating war (*ius ad bellum*) and the conduct of waging parties (*ius in bello*), including occupation, and other critical terms of the law. Indeed, the wording "armed conflict" is relevant in the Conventions [7, p. 182, 8, pp. 40–41]. Therefore, any use of the term "warfare" which does not involve the use of lethal weapons, is inappropriate [7, p. 191, 8, p. 45]. Due to overuse and misuse, "warfare" is now also applied to military operations other than war (MOOTW) [9, p. 154, 8, pp. 40–41]. Cyber-attacks may violate international law, when conducted or orchestrated by states, or may constitute cybercrime, but certainly cannot be treated as kinetic attacks in the light of IHL [7, p. 191, 8, pp. 42, 44–45]. Information warfare (IW) is not per se a change in the nature of war but rather a technological advance that can enhance lethal capacities [10, pp. 16–19, 8, pp. 44–45]. There is no evidence of any change to the nature of war [3, pp. 91–92, 98, 10] – what changes is technology, along with techniques, tactics, and procedures [9, p. 152–156, 8, p. 37]. The topics of this paper should not be examined in isolation but should be seen as the first part of a larger argument. Nevertheless, there is an emerging doctrine that aims to characterise as "warfare" and/or "war" actions that are MOOTW; this trend mainly concerns "hybrid" operations, among which falls the cognitive domain[1]. That is why this premise is relevant to distinguish MOOTW activities from actions involving the use of actual force.

As M. L. R. Smith writes [11, p. 52], "Call it what you will – new war, ethnic war, guerrilla war, low-intensity war, terrorism, or the war on terrorism – in the end, there is only one meaningful category of war, and that is war itself" and Geneva Conventions apply. On these grounds one must reject the argument of Israeli military historian and theorist Martin van Creveld [12, pp. 57–58] "[t]hat organized violence should only be called 'war' if it were waged by the state, for the state, and against the state".

[1]See §3: Cognitive Warfare.

A state-centric approach to war is contradicted by the Conventions, which are crucial to some extent. Clausewitz conceptualised war as the application of violent means to realise military aims to achieve political ends, regardless of who the contenders are [3, p. 95].

2. Ruses of (Hybrid) Warfare

Foucault inverts Clausewitz's traditional conception of war and says that politics is the continuation of war by other means [13, p. 19]. Hybrid warfare is a concept that includes a wide range of tools – a bouquet of various techniques, methods, technologies, tactics, procedures and means, military and civilian, conventional and unconventional – for achieving a political or military objective [8, p. 37, 9, p. 151]. It is questionable whether *ruse de guerre* is legitimate or not. Misinformation, deception and electronic deception, electronic warfare, and psychological warfare are customarily accepted as lawful, and therefore they do not violate any general rule of international law applicable to armed conflict, so long as they do not involve treachery or perfidy [14, § 50–51, 15, §§ 8–3(b), 8–4(a), 8–5, 16, §§ 12.1, 12.1.1].

The European Union's definition of hybrid activities ranges from cyber-attacks through to disinformation; a combination of "coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological)" [8, pp. 42–43]. The use of these tactics, aimed at targeting political institutions and influencing public opinion [9, p. 153, 155], is facilitated by rapid technological advances that reach a broad audience and which therefore boosts their impact.

NATO encompasses propaganda, deception, sabotage, and other non-military tactics among the hybrid methods of warfare [17]. The allies endorsed a vague definition of hybrid warfare at the 2016 Warsaw Summit: "a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures" that are "employed in a highly integrated design by state and non-state actors to achieve their objective" [18, § 72]. The final communiqué issued at the 2021 meeting in Brussels groups cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and sophisticated emerging and disruptive technologies [19, §§ 3, 12, 31].

While the Alliance has defined hybrid threats, the U.S. Department of Defense (DOD) has not officially provided a definition and has no plans to do so because hybrid warfare is not considered a new form of warfare since is a very broad term that blends conventional, unconventional, and irregular approaches across the full spectrum of conflict [20, p. 2, 11, 14].

Matuszczyk [21, p. 21] finds that these ruses of war, that go beyond conventional military capabilities, are simply creative, clever, unorthodox means. Bearing in mind that IHL sets the limits for acceptable wartime conduct (*ius in bello*), hybrid operations which do not involve the use of lethal force (despite being referred to as "warfare") fall below the threshold of armed conflict and cannot be characterised as such [8] – the lexicon and terminology are relevant to this end. If we accept that Clausewitz's famous statement that war is not merely an act of policy but a true political instrument, a continuation of political intercourse carried on with other means, we must therefore consider propaganda as a political tool [22, p. 23].

3. Cognitive Warfare

Although there is no common definition of hybrid warfare, the inclusion of propaganda, information and influence operations, deception and psychological operations is widely accepted [9, p. 151]. Information warfare includes a set of techniques and technologies that ranges from electronic warfare to propaganda [9, p. 153], intertwined with the real and the virtual operational domains. The virtual realm encompasses electronic

warfare (EW), electromagnetic spectrum operations (EMSO), cyberspace operations (CO), information warfare (IW), psychological operations (PSYOP), now better known as military information support operations (MISO), information operations (InfoOps or IO), also known as influence operations, strategic communications (STRATCOM), military deception (MILDEC), computer network operations (CNO), operations security (OPSEC), perception management (PM), public information (PI), and public diplomacy (PD) [9, pp. 152–154].

Joint Publication 3-13, which provides doctrine and guiding principles for the U.S. Armed Forces, characterises IO as intended "to influence, deceive, disrupt, corrupt, or usurp the decision making" [23, § GL-3]. A 2018 U.S. Army pamphlet drafted by the Training and Doctrine Command (TRADOC) proposes the following definition of IW: "Employing information capabilities in a deliberate disinformation campaign supported by actions of the intelligence organizations designed to confuse the enemy and achieve strategic objectives at minimal cost" [24, § GL-6]. The publication highlights the relevance of information environment operations (IEO) and the convergence between the physical, virtual, and cognitive dimensions [24, §§ 3-3(d), 3-8(e), C-1].

The Information Environment (IE) impacts on the three dimensions (physical, virtual, cognitive). The fact that most cognitive activities occur primarily in the virtual domain does not mean that they have no effects in the real world. We can distinguish between two types of information disruption. The first is cognitive disruption, which includes any action (e.g., disinformation and propaganda) that directly targets individuals. The second is a functional disruption (e.g., cyberspace and electromagnetic attack) that directly targets systems and facilities (e.g., computers, weapons, vehicles) [25, § 3–15].

A U.S. Marine Corps publication introduces a conceptual framework on the ever-changing information environment in all warfighting domains, and highlights that information is "the foundation of all human interaction", accelerated and expanded by technologies "with a tempo and scale previously unimaginable" [25, Foreword]. The booklet quotes Sun Tzu's maxim "All warfare is based on deception" and acknowledges the relevance of deception defined as "an information activity [...] to deceive the human mind, the machine the human relies on, or both" [25, §§ 2–22, 2–23]. The human-machine interaction is a fundamental component of cognitive warfare (CogWar) and plays a central and crucial role, due to the way our perception and judgment are affected, thus making it an unprecedented challenge.

Today's world is characterised by the widespread use of mobile digital communications and media which operate in largely ungoverned digital spaces [25, § 3–18]. The intersection of the information, physical and cognitive/social domains [9, p. 152], empowered by the digital ecosystem – the Internet, social media, and communication applications – creates the conditions for cognitive operations. Though there is nothing new among its individual components, the novelty in CogWar is the speed and power of dissemination of beliefs – false or true – instilled deeply in the consciousness of targets. The "infodemic" that arose in the context of the COVID-19 pandemic [26] can serve as a touchstone. This blurring effect makes people unknowingly susceptible to placing undue trust in specific information and sources or withholding it altogether due to outright confusion.

As human cognition is highly susceptible to manipulation and deception, CogWar aims to influence thinking processes, such as perceptions, decision making and behaviour [25, § 2–19]. Recognising and dispelling misinformation and disinformation requires critical thinking skills to identify untrustworthy information sources, and to understand how one's own potential cognitive biases may increase one's susceptibility to manipulation or influence [25, § 2–15]. This weaponised use of information serves to build and reinforce biased or false narratives, altering the perception and the behaviour of individuals and ultimately that of society [9, pp. 162–165]. Indeed, CogWar targets

influential individuals, specific groups, and large numbers of citizens selectively and serially within society, with the potential to fracture and fragment an entire society or disrupt alliances [27].

In short, CogWar is a form of propaganda spread through manipulated media or social media for political or military purposes and aimed at fostering and instilling biased and conflicting narratives among targeted individuals, so as to make them behave accordingly by clouding their judgement. Therefore, what is most concerning about the cognitive effects of CogWar in peacetime is not its impact on the battlefield but the political and social consequences.

Cognitive science is the study of the human mind and brain, focusing on how the mind represents and manipulates knowledge and how mental representations and processes are actualised in the brain. Its interdisciplinary features – linguistics, psychology, neuroscience, philosophy, computer science/artificial intelligence, anthropology, and biology – make cognitive science an autonomous academic discipline which studies the mind and its processes from different perspectives and approaches. It deals with human behaviour, with a focus on the mind and its interactions with the surrounding world, and how nervous systems represent, process, and transform information, and therefore is crucial to understanding the relevance and the impact of CogWar on brain, mind, and behaviour.

There are different views regarding the definition and intended scope of cognitive science, which can be considered "a multidisciplinary endeavour" that integrates methods and theories [28]. Paul Thagard [29] connects the origins of cognitive science to the first studies about the nature of human knowledge, of mind and mental operations, and to experimental psychology, linking them to the mid-50s, when primitive computers appeared, and artificial intelligence (AI) started to become conceptualised. In such context, Arthur Samuel [30] coined the term "machine learning" in 1959, following the publication (1950) of Alan Turing's seminal paper "Computing Machinery and Intelligence" [31]. Since then, AI, which comes from a deep learning approach based on neural networks, has become a central part of cognitive science [29].

While on the one hand it is clear that cognitive science is deeply interconnected to the human mind, on the other hand in order for it to be an autonomous discipline it needs an artificial – electronic and digital – environment provided by computers. Against this background, artificial intelligence and machine learning play a fundamental role, along with digital multimedia platforms, that empower global interconnectivity.

Thagard [29] finds that people have mental rules and procedures for generating new rules. CogWar techniques rely on such mental patterns and thereby influence the decision-making process and the behaviour of target populations by predicting and manipulating the results of perceptions and actions[2]. From these definitions and concepts we can infer the relevance and impact of CogWar, and the attention and concerns it raises.

The importance of CogWar and related topics is highlighted, inter alia, by the recent release (Sep. 2022) of the U.S. *Joint Publication 3.04 – Information in Joint Operations*, which provides fundamental principles and guidance to plan, coordinate, execute and assess the use of information during joint operations [32]. The revised doctrine, which has not been publicly released, briefly introduces cognition and its cognitive impact within the IE [32, §§ I-7, III-3, VI-2].

Both the U.S. joint doctrine and NATO policy have already recognised cyberspace as an operational military domain and are striving to include the cognitive realm among the battlefields [7, p. 178, 181]. As the cognitive dimension becomes ever more

[2]For a discussion on behaviourism, see, e.g., G. Graham, "Behaviorism," in The Stanford Encyclopedia of Philosophy (Spring 2023 Edition), E.N. Zalta, U. Nodelman, Eds. [Online]. Available: https://plato.stanford.edu/archives/spr2023/entries/behaviorism/. [Accessed: July 4, 2023].

relevant in the present and future geopolitical challenges, NATO is taking the necessary action against "weaponised information" in modern warfare. The NATO Allied Command Transformation (ACT) acknowledges that "the lines between peace and war, political and military, strategic and tactical, physical and non-physical are blurring" [33] and the Supreme Allied Command Transformation (SACT) Concept Development Branch (CNDV) has been accordingly tasked by SACT to develop a concept on cognitive warfare [27]. The work is part of the implementation of the NATO Warfighting Capstone Concept (NWCC) through the Warfare Development Agenda (WDA). The CogWar Concept is a Line of Delivery (LoD) nested under the cross-domain command of the Warfighting Development Imperative (WDI) [34, § 1], as identified by the NWCC.

A cognitive warfare exploratory concept is currently under development by a NATO ACT team of experts. The goal is to develop an Exploratory CogWar Concept for approval by SACT during 2023 in order to implement the NWCC and leverage the WDA. This exploratory concept will include a final Cognitive Warfare Concept, to be approved by the Military Committee (MC) in the summer of 2024 – the MC develops strategic policy and concepts and provides guidance to SACT and as such is an essential link between the political decision-making process and the military structure of NATO, being tasked for translating political decision and guidance into military direction [35].

NATO's Military Strategy, adopted in May 2019, provides the Alliance with military-strategic objectives and the ways and means to implement them through two high-level concepts: the NWCC, as part of the WDA – a planning tool to implement the Warfighting Capstone Concept – and the Allied Command Operations (ACO) Concept for the Deterrence and Defence of the Euro-Atlantic Area (DDA) [33, 34]. Endorsed by NATO Heads of State and governments in 2021, the NWCC, often referred to as NATO's North Star, sets forth a 20-year vision by anticipating threats and understanding the strategic environment and specifically focuses on multi-domain operations (MDO), resilience, cognitive work and much more, enabled by digital transformation [33, 34]. MDO are how operations are conducted in time and space with synchronisation of all domains [36] and are described by the U.S. Training and Doctrine Command (TRADOC) as a mix of "unconventional and information warfare (social media, false narratives, cyber-attacks)" [24, vi, §§ 2-2, C-2, D-3].

According to the definition developed by the NATO team of experts, "'Cognitive Warfare' is the convergence of 'Cyber-Psychology', 'Weaponization of Neurosciences', and 'Cyber-Influence' for a provoked alteration of the perception of the world and its rational analysis by the military, politicians, and other actors and decision-makers, to alter their decision or action, for obtaining strategic superiority at all levels of tactical intervention concerning individual or collective natural intelligence, as well as artificial or augmented intelligence in hybrid systems" [8, p. 44].

The NATO Science and Technology Organization (STO) has endorsed a variety of Exploratory Teams (ET) and Research Task Groups (RTGs) on the subject of CogWar [37][3]. The System Analysis and Studies (SAS) Panel approved the following RTGs: SAS-177 on Defending Democracy in the Information Environment: Foundations and Roles for Defence; SAS-185 on Indicators and Warnings for Cognitive Warfare in Cyberspace. The Information Systems Technology (IST) Panel endorsed the following activities: IST-177 (RTG) on Social Media Exploitation for Operations in the Information Environment; IST-ET-123 on Exploring Countermeasures against Misinformation of a Nation's Population. Interdisciplinary research led by the Human Factors and Medicine (HFM) Panel include: HFM-374-RTG CogArmy: Cognitive training and teamwork assessment of Army personnel; HFM-ET-214 Cognitive Security: building and maintaining resistance to offensive cognitive strategies; HFM-ET-215 The Ethical and Legal Challenges of Cognitive Warfare; HFM-ET-216 Methods and Weapons of Adversary Cognitive Warfare; HFM-IST-ET-213 Visualization of Cognitive Warfare

[3]Situation updated as of 5 July 2023.

Situational Awareness; HFM-373-RTG Technology Enablers for Monitoring and Assessment of Humans in CogWar. These research activities were approved by different panels – which reinforces the cross-disciplinary of the topic (a good example of this is the SAS-HFM-ET-FE on Early Warning System for Cognitive Warfare in Cyberspace). Most of this research activity is classified or restricted and not publicly releasable and therefore we will not dwell on such content in this article.

In this context, the NATO STO Human Factors & Medicine Panel organised an HFM-361 Research Symposium (RSY) on Mitigating and responding to Cognitive Warfare in Madrid on 13–14 November 2023, aimed at supporting the WDA (as stated in the NATO NWCC) and providing information for science and technology guidance on improving countermeasures to CogWar, so as to meet and mitigate current and future security and defence challenges [38]. The proposal for a symposium on Meaningful Human Control in Information Warfare (HFM-377-RSY) to be held in the coming year is still pending.

4. The Metaverse: A New Domain of Warfare?

The term "metaverse" – a portmanteau which combines the words "meta" (meaning beyond) and "verse" (short for the universe) – increases the confusion on and around defence concepts that lack a workable definition. This hip buzzword was coined in 1992 by visionary author Neal Stephenson in his dystopian sci-fi thriller *Snow Crash* [39], which predicted the metaverse as a convergence between the real and the virtual world; a universe beyond the physical where physical reality is merged and interacts with digital virtuality [40, p. 486] facilitated by the Internet of Things (IoT). According to one of the many similar definitions, IoT "is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" [41].

The two words – metaverse and war – may sound completely unrelated but on closer consideration they are more intertwined than they may appear at first glance. The virtual and physical worlds are becoming increasingly interconnected, interdependent, and indistinguishable from one another. Metaverse wars draw together online and offline worlds. In traditional warfare, enemies go to war with (or over) something tangible. Since cyberspace was elevated to the domain of operations, just as for the three traditional realms of land, air, and sea [7, p. 178, 181], cyberspace became a virtual battlefield. This new way of waging war where opponents can do battle in a virtual environment could replace physical wars.

What happens in cyberspace does not necessarily stay in cyberspace. The metaverse can serve as a bridge to bring the actual force from the virtual to the real world, going far beyond the boundaries of a traditional conflict. As Stephenson wrote, "The Metaverse has now become a place where you can get killed" [39, p. 346] – a fictional statement which genuinely raises concerns. Kinetic actions can be materialised through cyberspace and reverberate their effects in the classic operational and physical domains. However, until cyber actions involve the use of lethal force, they fall below the threshold of armed conflict [7, pp. 189–191, 8, pp. 40–41].

Even if virtual actions cannot replace physical warfare as such, it does not mean that cyberwarfare has no negative impact. A drone attack conducted virtually can have lethal effects on the battleground. As war becomes the counterpart of communication, the latter unfolds its effects, even if not lethal, in the real world. This implies that a nation's power would no longer be decided just by its resources and manpower, but by its critical enabling capabilities across all domains. Stephenson writes that everything in the metaverse "depends upon the ability of different computers to swap information very precisely, at high speed, and at just the right times" and that "people who go into the Metaverse… understand

that information is power" [39, p. 400, 431]. If we connect these fictional words to the real world, we can easily imagine the impact of the metaverse on military operations, where the convergence between cyberoperations and electromagnetic operations plays a crucial role in gaining full spectrum dominance [42].

The concept of "full spectrum operations" highlights the influence of full--dimension operations on future doctrine [42]. Given the cross-domain, multi-domain, or all-domain operations doctrine, which prompts the military to conduct full spectrum operations to exert control over all dimensions of the battlespace [24], it seems clear that the metaverse may result in a new domain of warfare over time, although it is still too early to say how. What is also clear is the legal framework, which should be respected.

The significance of the interconnection between the cyber domain and the metaverse for multi-domain operations is confirmed by research commissioned by the Italian Ministry of Defence, in the scope of the Annual Research Plan (2023), with the purpose of identifying and exploring dual-use and innovative technologies to enhance military capabilities and gain a tactical advantage, in line with NATO STO trends [43].

While digital transformation enables MDO, emerging and disruptive technologies – including, *inter alia*, virtual and augmented reality – have further complicated the operational environment. The multi-domain environment can be dubbed the "metaverse", an immersive visual interaction between physical and virtual objects facilitated by advancing virtual reality (VR) and haptic technology [44, p. 97, 99]. The metaverse is bringing the physical and digital worlds closer together by expanding the possibilities of virtual and mixed reality and finally interacting with the physical and digital worlds. Potential applications in the metaverse include building and manipulating 3D objects and creating more intuitive, human-centred interfaces through AI [44, p. 94].

The next generation of wearable technologies – textile computing technologies that can sense and react to the human body – will enhance the experience of the users to provide a fully integrated human-computer interaction through digitisation of human biodata, activities, behaviours, and relationships, turning textiles into bidirectional interfaces that might find effective military applications [44, p. 99].

5. Conclusions

Emerging and evolving threats are coming from the virtual and cyber domains. Even if this appears to be nothing new, what is novel is the speed, scale and intensity of unconventional attacks, facilitated by rapid technological change and global interconnectivity. It is more than likely that such threats will increase in the future until they become prevalent over conventional (kinetic) means of warfare, although rapid technological advance and emerging military doctrine prevent us from reaching any definite conclusion at this point. Future research should scrutinise the impact of cognitive actions and the metaverse on individuals – a broad audience encompassing political and military leaders, policy and decision-makers and the society as a whole – and how international relations and warfare may be affected.

While rapid technological change makes the future of warfare uncertain and unpredictable, the metaverse seems to have the potential to become a new battlefield where information and cognitive operations could find their "natural" environment. Nevertheless, such operations are lawful either in the real or the virtual world; the emerging military doctrine cannot equate non-kinetic and non-lethal actions to a conventional attack.

"If we hold to the assertions by Sun Tzŭ, Clausewitz, M.L.R. Smith and Foucault, we must conclude that, while there is no distinction between political and military activity, the latter is characterised by the use of lethal weapons, and any other activity

has to be considered as below the threshold of armed conflict and outside the scope of war(fare) according to IHL. This also applies to actions in the information sphere and cognitive realm, together with cyberattacks originating from the metaverse, whose hybrid nature supports both kinetic and non-kinetic operations".

Although the legal framework is clear, governments and military organisations should strive to reach a legally binding and undisputed definition of threats coming from the digital world, whilst taking care not to brand them as "warfare" so as to avoid triggering any conventional response. International law cannot be made through one party's doctrine or policy. Peace is the most valuable commodity and is too precious to be endangered by virtual conflicts.

Funding and Acknowledgements

The author gratefully acknowledges the Ministry of University and Research (MUR), Italy, for supporting his work through the Young Researchers-Seal of Excellence (SOE) grant funded by NextGenerationEU (NGEU) under the National Recovery and Resilience Plan (NRRP).

REFERENCES

[1] Sun Tzŭ, *The Art of War*. London: Luzac & Co., 1910.

[2] C. von Clausewitz, *On War*. Princeton: Princeton University Press, 1984.

[3] B. Schuurman, "Clausewitz and the 'New Wars' Scholars," *The US Army War College Quarterly: Parameters*, vol. 40, no. 1, pp. 89–100, 2010, doi: 10.55540/0031-1723.2515.

[4] M. Kaldor, "Elaborating the 'New War' Thesis," in *Re-thinking the Nature of War*, I. Duyvesteyn, J. Angstrom, Eds. New York: Frank Cass, 2005, pp. 210–224.

[5] L. Freedman, "War Evolves into the Fourth Generation: A Comment on Thomas X. Hammes," in *Global Insurgency and the Future of Armed Conflict: Debating Fourth-Generation Warfare*, T. Terriff, A. Karp, R. Karp, Eds. New York: Routledge, 2008, pp. 78–86.

[6] M. Evans, "Elegant Irrelevance Revisited: A Critique of Fourth Generation Warfare," in *Global Insurgency and the Future of Armed Conflict: Debating Fourth-Generation Warfare*, T. Terriff, A. Karp, R. Karp, Eds. New York: Routledge, 2008, pp. 67–74.

[7] M. Marsili, "The War on Cyberterrorism," *Democracy and Security*, vol. 15, no. 2, pp. 172–199, 2019, doi: 10.1080/17419166.2018.

[8] M. M. Marsili, "Hybrid Warfare: Above or Below the Threshold of Armed Conflict?," *HSZ-HDR*, vol. 150, no. 1–2, pp. 36–48, 2023, doi: 10.5281/zenodo.7557494.

[9] M. Marsili, "The Russian Influence Strategy in Its Contested Neighbourhood," in *The Russian Federation in Global Information Warfare. Influence Operations in Europe and Its Neighborhood*, H. Mölder, V. Sazonov, A. Chochia, T. Kerikmäe, Eds. Cham: Springer, 2021, pp. 149–172, doi: 10.1007/978-3-030-73955-3_8.

[10] C.S. Gray, "The Changing Nature of Warfare?," *Naval War College Review*, vol. 49, no. 2, pp. 7–22, 1996.

[11] M.L.R. Smith, "Strategy in the age of 'low-intensity' warfare: why Clausewitz is still more relevant than his critics," in *Re-thinking the Nature of War*, I. Duyvesteyn, J. Angstrom, Eds. New York: Frank Cass, 2005, pp. 28–64.

[12] M. van Creveld, *On Future War*. London: Brassey's, 1991.

[13] M. Marsili, "From Battlefield to Political Arena. Shifting the Clausewitzian Paradigm," *Political Reflection*, vol. 7, no. 2 (issue 27), pp. 19–25, 2021, doi: 10.5281/zenodo.4554695.

[14] U.S. Department of the Army, Field Manual 27-10, *The Law of Land Warfare. Washington*, DC: U.S. Department of the Army, 18 July 1956, as modified by Change No. 1, 15 July 1976.

[15] U.S. Department of the Air Force, *Air Force Pamphlet 110-31, International Law – The Conduct of Armed Conflict and Air Operations. Washington*, DC: U.S. Department of the Air Force, 1976.

[16] U.S. Navy, U.S. Marine Corps, U.S. Coast Guard, The Commander's Handbook on the Law of Naval Operations, NWP 1-14M/MCTP 11-10B/ COMDTPUB P5800.7A. Department of the Navy, Office of the Chief of Naval Operations and Headquarters, US Marine Corps, and Department of Homeland Security, U.S. Coast Guard, Edition March 2022.

[17] NATO (2023, Apr. 4). *NATO's response to hybrid threats.* [Online]. Available: https://www.nato.int/cps/en/natohq/topics_156338.htm. [Accessed: Apr. 7, 2023].

[18] Heads of State and Government. (2016, July 9). *Warsaw Summit Communiqué.* [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_133169.htm. [Accessed: Apr. 18, 2023].

[19] Heads of State and Government. (2021, June 14). Brussels *Summit Communiqué*. [Online]. Available: https://www.nato.int/cps/en/natohq/news_185000.htm. [Accessed: Apr. 18, 2023].

[20] U.S. Government Accountability Office. (2010, Sep. 10). *Hybrid Warfare*, GAO-10-1036R. [Online]. Available: https://www.gao.gov/products/gao-10-1036r. [Accessed: Apr. 17, 2023].

[21] A. Matuszczyk, *Creative Stratagems: Creative and Systems Thinking in Handling Social Conflict*. Kibworth: Modern Society Publishing, 2012.

[22] M.M. Marsili, "Propaganda and International Relations: An Outlook in Wartime," *ArtCiencia.com*, no. 19, pp. 1–26, 2015, doi: 10.25770/artc.11095.

[23] Joint Chiefs of Staff (JCS). JP 3-13, *Information Operations (Joint Publication 3-13)*, Incorporating Change 1, 20 November 2014. Washington, DC: JCS, 27 November 2012.

[24] U.S. Training and Doctrine Command (TRADOC). (2018, Dec. 6). *The U.S. Army in Multi-Domain Operations 2028.* [Online]. Available: https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf. [Accessed: Apr. 20, 2023].

[25] U.S. Marine Corps, *Information*, MCDP 8. Washington, DC: Department of the Navy, 2022.

[26] M. Marsili, "COVID-19 Infodemic: Fake News, Real Censorship. Information and Freedom of Expression in Time of Coronavirus," *Europea*, vol. 10, no. 2, pp. 147–170, 2020, doi: 10.4399/97888255402468.

[27] K. Cao, S. Glaister, A. Pena, D. Rhee, W. Rong, A. Rovalino, S. Bishop, R. Khanna, J. Singh Saini. (2021, May 20). *Countering cognitive warfare: awareness and resilience*, NATO Review. [Online]. Available: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html. [Accessed: Apr. 8, 2023].

[28] R. Núñez, M. Allen, R. Gao et al., "What happened to cognitive science?," *Nat Hum Behav*, vol. 3, pp. 782–791, 2019, doi: 10.1038/s41562-019-0626-2.

[29] P. Thagard. (1996). *Cognitive Science*. [Online]. Available: https://plato.stanford.edu/archives/spr2023/entries/cognitive-science/. [Accessed: July 4, 2023].

[30] A.L. Samuel, "Some Studies in Machine Learning Using the Game of Checkers," *IBM J. Res. Dev.*, vol. 3, no. 3, 1959, pp. 210–229, doi: 10.1147/rd.33.0210.

[31] A.M. Turing, "Computing Machinery and Intelligence," *Mind*, vol. 59, no. 236, pp. 433–460, 1959, doi: 10.1093/mind/LIX.236.433.

[32] Joint Chiefs of Staff (JCS). *JP 3-04, Information in Joint Operations (Joint Publication 3-04)*. Washington, DC: JCS, 2022.

[33] NATO ACT. (2022, Mar. 29). *The Alliance's Warfare Development Agenda: Achieving a 20-year Transformation*. [Online]. Available: https://www.act.nato.int/articles/wda-achieving-20-year-transformation. [Accessed: Apr. 16, 2023].

[34] NATO ACT. NATO *Warfighting Capstone Concept (NWCC)*. [Online]. Available: https://www.act.nato.int/nwcc. [Accessed: Apr. 16, 2023].

[35] NATO. (2022, Oct. 3). *Military Committee*. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_49633.htm. [Accessed: Apr. 20, 2023].

[36] M. Marsili, "Shaping the Holistic Concept of Multi-Domain in a Legal Vacuum. A Tricky Issue". *II Encontro Anual da Investigação & Desenvolvimento em Ciências Militares (EAI&DCM2019)*, 2019, doi: 10.5281/zenodo.3473959.

[37] HQ Supreme Allied Commander Transformation Strategic Plans and Policy Directorate. (2022, Sep. 29). *Cognitive Warfare (CW) Initial Validation Planning Workshop 27–28 October 2022*, ACT/SPP/CNDV/TT-4563/SER:NU.

[38] NATO STO. HFM-361 on Mitigating and responding to cognitive warfare. [Online]. Available: https://events.sto.nato.int/index.php/event-summary/event/17-symposium/507-hfm-361-on-mitigating-and-responding-to-cognitive-warfare. [Accessed: July 4, 2023].

[39] N. Stephenson, *Snow Crash*. New York: Bantam Books, 1992.

[40] S. Mystakidis, "Metaverse," *Encyclopedia*, vol. 2 no. 1, pp. 486–497, 2022, doi: 10.3390/encyclopedia2010031.

[41] Gartner. *Internet Of Things (iot)*. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/internet-of-things. [Accessed: July 4, 2023].

[42] Joint Chiefs of Staff (JCS), JP 3-0, *Joint Operations (Joint Publication 3-0)*. Washington, DC: JCS, 2022.

[43] Istituto di ricerca e analisi della difesa - IRAD (2023, May 24). *Avviso Esito Pubblico Ricerche 2023*. [Online]. Available: https://irad.difesa.it/Comunicazione/Dettaglio/17. [Accessed: July 4, 2023].

[44] M. Marsili, "Epidermal Systems and Virtual Reality: Emerging Disruptive Technology for Military Applications," *Key Eng. Mater.*, vol. 839, pp. 93–101, 2021, doi: 10.4028/www.scientific.net/KEM.893.93.