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

Marco Marsili

Cà Foscari University of Venice

Ca'Foscari University of Venice
Department of Philosophy and Cultural Heritage

Assumptions from classic treatises on political-military analysis and strategy

- "In warfare, there are no constant conditions" (Sun Tzŭ, *The Art of War,* § 32).
- War is "an act of force to compel our enemy to do our will…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" (Clausewitz, *On War).*
- "Politics is the continuation of war by other means" (M. Foucault, *Society Must Be Defended: Lectures at the Collège de France*, 1975-1976, trans. David Macey, 2003).

An umbrela concept for comprehensive warfare

- 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.
- Hybrid threats include non-kinetic and non-lethal actions that arise in digital, cybernetic, and virtual environments and materialize in the real world.
- Although vague, hybrid activities include cyberwarfare, information warfare, and the emerging and evolving concept of cognitive warfare (CogWar) which appears from their intersection.
- All these terms/concepts are fluid, nebulous, and lack an undisputed legal definition.
- Therefore, is questioned which *ruse de guerre* is legitimate or not.

https://mpcoe.org/event,187,mp-hybrid-warfare-workshop-13-15-october-2020-save-the-date

International Humanitarian Law

Law of War

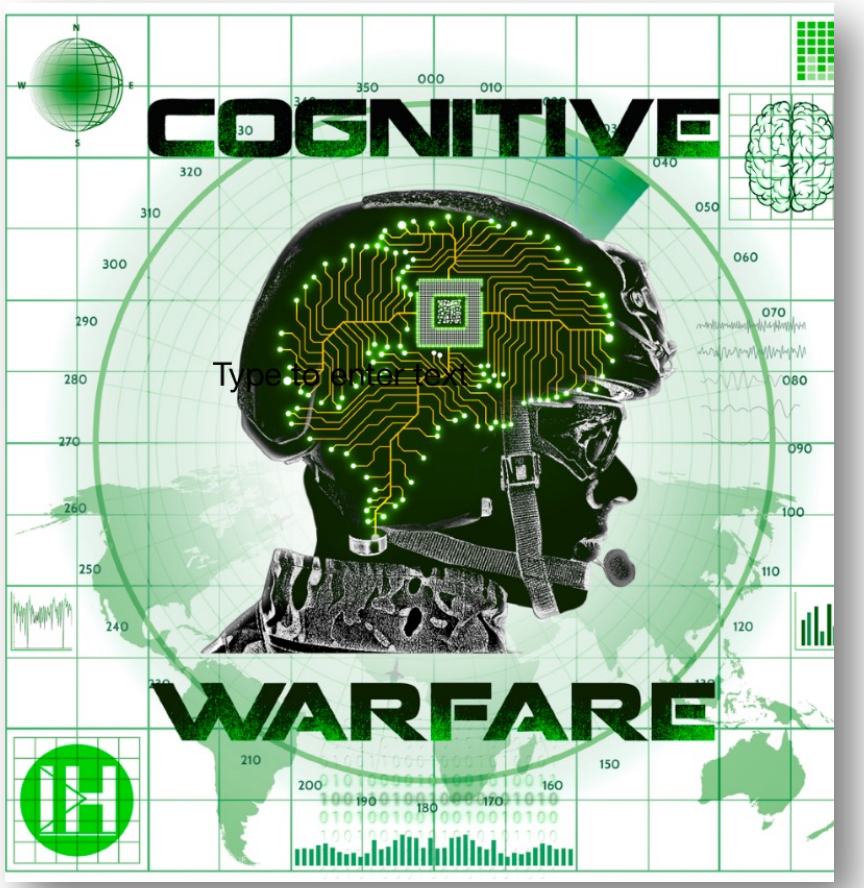
Despite much, too much rhetoric on the extension of the term “war” or “warfare”, “armed conflict” (the wording is crucial) is regulated by the legal framework provided by the Geneva Conventions, which define the perimeter of international humanitarian law (IHL), i.e., the “law of war” — IHL regulates the conditions for initiating war (*ius ad bellum*) and the conduct of waging parties (*ius in bello*).

- 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 IHL, so long as they do not involve treachery or perfidy.
- The European Union's definition of hybrid activities ranges from cyber-attacks through disinformation.
- NATO encompasses propaganda, deception, sabotage and other non-military tactics among hybrid methods of warfare.
- The U.S. Department of Defense has not officially provided a definition and has no plans to do so because hybrid 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.

Warfare or what?

- Any use of the term “warfare”, which does not involve the use of lethal weapons, is inappropriate—lexicon and terms are relevant.
- Due to overuse and misuse, “warfare” is now also applied to military operations other than war (MOOTW) that fall below the threshold of armed conflict.
- 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.
- “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” (M. L. R. Smith, 2005).

Weaponization of information



- Although there is no common definition of hybrid warfare, the inclusion of propaganda, information and influence operations, deception and psychological operations is widely accepted.
- Information warfare includes a set of techniques and technologies intertwined between the real and the virtual operational domains: electronic warfare, electromagnetic spectrum operation, cyberspace operations, propaganda, psychological operations (now better known as military information support operations), information operations (also known as influence operations), strategic communications, military deception, computer network operations, operations security, perception management, public information, public diplomacy.
- Cognitive warfare is a form of propaganda spread through manipulated media or social media for political or military purposes and aimed to support and install biased and conflicting narratives in target individuals to make them behave accordingly by fogging their minds. Therefore, what concerns most about the cognitive effects in peacetime, is not the impact on the battlefield, but the political and social consequences.
- The fact that most cognitive activities occur primarily in the virtual domain does not mean that they have no effects in the real world.
- A CogWar exploratory concept, developed by a NATO ACT team of experts will be approval by the Supreme Allied Command Transformation (SACT) in 2023.

Breaking barriers

- The virtual and physical worlds are becoming increasingly interconnected, interdependent, and indistinguishable from one another.
- The human-machine interaction is a fundamental component of CogWar and plays a central and crucial role due to the way our perception and judgment are affected, thus making it an unprecedented challenge.
- 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.
- Even if virtual actions cannot as-such replace physical warfare, it does not mean that they have no negative impact in the real world.

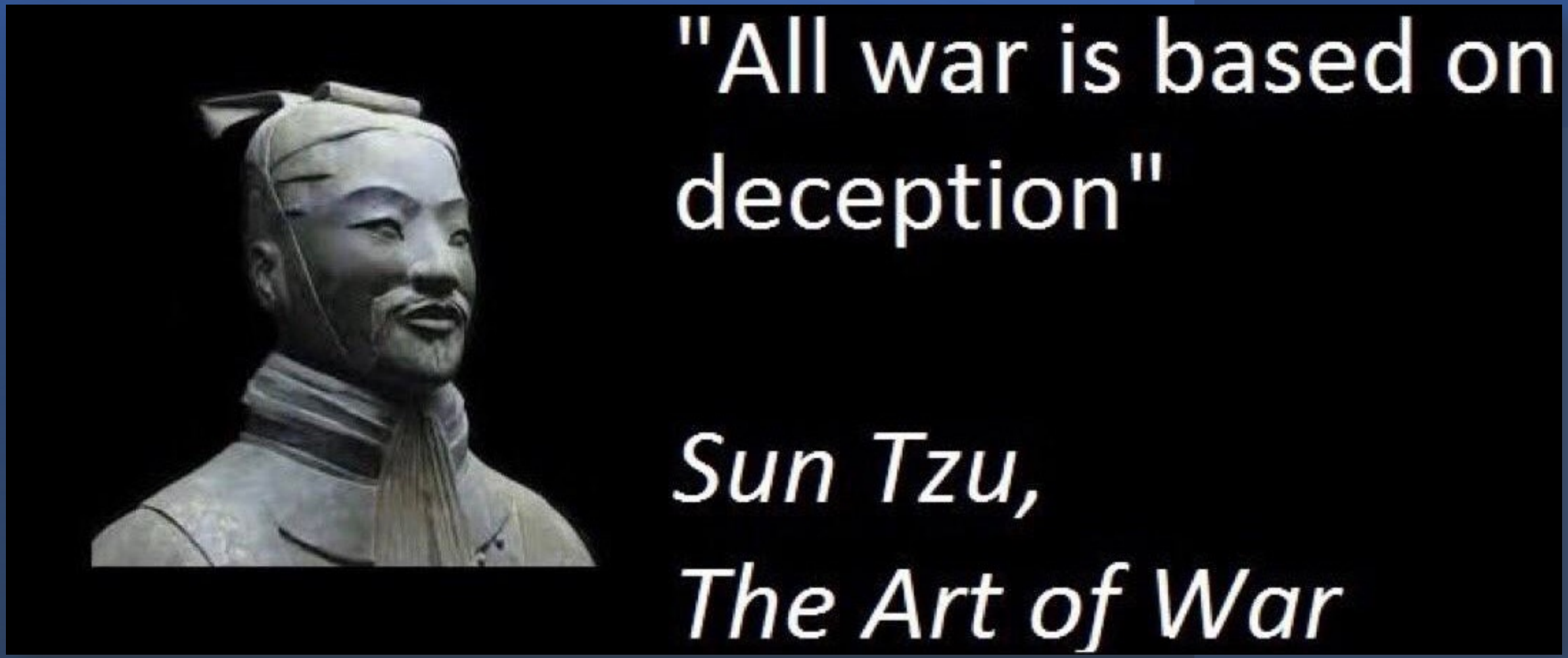
”The Metaverse has now become a place where you can get killed”.

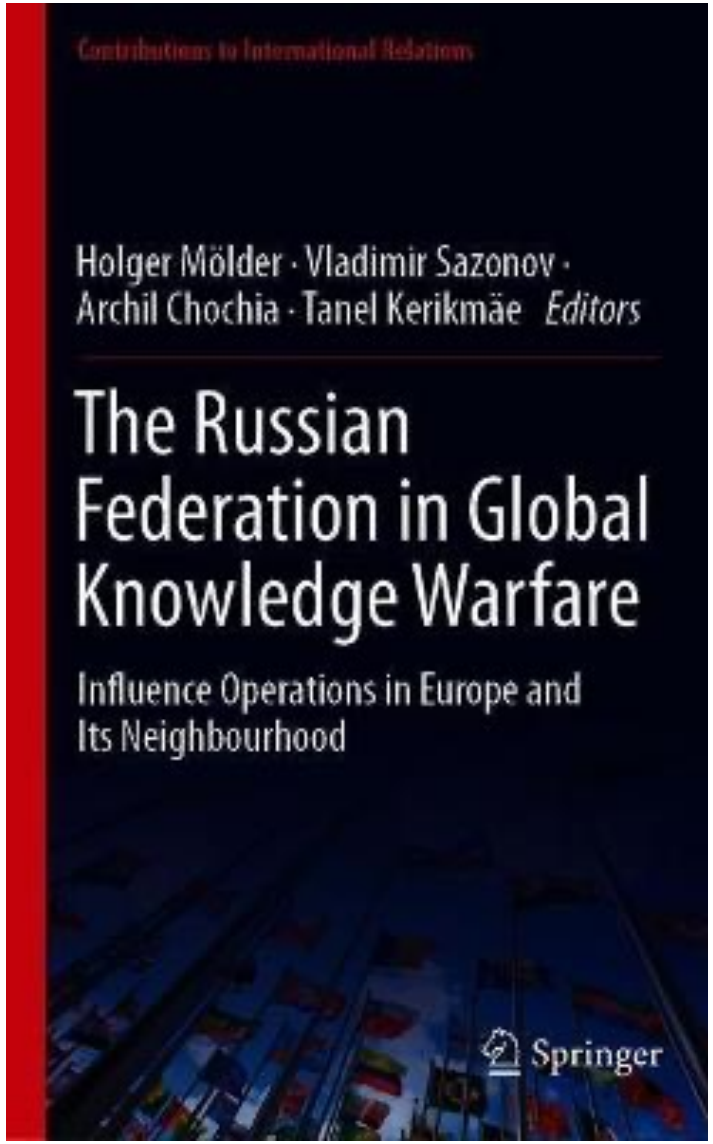
“The people who go into the Metaverse…understand that information is power”.

Neal Stephenson, *Snow Crash* (1992).

Findings and conclusions

- Emerging and evolving threats come from the virtual world.
- Even if it is nothing new, what is new is the speed, scale and intensity of unconventional attacks, facilitated by rapid technological change and global interconnectivity.
- The metaverse and war may sound completely unrelated but are intertwined more than it appears—the metaverse breaks the barrier between the virtual and the real word.
- While the rapid technological advance 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.
- It is more than likely that such threats will increase in the future until they become prevalent over conventional (kinetic) means of warfare.
- Conflicts must remain in the digital environment, where they are lawful, and must not turn into armed conflicts.
- Governments and military organizations should strive to reach a legally binding and undisputed definition of threats coming from the digital world, avoiding branding them as "warfare" not to trigger any conventional response.


"All war is based on deception"
Sun Tzu,
The Art of War



Further reading by the author suggested on this topic

- 2023 – Military Emerging Disruptive Technologies: Compliance with International Law and Ethical Standards. In Ignas Kalpokas (ed.), *Intelligent and Autonomous: Emergent Digital Technologies and the Challenges of Disinformation, Security, and Regulation*, Brill (Series Value Inquiry Book - VIBS). TBP 26. Oct. 2023.
- 2023 – Hybrid Warfare: Above or Below the Threshold of Armed Conflict?, *Honvédségi Szemle – Hungarian Defence Review*, *150*(1–2), 36-48. doi: 10.5281/zenodo.7557494.
- 2021 – The Russian Influence Strategy in its Contested Neighbourhood. In Holger Mölder, Vladimir Sazonov, Archil Chochia and Tanel Kerikmäe (eds.), *The Russian Federation in Global Information Warfare. Influence Operations in Europe and Its Neighborhood*, 149-172. Cham: Springer (series Contributions to International Relations - CIR). https://doi.org/10.1007/978-3-030-73955-3_8.
- 2021 – Epidermal Systems and Virtual Reality: Emerging Disruptive Technology for Military Applications, *Key Engineering Materials, 839,* 93-101. https://doi.org/10.4028/www.scientific.net/KEM.893.93.
- 2019 – The War on Cyberterrorism, *Democracy and Security*, *15*(2), 172-199. https://doi.org/10.1080/17419166.2018.1496826.

Full paper to be published in *Applied Cybersecurity & Internet Governance* (ACIG), vol. 2, no. 1, June 2023. ISSN: 2956-3119 | E-ISSN: 2956-4395. https://acigjournal.com/

Ca' Foscari
University
of Venice
Department of Philosophy
and Cultural Heritage

"That's all Folks!"

Thanks for your attention

La commedia è finita!

Funded by the European Union
NextGenerationEU

This study was supported by the Ministry of University and Research (MUR), Italy, through the Young Researchers-Seal of Excellence (SOE) grant funded by NextGenerationEU (NGEU) under the National Recovery and Resilience Plan (NRRP).

- Skype: marcomarsili
- Twitter: @marcomarsili1
- Telegram: @MarcoMarsili
- Facebook :@marco.marsili1
- E-mail: info@marcomarsili.it
- Slack: marco-marsili.slack.com
- Site: https://www.marcomarsili.it
- ORCiD: 0000-0003-1848-9775

DOI: https://doi.org/10.5281/zenodo.7879303

Ca' Foscari University of Venice
Department of Philosophy and Cultural Heritage
CATÓLICA CIEP · CENTRO DE INVESTIGAÇÃO DO INSTITUTO DE ESTUDOS POLÍTICOS
cei_iscte Centro de Estudos Internacionais
CINAMIL MILITARY ACADEMY RESEARCH CENTER
IUM Instituto Universitário Militar
cesran international CENTRE FOR STRATEGIC RESEARCH AND ANALYSIS - CESRAN

Dipartimento di Filosofia e Beni Culturali, Università Cà Foscari di Veenzia (DFBC-UNIVE); Centro de Investigação e Desenvolvimento do Instituto Universitário Militar (CIDIUM); Centro de Investigação, Desenvolvimento e Inovação da Academia Militar (CINAMIL); Centro de Investigação do Instituto de Estudos Políticos da Universidade Católica Portuguesa (CIEP-UCP); Centro de Estudos Internacionais (CEI-IUL) do Instituto Universitário de Lisboa (ISCTE-IUL); Centre for Strategic Research and Analysis (CESRAN)