Name: Ms. Alexandra Borgeaud dit Avocat

Citizenship: Switzerland

Email address : Alexandra.borgeaudditavocat@geneva-academy.ch

Affiliation: Center for Security Analyses and Prevention (CBAP), Prague

Ideathon Hack the Mind
Cognitive Warfare: Battlefield of Tomorrow

Word Count – Essay, excluding bibliography and abstract (150 words): **1,785**

Abstract

In a current geopolitical climate characterised by the return to 'bloc thinking', and the

perception that military strength equals a higher degree of security, modern technologies and revolutionary developments in neuroscience add yet another layer of complexity in an already challenging state of affairs. The concept of cognitive warfare and its disruptive potential have gained growing attention over the past couple years. This essay will address how new technologies and better understanding of human heuristics via neuroscience can influence the future of armed conflicts, before unpacking the concept itself and analyse what distinguishes it from information warfare. Finally, the fourth part will explore possible solutions to tackle the technical, legal, ethical, and political issues, the ultimate aim being to provide academics and policy makers with conceptual clarity and potential governance solutions. As shall be seen, the emergence of a new concept does not mean that 'old' solutions should be forgotten.

• Introduction

"Power is in tearing human minds to pieces and putting together again in new shapes of your own choosing."

The past couple years have witnessed a growing interest, from both civil and military communities, for Cognitive Warfare. However, is this concept truly new? If so, what distinguishes it from Information or Cyber Warfare? What role do modern technologies and neuroscience advancements play in such a distinction? Most importantly, what could be the consequences for the international security environment and the future of conflict? This short essay will attempt to answer these questions, first by providing an overview of the possible military applications of new technologies and breakthroughs in neuroscience, before addressing how these could influence the human brain and mind and the potential impact for future armed conflicts. Part III will in turn unpack the concept of cognitive warfare and analyse, building on the recent literature from military and intelligence organisations, what distinguishes it from information warfare. Finally, the fourth part will explore possible solutions to tackle the technical, legal, ethical, and political issues raised by the concept of cognitive warfare.

• New Technologies, Neuroscience, and the Future of Conflict

In a current geopolitical climate characterised by the return to 'bloc thinking', and the perception that military strength equals a higher degree of security, modern technologies and revolutionary developments in neuroscience add yet another layer of complexity in an already challenging state of affairs, and have gained a lot of attention over the past decade.

On the one hand, the growing consensus is that "today's technological advances are deemed disruptive not only in market terms but also in the sense that they are "provok[ing] disruptions of legal and regulatory orders", having the potential to "disturb the deep values upon which the legitimacy of existing social orders rests and on which accepted legal and regulatory frameworks draw." This is especially true in

the military field, as the world is witnessing an "ever-closer fusion of computers and warfare at a time of unprecedented soul-searching about democracy itself." According the NATO Science and Technology Organization, "over the next 20 years, four overarching characteristics can be expected to define many key advanced military technologies: 1. Intelligent, by exploiting integrated AI, knowledge-focused analytic capabilities, as well as AI – human teaming; 2. Interconnected, by exploiting the network of virtual and physical domains; 3. Distributed; and 4. Digital, by blending human, physical and information domains to support novel disruptive effects." Beyond the physical and virtual domains, the present essay focuses on the cognitive space, where hacking tools can be used for political purposes to distort images, produce, and disseminate fake news through tactics such as targeted data collection, content creation, and false amplification. A specific example of content creation is a DeepFake, a recent machine learning-based technology, built around convolutional neural networks, used to produce or alter video/image content so that it presents something that did not, in fact, occur.

On the other hand, advances in neuroscience and behavioural economics have allowed for enormous progress in understanding how the brain works and the underlying mechanisms of heuristics and cognitive biases. Defence departments and intelligence agencies increasingly rely on brain research to extract tools and methods that could be employed as weapons "to directly affect cognitive and physical abilities of both friendly forces (i.e.- optimization effects) and adversaries (i.e.- denigration effects)."

One could easily imagine the consequences of such tools, especially when combining both technological and heuristic dimensions, to a military context. By creating and disseminating DeepFakes, for example, a growing number of actors can take advantage of people's inherent and numerous cognitive biases, as well as cognitive vulnerability— "a premise that the audience is already predisposed to accept without too much critical thinking because it makes a fundamental emotional appeal to existing fears or anxieties," to manipulate a given narrative. Indeed, by assessing, accessing, and targeting neural structure and cognitive, emotional, and behavioural functions of both individuals and groups, they could, *inter alia*, be used by state and non-state actors alike to recruit new members into their armed forces, to augment warfighters' cognitive performance, to deceive the enemy by claiming a crucial

victory, or to manipulate public opinion into supporting a protracted conflict. By offering the opportunity to inflict a defeat without using physical force, "the control over knowledge, beliefs, and ideas are increasingly regarded as a complement to control over tangible resources such as military forces, raw materials, and economic productive capability."

• Cognitive Warfare: A Proposed Definition

However, is the concept of cognitive warfare really new? If so, what distinguishes it from information or cyber warfare? Giuseppe defines it as "the capacity to use knowledge for the purpose of conflict." At this point, a first caveat should be introduced. Indeed, and for reasons further detailed in the next section, one should be wary of using the term 'warfare' to refer to disinformation or instances manipulation of public discourse in peacetime.

Focusing then on wartime, does cognitive warfare represent a new concept? After all, Sun Tzu was, in its seminal work *The Art of War* (Vth century BC), already referring to such methods by stating that "the highest form of warfare is to out-think the enemy." While disinformation and propaganda have indeed played a critical role in warfare over the centuries, the 1990s saw the emergence of the term 'information operations and warfare' to describe "the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent," to be placed in a new landscape of "increasingly digitised and networked infrastructure underpinning contemporary warfare." Nevertheless, information operations remained largely accessory to traditional kinetic efforts in the battlefield. The advent of 'hyper-connectivity' at the end of the 2000s marked a turning point, an unprecedented democratisation not only of information, but of various tools and platforms, enabling state and non-state actors alike to influence, anonymously if needed, an ever-larger global audience. Cognitive warfare thus appears as information warfare "with something added," namely the ability to combine the understanding of subconscious, emotional, and behavioural functions of individuals with technology to steer human behaviour and beliefs into the desired direction.

• Possible Solutions at the Technical, Legal, Ethical, and Political Level

The previous section has established that cognitive warfare might indeed constitute a new phenomenon. Should the existing legal and governance frameworks be updated as a result?

At the technical level, innovative tools are urgently needed to detect DeepFakes and fake news in general. AI-enabled fact-checkers or digital forensic software could constitute possible solutions.

At the legal level, the use the term 'warfare' when referring to a situation of conflict has major implications for two bodies of international law: *jus ad bellum*, or the rules governing the use of force, and *jus in bello*, or international humanitarian law (IHL). With regard to IHL, ruses of war, or "acts which are intended to mislead an adversary or to induce him to act recklessly," "and the employment of methods necessary to obtain information about the enemy and the country are considered permissible." IHL however prohibits perfidy – "acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under" IHL. There are no a priori reasons why these rules could not apply to cognitive warfare. With regard to *jus ad bellum*, could DeepFakes or fake news ever amount to a "threat to the peace, breach of the peace, or act of aggression" under Article 39 of the UN Charter, thus triggering the right to self-defence of the targeted state (Article 51)? The Tallinn Manual on the International Law Applicable to Cyber Warfare could provide a useful starting point and could be further developed to take into account technological developments.

It seems however that the international community should first and foremost focus on the ethical dimension of cognitive warfare, as well as political and diplomatic solutions, as cognitive 'weapons' primarily endanger trust in an already polarised geopolitical climate and raise crucial neuroethics issues. The adoption of confidence and security-building measures, continued information sharing and dialogue in multilateral fora such as the UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security or

the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security would constitute positive first steps. The adoption of a multi-stakeholder approach to governance, bringing together experts working in areas such as cognitive science, computer science, ethics, public policy, and psychology, also constitutes a *sine qua non* condition to tackle the issues raised by the emergence of cognitive warfare.

• Conclusion

This short essay aimed at providing both academics and policy makers with conceptual clarity and potential governance solutions. While cognitive warfare might indeed constitute a new phenomenon to be dealt with, traditional governance solutions – solid legal frameworks, cooperation, information sharing, and trust building – might be still worth considering. Such solutions should be explored and implemented long before an actual conflict arises.

• Bibliography

Bienvenue, E., Rogers, Z. & Troath, S., 'Cognitive Warfare', The COVE, 19 September 2018

Dunn Cavelty, M., 'Cyber-security' in Collins, A. (ed.) *Contemporary Security Studies* (Oxford University Press: Oxfrord, 2015)

Giordano, J., 'Is neuroscience the future of warfare?', Defence iQ, 17 April 2019.

Giuseppe, G., 'The cognitive warfare: Aspects of new strategic thinking', Modern Diplomacy, 5 March 2018.

Kasapoglu, C. & Kirdemir, B., 'Artificial Intelligence and the Future of Conflict', in Valasek, T. (ed.), New Perspectives on Shared Security: NATO's Next 70 Years (Carnegie Europe, 2019), pp. 35 – 36.

Kavanagh, C., 'New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?', Paper, Carnegie Endowment for International Peace, 28 August 2019, p. 2.

Orwell, G., *1984* (Penguin Classics, London: 2013)

Rosner, Y., & Siman-Tov, D.). Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion, 8 March 2018

Libicki, M. L., 'The Convergence of Information Warfare', Strategic Studies Quarterly, Spring 2017

Trapp, J., & Tzu, S., *The Art of War* (New York: Chartwell Books, 2012)

Tversky, A.; Kahneman, D., "Judgment under Uncertainty: Heuristics and Biases", *Science* Vol. 185, Issue 4157, pp. 1124–1131, 1974

Valasek, T. (ed.), *New Perspectives on Shared Security: NATO's Next 70 Years* (Carnegie Europe, 2019).

Waltzman, R., "The Weaponization of Information: The Need for Cognitive Security," RAND Corporation, April 27, 2017

Reports

NATO StratCom Centre of Excellence, 'Digital Hydra: Security Implications of False Information Online', Report, November 2017

NATO Science & Technology Organization, 'Science & Technology Trends 2020-2040: Exploring the S&T Edge', Report, March 2020

Websites

RAND Corporation, "Information Operations," Website. https://www.rand.org/topics/information-operations.html (accessed on 24 September 2020)