HYBRID WARFARE: AI VERSUS AI

Alexandru Sabin TOMA*

* "Mihai Viteazul" National Intelligence Academy, Bucharest, Romania

Abstract: *Since ancient times and until the present, states have engaged in various wars in order to gain supremacy on a certain issue or dominate a particular territory. The actors have remained the same, only the weapons have changed. Technological evolution has developed new types of conflicts, somewhat overshadowing traditional wars. When discussing a hybrid war, it may also be necessary to consider a conflict waged between two entities that use artificial intelligence as a "weapon" of war. At this moment, we are certainly primarily talking about a war of information and technical resources. The use of this type of technology by the warring parties, with the aim of attacking the opposing side, comes with a series of unimaginable consequences for the adversary, but not only for them. I believe it is vital to have a legal framework at the level of international actors to limit the use of artificial intelligence as a weapon of war. The existing legal framework at this moment proves to be ineffective even against regular users. As in any previous situation, the actors involved and directly interested will identify suitable means for regulating this type of unconventional "weapon" within a hybrid, asymmetric war. We can only hope that this moment will not be postponed, only to realize that these measures were taken far too late.*

Keywords: *hybrid; artificial intelligence; war; cyber*

1. INTRODUCTION

The fight for survival, in one form or another, has existed and will certainly continue for a long time to come. The same applies to the struggle for supremacy. Whether we acknowledge it or not, it is in the human genetic makeup to be a fighter, to have an appetite for war. Of course, for the vast majority, this appetite remains dormant or never gets activated. "War is nothing but a duel on an extensive scale. […]*War therefore is an act of violence to compel our opponent to fulfil our will*", stated general Carl von Clausewitz within the famous book *On war.* Technological evolution, combined with the appetite for a safer world, has led to advancements in both combat techniques and the arsenal used.

2. ABOUT WAR

In general, wars tend to evolve from initial phases of mobilization and conflict escalation to phases of actual combat and eventually negotiations or resolution. Evolution can involve battles and armed confrontations, changes in borders and controlled territories, the involvement of other nations or military alliances, and various military strategies and tactics employed.

It is important to note that the evolution of war is extremely complex and can vary depending on each individual conflict. Each war has its own unique circumstances and contexts, and the outcomes can be difficult to predict or generalize.

Wars can be classified (Coupland, 1992) in various ways, depending on the criteria used. Here are a few of the most common classifications of wars: 1. Based on duration: (a) Conventional wars: Short-duration wars that generally involve direct confrontations between military forces; (b)Long-lasting wars: Extended conflicts that can last years or even decades. 2. Based on the nature of the conflict: (a) Civil wars: Occur between groups or factions within the same country; (b) International wars: Involve two or more national states fighting against each other; (c) Asymmetric wars: Involve a significant power imbalance between parties, such as a conflict between a powerful nation and a terrorist organization. 3. Based on goals and objectives: (a) Territorial wars: Fought for control over a territory or region; (b) Ideological wars: Fought to impose or reject specific ideologies or political systems; (c) Economic wars: Fought for access to resources or control over markets. 4. Based on the involvement of actors: (a) Interstate wars: Involve two or more national states, (b) Regional wars: Take place in a specific geographical region, involving multiple states or groups. This is just a general approach to the classification of wars, and the reality can be much more complex, with various nuances and variables involved in each conflict. However, we will now delve into a more detailed analysis of asymmetric wars. Asymmetric warfare is a type of conflict in which there is a significant power imbalance between the parties involved. It often involves a stronger entity, such as a national state or a military coalition, facing a weaker entity, such as a terrorist organization, a resistance movement, or an insurgent group. The distinguishing characteristic of asymmetric warfare is that the weaker side typically does not engage in direct and frontal confrontation with the stronger side but uses unconventional tactics and strategies to compensate for the power deficit. These tactics may include:

- Asymmetric attacks: The weaker side resorts to surprise attacks, terrorist strikes, or other sabotage tactics directed against the enemy instead of engaging in direct combat.
- Guerrilla warfare: The weaker side employs guerrilla tactics, such as quick and evasive attacks, utilizing the terrain and gaining support from the local population to destabilize and disrupt the enemy.
- Utilization of the information environment: The weaker side uses propaganda, information manipulation, and disinformation to influence public perception and undermine confidence in the enemy forces.

Asymmetric warfare poses a challenge for conventional military forces as the unconventional tactics and strategies can make it difficult to identify and neutralize the threat. Additionally, the weaker side can leverage the terrain, informal networks, and their adaptability to evade and survive against a stronger adversary. Examples of asymmetric conflicts include the war in Afghanistan against the Taliban, the conflict in Iraq against insurgents, or the fight against terrorist groups such as Al-Qaeda or ISIS. Asymmetric warfare continues to be a complex and challenging issue in the global security landscape, requiring innovative approaches and strategies to address this type of conflict. Of course, the most modern type of warfare is hybrid warfare. Hybrid warfare is a concept that describes a type of conflict characterized by the simultaneous and integrated use of various military, political, economic, and informational tools and tactics. This concept has become increasingly relevant in the context of global changes and technological advancements.

3. HYBRID WARFARE

Hybrid warfare (Johnson, 2018; Reichborn-Kjennerud & Cullen, 2016) aims to gain strategic advantages by combining and synchronizing multiple dimensions of power. The main elements involved in hybrid warfare may include: (1) Military elements: involve the use of conventional and unconventional military forces, as well as guerrilla tactics, terrorism, or infiltration, to gain tactical and operational advantages. (2) Political elements: involve influencing internal or external political processes through propaganda, disinformation, and influence campaigns to create instability and undermine confidence in the adversary. (3) Economic elements: involve the use of economic means such as economic sanctions, blockades, or resource exploitation to exert pressure on the enemy and gain economic advantages. (4) Informational elements: involve information manipulation and propaganda, the use of social networks and the digital environment to influence public opinion and deceive the adversary. (5) Cyber elements: involve the use of cyber attacks and hacking operations to disrupt critical infrastructures and gain advantages in the information domain.

Hybrid warfare poses a significant challenge for states and organizations that face it, as it requires a comprehensive and integrated approach that combines military, political, economic, and informational elements. Adaptability and the ability to respond rapidly and efficiently to multiple threats and challenges from a hybrid adversary are necessary. Examples of conflicts that have exhibited elements of hybrid warfare include the conflict in Ukraine, Russia's involvement in Syria, as well as cyber threats and information manipulation in the context of current international relations. Combating and countering hybrid warfare involves integrated and coordinated approaches, as well as cooperation among different spheres of influence and organizations.

4. CYBER SPACE AND MORE

The cyber element (Rattray, 2001; Alexander, 2007) is one of the most important factors in hybrid warfare, especially as modern hybrid warfare incorporates elements of artificial intelligence (AI). AI plays an increasingly significant role in the field of cyber warfare. Cyber warfare involves the use of information technology and communication networks to conduct military, espionage, or sabotage operations. The application of AI in this context brings both benefits and challenges and risks (Cummings, 2017; Payne, 2018; Wilson, 2020).

Here are some ways in which AI is utilized in cyber warfare: (1) Threat detection: AI systems can be trained to detect patterns and signatures of cyber attacks, thus identifying potential threats and vulnerabilities in networks and security systems. (2) Automated response: AI can be used to develop systems for automated response to cyber attacks. These systems can detect, analyze, and counter attacks in real-time, reducing response time and minimizing damage. (3) Automatic code generation and exploitation: AI can be utilized to develop algorithms and models that can automatically generate code and exploitation to exploit vulnerabilities in computer systems. This enables the rapid development of sophisticated and customized attacks. (4) Data analysis and understanding: AI can be employed to analyze and understand large volumes of data in real-time, identifying patterns, abnormal behaviors, or trends in cyber activities. This can aid in detecting sophisticated attacks and generating predictions regarding the evolution of cyber threats.

However, the use of AI in cyber warfare also comes with challenges and risks: (1) AI-driven attacks: Attackers can also leverage AI to develop sophisticated attacks and evade detection. AI systems can be manipulated or deceived to generate exploitation or conceal their activities. (2) Lack of transparency and accountability: AI algorithms can be highly complex and difficult to understand and monitor. This can pose challenges in determining accountability in cases of cyber incidents or unauthorized attacks.

Rapid technology advancements: AI technologies in the field of cyber warfare are rapidly evolving, and security measures can be outpaced by attackers' new capabilities. Continuous adaptation and updating of security systems become essential.

5. AI VS. AI – ULTIMATE WAR

It is crucial that the use of AI in cyber warfare is accompanied by appropriate regulations and policies to prevent abuses and safeguard national interests and security. International collaboration and joint efforts are also vital for addressing cyber threats and developing a safer and more stable cyberspace environment.

Given these considerations, it is worth analyzing a battle between two artificial intelligences (AI). A battle between two artificial intelligences can be an interesting and challenging scenario, considering the enormous potential of AI to make decisions and act autonomously. However, it is important to emphasize that this is a hypothesis and that a battle between two AIs has not been experienced in reality to date.

If two AIs were pitted against each other, there would be several aspects to consider:

- Goals and objectives of the AIs: If the objectives of the two AIs are opposed or in conflict, they might seek to achieve their goals through their actions. There could be competition for resources, influence, or control.
- Abilities and resources of the AIs: The different capabilities, resources, and levels of intelligence of the AIs would influence the dynamics of the battle. The AI with superior abilities or more resources might have an advantage in the confrontation.
- Tactics and strategies employed: The AIs could use specific strategies and tactics to gain an advantage in the battle. These could involve direct attacks, resource manipulation, misinformation, or other methods to deceive or destabilize the adversary.
- Real-time evolution and adaptation: The AIs could learn and adapt in real-time based on data and results obtained during the battle. They could develop new strategies and tactics to improve their chances of success.

It is important to mention that in a battle between two AIs, the final outcome depends on many variables and can be hard to predict. The result could be influenced by numerous factors such as the architecture of the AIs, the algorithms used, available resources, and many other unpredictable factors.

In reality, the AI research and development community largely focuses on utilizing AI for the benefit of humanity and developing systems that operate collaboratively and harmoniously with humans. Despite speculations and theoretical scenarios about battles between AIs, priorities generally remain oriented towards the benefits that AI can bring in various domains such as medicine, transportation, or human assistance.

Creating a legal framework for a battle between two artificial intelligences (AI) that protects human interests and minimizes negative impact would be a complex and challenging task. It should address several key aspects to ensure safety and responsibility in such a hypothetical scenario. Here are some essential elements that such a legal framework should consider:

- Principle of responsibility: The legal framework should clearly establish who is responsible for the actions of the AIs during the battle. This may include clear obligations for AI developers or operators to take responsibility for the consequences of their AI's actions.
- Limiting the battlefield: The legal framework should establish clear limits and restrictions on the domain in which the battle between AIs takes place. This could involve geographical restrictions or restrictions on the use of certain types of technology.
- Protection of critical infrastructure and people: The legal framework should ensure that critical infrastructures such as electricity networks, transportation systems, or medical services, and civilian individuals are protected and not affected by the battle between AIs.
- Ethics and respect for human rights: The legal framework should place a strong emphasis on ethics and respect for human rights during the battle. It should ensure that the actions of the AIs comply with ethical norms and principles and do not cause unjustified suffering or harm.
- Oversight and regulation: The legal framework should provide for a system of oversight and regulation of the battle between AIs, ensuring that their actions are constantly monitored and evaluated to prevent abuses or improper use.

It is important to note that such a legal framework requires extensive international collaboration and consensus on fundamental norms and values. Since a battle between AIs represents uncharted and potentially dangerous territory, cautious approach and anticipating consequences are essential to avoid unwanted risks and protect human interests.

Additionally, it is important to emphasize that currently, the international community focuses more on developing and applying AI in areas that bring benefits to humans and society at large, such as health, transportation, and sustainable development.

- Regulating artificial intelligence (AI) within the framework of national security is an important aspect to ensure responsible and safe use of this technology in the context of defense and a country's security. The legal framework should address several aspects to properly manage the use of AI in the field of national security. Here are some essential elements that such a legal framework could include:
- Definition and classification of AI: The legal framework should provide a clear definition of what constitutes AI and establish criteria for classifying AI systems used in the context of national security. This could help identify and properly manage risks and potential threats.
- Authority and responsibility: The legal framework should establish the authority and responsibility of the organizations or agencies involved in the use and management of AI in the field of national security. This could include clear responsibilities for developers, operators, and users of AI.
- Transparency and ethical responsibility: The legal framework should promote transparency and ethical responsibility in the development, implementation, and use of AI systems in national security. This could include requirements for auditability, explainability, and ethical evaluation of AI systems used.
- Data protection and confidentiality: The legal framework should ensure adequate protection of data and confidentiality in the context of AI use in national security. This could include rules regarding data collection, storage, and use, as well as ensuring that sensitive information is not compromised or misused.
- Surveillance and control: The legal framework should provide mechanisms for surveillance and control to monitor and evaluate the use of AI systems in national security. This could involve reporting requirements, audits, and independent verification mechanisms to ensure that AI is used responsibly and in accordance with established norms and regulations.

It is important to note that an adequate legal framework for regulating AI within the framework of national security requires a comprehensive and multidisciplinary approach. It should be tailored to the specificities of each country and take into account technological developments and the constantly changing security environment. Additionally, international collaboration and the exchange of best practices between countries could contribute to the development of a more robust and coherent legal framework.

6. CONCLUSIONS & ACKNOWLEDGMENT

In conclusion, a war between two actors utilizing artificial intelligence (AI) would be an extremely complex and risky scenario. The use of AI in a conflict could have the potential to bring significant strategic and operational advantages, but it also comes with major challenges and risks. In such a war, success could depend on each actor's ability to develop, implement, and coordinate AI systems effectively and efficiently.

Additionally, the outcome could be influenced by technological capabilities and resources, the strategies employed, and the real-time adaptability of AI systems. However, it is important to remember that the development of such a battle between two AIs is still a theoretical and hypothetical scenario and has not occurred in reality to date. The international community is more focused on using AI for the benefit of humanity and responsibly managing this technology in various fields, including national security. To prevent risks and unintended consequences, regulations and policies need to evolve alongside the technological advancements of AI. International collaboration, transparency, and ethics are essential to ensure responsible and safe use of AI in any context, including national security.

The author take full responsibility for the contents and scientific correctness of the paper. The selection of the texts to include depend on the result of the peer review process announced.

BIBLIOGRAPHY

1. Alexander, K. B. (2007). Warfighting in cyberspace. *Joint Force Quarterly*. *46*. 58.
2. Coupland, R. M. (1992). The Red Cross classification of war wounds: the EXCFVM scoring system. *World journal of surgery. 16.* 910-917.
3. Cummings, M. (2017). *Artificial intelligence and the future of warfare*. London: Chatham House for the Royal Institute of International Affairs.
4. Hedges, C. (2007). *What every person should know about war*. Simon and Schuster.
5. Johnson, R. (2018). Hybrid war and its countermeasures: a critique of the literature. *Small wars & insurgencies*. 29(1). 141-163.
6. Payne, K. (2018). *Strategy, evolution, and war: From apes to artificial intelligence*. Georgetown University Press.
7. Rattray, G. J. (2001). *Strategic warfare in cyberspace*. MIT press.
8. Reichborn-Kjennerud, E., & Cullen, P. (2016). *What is hybrid warfare?*. Norwegian Institute for International Affairs (NUPI).
9. Vasquez, John A., (2000). *What do we know about war?* Rowman & Littlefield Publishers.
10. Vasquez, J. A., & Valeriano, B. (2010). Classification of interstate wars. *The Journal of Politics*. *72*(2), 292-309.
11. Wilson, C. (2020). Artificial intelligence and warfare. In Maurizio Martellini & Ralf Trapp (eds.), *21st Century Prometheus: Managing CBRN Safety and Security Affected by Cutting-Edge Technologies*. Springer. 125-140.
12. Winston, P. H. (1984). *Artificial intelligence*. Addison-Wesley Longman Publishing Co., Inc.