ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ	ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ	ΤΜΗΜΑ ΝΟΜΙΚΗΣ
ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ “ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ”	

“AI-RELATED OFFENSIVE TECHNOLOGIES IN (CYBER) WARFARE AND NUCLEAR SECURITY”

Διπλωματική Εργασία

της

Αναστασίας (Τατιάνας) Κυτταρούδη

Ορεστιάδα, 09/2022

“AI-RELATED OFFENSIVE TECHNOLOGIES IN (CYBER) WARFARE AND NUCLEAR SECURITY”

Αναστασία (Τατιάνα) Κυτταρούδη

Πτυχίο Νομικής ΑΠΘ, 2020

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ “ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ”

Επιβλέπων Καθηγητής

Κωνσταντίνος Ψάννης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 3/11/2022

Απόστολος Χελιδόνης	Χρήστος Μαστροκώστας	Κωνσταντίνος Ψάννης

Αναστασία (Τατιάνα) Κυτταρούδη

Table of Contents

1. Abstract

Despite the world's generalized stability and peace maintenance, new technologies have affected every aspect of everyday life and practice, from transportation and communication to military capabilities. The new possibilities technologies such as Artificial Intelligence have introduced, along with the still unexplored aspects they entail, present an unprecedented multi-faceted reality in the military domain.

Weaponized offensive technologies are being developed in parallel with defensive capabilities, enabling a continuous race between the two and between the states that engage in Artificial Intelligence research and development. These novelties raise a new modus operandi on the conventional battlefield, but also in cyberspace, reshaping the very nature of war. Incorporating AI-enabled offensive technologies in (cyber) war is followed by unfamiliar benefits, challenges, legal and ethical questions.

In this paper, I will try to emphasize some of the most common AI-enabled technologies used in contemporary warfare, mention relevant case studies and some of the major states' policies and national developments, all while presenting both the benefits and the challenges of integrating cutting-edge technologies in the military sphere.

Key words: AI warfare, AI nuclear security, AI cyber warfare, AI war, AI offensive, combat AI

2. Introduction

The technological innovations of computers and relevant systems continue to amaze us and are being developed more rapidly than ever. Computer memory has increased, algorithms are more complex and, thus, execute more complicated tasks; all this progress has even come to a level where systems are able to teach themselves and improve on their own, with the help of Machine Learning, an application of Artificial Intelligence. Militaries across the world have realized the benefits that such advancements could offer and are already testing and using various AI technologies in their operations. We could not argue that the existing weaponized use within the military is as broad as the commercial use of AI, yet there are already some key countries, both in the field of research and practice, and these are the United States, China and Russia. The differentiating factor with this kind of use today is that AI alters the balance of power between nations, as new tools are being developed and used and new targets for offenses are being created, especially in cyberspace[1].

AI is a new criterium of strength, power and capabilities for states to perceive, rank and categorize other states as an ally or as a threat. This criterium, however, is not yet to be trusted, as the different level of AI development within a state will affect its judgement towards others. Taking into consideration that AI as a weaponized technology in the military is currently not explored and defined, especially in an internationally agreed way, it blurs the lines of objective judgement even more.

[1] Pavel Sharikov (2018) Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination, Bulletin of the Atomic Scientists, 74:6, 368-373, DOI: 10.1080/00963402.2018.1533185

This work will focus on the current tendencies, policies and major types of AI-backed weaponized technologies, as well as their implications for the nature of war, diplomatic relations and society. It does not constitute nor specialize in analyzing the technicalities of the technologies as they are, rather than providing insight on the theoretical impact of AI introduction to the military.

Warfare has changed in nature, but also expanded to new terrains, namely cyberspace. It can now be multi-faceted simultaneously and it can contain an enormous amount of contrasting data, that only AI can assist in sorting and analyzing at a speed that favors decision-making before the adversary. The aforementioned breakthroughs showcase that not only is it necessary to integrate state-of-the-art technologies and methods in military tasks and operations, but also to re-evaluate the nature and context of war itself.

The Pentagon itself came across a security paradox as per the use and rise of our dependency on digital technologies, where the latter offer us both powers and at a speed that humanity has never encountered before, yet at the same time these powers are the ones that render its users feeling more and more insecure[2].

This technological dominance will definitely alter balances, redistribute wealth, create new alliances and maybe tear old ones apart, as well as present the world with new types of threats.

3. Definitions

[2] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

Autonomy, in human-machine interaction and cooperation, is divided into three categories, useful to understand for the better understanding of the notions described in this thesis. The systems' tasks that are fully controlled by a person are called "*human-in-the-loop"*. Systems that can operate in a semi-autonomous way, thus completing tasks on their own, with humans however being in charge of reviewing functions or decisions by the systems and with the ability to intervene, are "*human-supervised"* systems. The third category is "*human-out-of-the-loop"* where, as the title indicates, the system operates autonomously, with humans not being able to intervene[3].

Escalation is "*an increase in the intensity or scope of conflict that crosses a threshold(s) considered significant by one or more of the participants*"[4].

The term **"cyber"** is used to explain everything that has to do from "*networks to hardware, software, automation, industrial controls, hacking, bullying, warfare... social media*"[5].

AI (Artificial Intelligence) is considered a "*generic term that washes over meaningful distinctions between its different manifestations*", something that

[3] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

[4] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23.), where Forrest E. Morgan, Karl P. Mueller et al., "Dangerous Thresholds: Managing Escalation in the 21st Century (Santa Monica, CA: Rand Cooperation, 2008), p. 8.

[5] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022]

creates "confusion, especially regarding claims about its revolutionary effects". More technically defined, though, "*AI consists of algorithms that form the basis of pattern recognition software. When combined with high-performance computing power, data scientists are able to probe and find meaning in massive data collections. AI also includes language processing, knowledge representation and inferential reasoning*". AI is divided into Narrow and General AI, with ***Narrow AI*** enabling "*discrete problem-solving tools designed to perform specific narrow tasks*", while ***General AI*** is all about "*technologies designed to mimic and recreate functions of the human brain*". Nowadays, more and more theoretical approaches and research have been focused on the so-called ***Artificial Superintelligence (ASI)***, a term first introduced by philosopher Nick Bostrom who defines it as "*intelligence which possesses cognition that significantly and consistently outstrips human cognition*"[6]. Nevertheless, ASI remains a theoretical concept, as we are still far from its practice in real life.

Narrow AI is the technology that allows the analysis of vast amounts of unprocessed data, a function extremely helpful in the military context and especially at times of crisis where quick action is called for[7].

Lethal Autonomous Weapons Systems (LAWS): With the term already indicating the severity of this technology, LAWS or, otherwise, "killer robots" is a term that does not enjoy international official adoption, yet it is generally defined as a system of weapons able to select and attack targets without any need

[6] Yen Koh, T., n.d. *Intelligent Machines vs. Human Intelligence*. [online] Ebsco.com. Available at: <https://www.ebsco.com/apps/landing-page/assets/POVRC_Intelligent_Machines_vs_Human_Intelligence.pdf> [Accessed 19 September 2022]

[7] MacDonald, N. and Howell, G., 2019. Killing Me Softly: Competition in Artificial Intelligence and Unmanned Aerial Vehicles. [online] JSTOR. Available at: <https://www.jstor.org/stable/26864279> [Accessed 6 September 2022]

for human control or intervention[8]. Development of LAWS is a result of a militarizing Narrow AI since 2017[9]. Independent researchers and experts have given their own definitions, with the essence of LAWS being described as "*weapons that can select, detect and engage targets with little to no human intervention*"[10]. Their strictly offensive nature is a determinative argument against their development and in favor of their ban in many countries, notably Japan, due to the pacific viewpoints and humanitarian concerns that rule the 21st century[11]. Currently and while LAWS are not per se regulated by the international humanitarian law, they have to be treated like other weapon systems; in accordance to the provisions and principles of IHL[12].

Hyperwar is a type of automated or autonomous conflict which uses AI and other relevant technologies and applications in such a way, that it could lead to a minimization of the need for human control over decision-making[13].

4. Methodology

[8] *Shifting the narrative: not weapons, but technologies of warfare - Humanitarian Law & Policy Blog* (2022). Available at: https://blogs.icrc.org/law-and-policy/2022/01/20/weapons-technologies-warfare/ (Accessed: 17 September 2022)

[9] Carayannis, E.G., Draper, J. Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence. AI & Soc (2022). https://doi.org/10.1007/s00146-021-01382-y

[10] Lethal Autonomous Weapons Systems: Recent Developments (2019). Available at: https://www.lawfareblog.com/lethal-autonomous-weapons-systems-recent-developments (Accessed: 19 September 2022)

[11] Ibid

[12] Davison, N. (2022) A legal perspective: Autonomous weapon systems under international humanitarian law | United Nations iLibrary, Un-ilibrary.org. Available at: https://www.un-ilibrary.org/content/books/9789213628942c005 (Accessed: 19 September 2022)

[13] Husain, A., 2021. *AI is Shaping the Future of War*. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022

Research on military AI technologies has up to now been mainly focused on the technicalities of these newly introduced systems and the ambiguous environment they create; thus, there currently exists a gap in matters related to its practical implications in the strategic field. Lacking case studies where cutting-edge AI technologies have been used on the battlefield, theoretical approaches would have been expected to address the possible outcomes stemming from their use; nevertheless, the existing bibliography is limited. The present thesis is informed by scientific research papers and articles available globally, either open-source or via academic institution subscriptions, all of them not older than 2018. The research for the drafting and final submission of the document was conducted between March and September of 2022 on scientific databases, among others Scopus and EBSCO, while also abstracting information on the subject by up-to-date reports and articles. Technology is one highly debated matter, with different countries not sharing the same viewpoints not even on the definition of, for example, Artificial Intelligence. Hence, the study varies according to the source of information, whether that comes from the United States military forces or a European report, each with its own principles, norms and practices.

5. General considerations and national policies' overview

Scholars in International Relations argue an interesting point: The actual effect of technology on war theory and practice can be found not on the tactical or operational level, but in the political and psychological field. This opinion is backed by the fact that technology does indeed come with a change in the existing balance of power. Newly acquired or developed technological assets redistribute resources, as these assets are considered to be the primary tool of global

dominance in the contemporary world. It is difficult, however, to be able to predict the actual effects, advantages and disadvantages of weaponized AI with certainty, as we have neither experienced it on a larger scale nor the technology itself remains static and non-changing[14].

As Rear Admiral Andrew Loiselle, deputy director for Future Joint Force Development on the Joint Staff 17 said, we "*cannot expect success fighting tomorrow's conflicts with yesterday's weapons and equipment*"[15].

When considering military uses of AI, a primary novel type of conflict that is considered to bring a "coup" in military operations is algorithmic warfare[16]. The military uses a variety of algorithms to categorize and forecast enemies, create personnel estimates, and devise strategies. Said algorithms expand and change as a result of national security crises, like a war[17]. Big data, the Cloud and intelligent machines are all participating in algorithmic warfare[18], rendering sensitive data

[14] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23.)

[15] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

[16] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022]

[17] Algorithmic Warfare or Algorithmic Warfare and Focal Point Analysis | Small Wars Journal (2022). Available at: https://smallwarsjournal.com/jrnl/art/algorithmic-warfare-or-algorithmic-warfare-and-focal-point-analysis (Accessed: 20 September 2022)

[18] Layton, P. (2018) "Algorithmic Warfare: Applying Artificial Intelligence to Warfighting", Air Power Development Centre, p. Available at: https://www.academia.edu/36620913/Algorithmic_Warfare_Applying_Artificial_Intelligence_to_Warfighting (Accessed: 20 September 2022)

fragile against a possible cyberattack that could destroy an enemy's national security and command system from the inside.

Artificial Intelligence can transform and alter the prevailing strategic and diplomatic balances. The fact that defensive technologies are being evolved indicates that offensive technologies are also being strengthened and enhanced. Two of the prevailing fears are the constant race for more efficient (thus, dangerous) military technologies between the nations, as well as the following concern about surprise attacks. Some countries view Artificial Intelligence as the new weapon and means of global dominance. Scientific literature on the matter considers that, if the United States do not catch up with militarized AI applications developed in other nations, then the balances of power will soon change towards a different direction than the one we know now[19]. The "Big 5" (USA, Russia, China, UK, France) each have their own agendas on technological developments and their employment in the military and tend to view technology itself in really distinct ways.

Despite the fact that a lot of –sensitive- information on AI's role on national agendas are disclosed and not publicly available for easily graspable reasons, still more than just hints complete a picture on some of the major national policies.

Russia, represented by the words of President Vladimir Putin in 2017, considers Artificial Intelligence as the tool towards ruling the contemporary world. However, updates on the field weren't nearly as close comparing to the ones in

[19] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022]

China or the United States. What is more, initiatives, advancements and developments are mainly governmentally backed and funded, thus limited in the full potential they could reach in cooperation with the private sector[20]. Above all, reliable data on AI developments are limited within the terse Russian Military Encyclopedia. Thus, scholars and researchers, as well as the public, cannot gain insight on the actual work on the field. What the Encyclopedia informs us, however, is that among Russia's goals with AI are *"the creation of knowledge systems, neuro-systems and systems of heuristic search*". We cannot be sure either for the meaning of this sentence or its exact aims and no official explanation about it has been provided[21].

Having already mentioned the distinctive definitions and opinions around AI, it is worth mentioning the distance of points of view between Russia and the United States. The US focuses on technical aspects of the matter, whereas Russia has on many occasions exhibited its interest and fixation on information, taking advantage of cyber space capabilities. Notably, in Russia there is no such term as "cybersecurity", rather "information security", a fact that pinpoints just how valuable the country considers information to be. The country views cyber warfare as a branch of information warfare and this cyberwarfare is seen as one to bring the "*third revolution in the military affairs"*, following gunpowder and nuclear weapons, as mentioned in "Artificial Intelligence – Here Are the Risks and Opportunities" by Ilnitsky and Losev[22]. The Russian military is more focused on developing better and safer information infrastructure to avoid any cyber threats and offenses and is working towards its "digital sovereignty" by setting

[20] Petrella, S., Miller, C. and Cooper, B. (2021) "Russia's Artificial Intelligence Strategy: The Role of State-Owned Firms", Orbis, 65(1), pp. 75-100. doi: 10.1016/j.orbis.2020.11.004

[21] Pavel Sharikov (2018) Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination, Bulletin of the Atomic Scientists, 74:6, 368-373, DOI: 10.1080/00963402.2018.1533185

[22] Andrei Ilnitsky and Aleksandr Losev, 'Iskusstvennyy Intellekt – Eto i Riski, i Vozmozhnosti' ['Artificial Intelligence – Here Are the Risks and Opportunities'], Krasnaya Zvezda [Red Star], 24 June 2019 [Accessed 15 September 2022]

up domestic operation systems. All of these measures are accompanied by the adoption of new and more laws on information security, where security is translated as increased governmental control. Of course, more funding is provided for the aforementioned measures on cyber and information security, with amounts up to 54 million USD in 2019. The thinking behind these actions is that the Russian government and military is convinced that its wins in the contemporary world will come from the cyber and information sphere, thus it is actively focusing on developing these capabilities, rather than its conventional weapons, tanks, missiles and arms used on the battlefield, in general[23]. As it will be explained in the Chapter of "Case Studies", Russia has used information warfare tactics in a number of situations, notably the 2016 US elections, along with the present-day war in Ukraine. Another domain of difference in the handling of AI technologies is that, in Russia, it is the military that is in charge of developing weaponized AI, whereas in the US, China and the UK, the private sector leads AI progress. Progresses made by the military in Russia include the development of AI-enhanced unmanned systems and weapons, as well as UAVs like Uran-9 UGVs, which were tested in operations in Syria with fears of once again appearing in Ukraine, as they are able to hit static targets, rendering them ideal for assassination attempts. An example is KUB-BLA, a kamikaze drone that can carry 1 kilogram of explosives, reach up to 130 kph and belongs to the category of loitering munitions, explained in the following sections[24]. The Federation has also tested their attack helicopters, the Mi-28N, which have incorporated a drone launcher able to deploy Intelligence, Surveillance and Reconnaissance systems and intelligent loitering munitions[25]. Apart from this

[23] Rod Thornton & Marina Miron (2020) Towards the 'Third Revolution in Military Affairs', The RUSI Journal, 165:3, 12-21, DOI: 10.1080/03071847.2020.176551

[24] Harding, T., 2022. *Russia's KUB-BLA kamikaze drone intercepted in Ukraine*. [online] The National News. Available at: <https://www.thenationalnews.com/world/uk-news/2022/03/14/russias-kub-bla-kamikaze-drone-intercepted-in-ukraine/> [Accessed 15 September 2022]

[25] Husain, A., 2021. AI is Shaping the Future of War. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

individual realm though, Russia is also working towards perfecting its missiles and their performance, with special consideration about electronic warfare and their air-defense and command-and-control systems[26].

China, through its President Xi Jinping, even if not expressing it directly, is working towards building robust military technologies and equipment, with the ultimate goal of leading the AI field globally by 2030, as stated in its 2017 "New Generation Artificial Intelligence Development Plan". Among its goals is a cooperation between civil and military developments of AI, in areas such as decision-making and national defense. China has expressed primary AI development interest for naval capabilities[27]. It considers that smart technologies in this sector are crucial for improving naval combat[28]. Today, the country's Liberation Army is actively working towards developing algorithms that ameliorate command decision-making by enabling data fusion and enhancing intelligence analysis. The budget provided for these projects is not insignificant and, with every year, China spends even more billions in the AI industry, ranking in close positions with the United States[29]. Its focus is first and foremost research and, afterwards, the attainment of tactical, rather than strategic and operational, goals. One of the exact technologies and AI applications that China is pursuing is procurement of a considerable number of UAVs in swarm format, but also smart

[26] Rod Thornton & Marina Miron (2020) Towards the 'Third Revolution in Military Affairs', The RUSI Journal, 165:3, 12-21, DOI: 10.1080/03071847.2020.1765514

[27] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

[28] Steven I. Davis (2022) Artificial intelligence at the operational level of war, Defense & Security Analysis, 38:1, 74-90, DOI: 10.1080/14751798.2022.2031692

[29] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

weapons and autonomously operating robot soldiers[30]. In 2020, China tested two drones, both with crucial technologies. The first one is a twin-rotor aircraft able to carry a 100 kg payload that supplies troops at high altitude, while the second one is a high-speed drone for Intelligence, Reconnaissance and Surveillance missions, but also for electronic warfare and ground strikes[31].

The United Kingdom has expressed its interest in AI and autonomous systems research and development accordingly, more practically since 2018, with the joint doctrine document "Human-Machine Teaming", where the benefit of *"superior maneuver options in and across all domains*" was recognized[32]. It has then presented its own Defence Artificial Intelligence Strategy in 2022. The UK considers the present-day security environment to be deteriorating. Thus, it has set the goal of modernizing its armed forces for defense preparedness. Urged by Russia's invasion in Ukraine in 2022, the UK talks about the need for "effective defence". As it is being understood, it is rather utopian for a nation to proclaim and support the offensive use of AI; yet, the lines between offensive and counter-force capabilities are not always so strictly distinct. As a result, it is difficult to assess just how close these mechanisms and policies can prove to be with offense and it remains to be seen. As far as what exactly this national Strategy pinpoints, it mainly focuses and urges experts to conduct research and experimentation on AI systems before exploitation and execution of their applications. The interesting part, however, is that, despite the spotlight being on theoretical explorations, what has been set as a high-priority goal is the strategic advantages

[30] Pavel Sharikov (2018) Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination, Bulletin of the Atomic Scientists, 74:6, 368-373, DOI: 10.1080/00963402.2018.1533185

[31] Husain, A., 2021. AI is Shaping the Future of War. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

[32] *Human-Machine Teaming (JCN 1/18)* (2018). Available at: https://www.gov.uk/government/publications/human-machine-teaming-jcn-118 (Accessed: 13 September 2022)

stemming from the development of cutting-edge technologies. When talking about military AI, the United Kingdom acknowledges that adversaries are willing to exploit the various uses and applications of AI and itself presents the beneficial use of AI as the solution, particularly for defence reasons[33].

Since 2019, **France** announced its vision of innovation drive in the weapon system. More specifically, an increase in budget allocated for AI was presented by the Armed Forces Minister. Just earlier, France had introduced its Man-Machine Teaming, a project focusing in incorporating AI in combat aircrafts and examining the plausibility of fighter jets and drones operating together so as to bypass defense systems. The biggest amount of the allocated budget, however, was intended for research rather than testing and using the AI applications[34]. In 2022, a high-scale project with multifaceted applications and capabilities was announced by the French Ministry of Defense and the French military procurement office Direction Générale de l'Armement published the relevant procurement. The project, under development since 2017, is called Artemis.IA and its objective is to give the country access to a big-data and AI independent and secure processing platform which can be used to exploit and analyze the enormous volumes of data coming from military hardware and other sensors. In the near future, the project is more than likely destined to be used in cybersecurity, military health monitoring, predictive maintenance or maritime surveillance[35].

---

[33] *Defence Artificial Intelligence Strategy* (2022). Available at: https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy (Accessed: 11 September 2022)

[34] *Intelligent design: inside France's €1.5bn AI strategy - Global Defence Technology | Issue 88 | June 2018* (2022). Available at: https://defence.nridigital.com/global_defence_technology_jun18/intelligent_design_inside_frances_15bn_ai_strategy (Accessed: 19 September 2022)

[35] Machi, V., 2022. *France approves final phase of Artemis big-data processing platform*. [online] Defense News. Available at: <https://www.defensenews.com/global/europe/2022/07/11/france-approves-final-phase-of-artemis-big-data-processing-platform/> [Accessed 19 September 2022]

Finally, **the United States**, even since the Obama Administration, have considered AI a key factor in the development of the country's national policies, as it has been demonstrated by the "Third Offset Strategy" by the Department of Defense. This was just the first step towards incorporating AI and other cutting-edge technologies into the agenda with more steps to come. That was the case when, in 2018, a practical action was taken by founding the Joint Artificial Intelligence Center with the subsequent Artificial Intelligence Strategy, one year later. What is worth noting though, is that in 2018 the United States stated their intention of leading AI developments with their Executive Order on Maintaining American Leadership in Artificial Intelligence, which, adding the fact that since then an increased budget is attributed to AI research and various projects, such as more than 600 projects of AI incorporation in the Air Force mission sets, is an act that demonstrates that they are not in favor of other nations catching up[36]. There exist, however, other scientific sources that stand by the fact that the Department of Defense has not taken active measures towards regulating said technologies and that this deficiency limits the potential that Artificial Intelligence could reach militarily[37]. In the end, and despite all that, the United States seem to be the current leader in the AI research and development field, according to official and publicly available sources.

Russia and **China** have their own goals for technological supremacy which they are actively and practically pursuing. They show a preference for dual-capable delivery systems, such as nuclear-capable apart from conventional stealth bombers, as well as technologically advanced conventional weapons, naturally drones, but also cyber weapons. China, even if cautious about its very own

[36] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022]

[37] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

systems in terms of their vulnerability under a cyberattack, is still positive in acquiring Artificial Augmented Intelligence (AGI) (UAVs belong in this category) in the direction of targeting and hitting an enemy, thus minimizing its need for deploying human military personnel in this type of operations and the subsequent cost, both financial and social[38].

China grants importance to research in AI, before developing its own technologies, thus it was the leading country research-wise in 2018. This key player is interested in acquiring and expanding swarming capabilities, unmanned teaming and multi-sensor fusion. This expertise led to China forming strategic diplomatic alliances advancing defensive and offensive technological infrastructure, exporting them, as well as creating relevant robust strategies for its technological capacities. More precisely, China has created ties with Pakistan, a country leading the development of mini-nuclear weapons. Apart from Asia, it deepens its affiliation with the Arab world and, particularly, with the United Arab Emirates and Saudi Arabia. As a result, China achieves a double-ended goal: it continues to work on its technological infrastructure, while also gaining allies who will benefit from imports of Chinese infrastructure, gaining access to equipment, but under China's norms and control[39].

One could argue that the information that is publicly available on matters related to AI capabilities of a particular state can be deceiving at worst, unverified or outdated at best. This seems to be the case for China, with analysts who misinterpret information on AI developments in the USA, amplifying its actual progress. What this teaches us is that the broad range of unverified information,

[38] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

[39] MacDonald, N. and Howell, G., 2019. Killing Me Softly: Competition in Artificial Intelligence and Unmanned Aerial Vehicles.. [online] JSTOR. Available at: <https://www.jstor.org/stable/26864279> [Accessed 6 September 2022]

especially in a field so vital for the existing balance of power and its stability, can distort facts and provoke an unwanted crisis[40].

Aside from major players like the aforementioned, there are also other countries that are developing and employing intelligent and AI-enabled systems in the military field. **Iran**, for example, has extensive drone production. Its production includes small, high-speed boats with autonomous drones or military-capable drones, like the Mohajer-6 that Iran exports to the Middle East, but also to Latin America. **Ukraine** works together with Turkey in producing a modernized TB2, a Medium Altitude Long Endurance unmanned combat aerial vehicle with the capability of autonomous operation and remote control. In a topic like this, it is **Israel** that cannot but be mentioned. Israel is one of the leading countries in UAV production, but also employment, as reality has showcased numerous times in operations against Palestine. Their Harop drones, loitering munitions equipped with launchers, have been exported to Azerbaijan and used by the Azeris against Armenians in the Nagorno-Karabakh conflict. **Azerbaijan** itself was able to take advantage of old military equipment, more specifically some soviet-era biplanes, and turn them into Destruction of Enemy Air Defense (DEAD) drones, used for identification of ground-to-air missile zones and destroy them with kamikaze hits. The race continues with other countries developing their own applications, systems and capabilities, notably **Pakistan**, **India**, **South Korea** and **Brazil**[41].

It seems that, for the time being, duties like planning and direction will and should remain a human responsibility. Intelligent systems are more than humanly capable of executing physical tasks or even thinking more rapidly, but decision-making on a level of conflict and war cannot -yet- be transmitted into them. Nevertheless, AI can still aid in these processes, by providing options based on

[40] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

[41] Husain, A., 2021. AI is Shaping the Future of War. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

data-processing coming from historical, cultural, diplomatic and political facts, as well as from previous operations and their outcomes. Let me mention, however, that the quality of the results is tightly dependent on the objectivity (or its absence) of data, human biases and, of course, the data's volume[42].

6. An initiation into offensive technologies

The fact that the international arena is still far from being conflict-free is rendering Artificial Intelligence, its developments and employment an even bigger risk. Michael Horowitz, professor and adjunct senior fellow at the Center for a New American Security, expressed the opinion that AI is more of an enabler for other capabilities than a technology itself[43]. This mindset is shared with Elsa Kania, Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security, who does not view AI as a weapon per se, but as a "*utility",* a helping tool for states to enhance their existing military capabilities[44]. While this thesis agrees with these statements, it seems that AI is more of a tool which enhances winning possibilities in (cyber) conflicts and also a new criterium of power, a mindset shared among the most powerful states in the political and diplomatic arena.

[42] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

[43] Horowitz, M. (2018) *Artificial Intelligence, International Competition, and the Balance of Power - Texas National Security Review*, *Texas National Security Review*. Available at: https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/ (Accessed: 16 September 2022)

[44] Foster, M., 2019. *Artificial Intelligence and Stability in Nuclear Crises*. [online] Usafa.edu. Available at: <https://www.usafa.edu/app/uploads/Space_Defense_Vol12_No01.pdf> [Accessed 16 September 2022]

Purely defensive technologies enabled by Artificial Intelligence in use by the military at the present time are, namely, planning, logistics and transportation[45]. Yet, at the current stage of development and practical use, it is vagueness that rules the distinctive line between defensive and offensive technologies, with the latter divided into technologies with an impact on the tactical/operational and the strategic level of war. While the first one refers to specific weapons, mechanisms and methods that are used during a conflict, the second one concerns a series of actions that are able to cause an imbalance of power between key players[46]. Instability is inherent with the use of this novelty, especially within the military by commanders and soldiers that are not experts on how it functions. This comes with a more intense likelihood of conflict or war; every state will have to deal with an uncertainty of an adversarial AI-enabled (cyber) attack, without yet having the necessary know-how for what the according counter measures are.

Examining this distinction between the tactical and operational level, the scientific community highlights the benefits that integrating Artificial Intelligence at the operational level of war brings in terms of competitiveness and force; by exploiting inter-functioning narrow AI systems at the operational level, commanders will explore a variety of new tools which will assist them in perfecting planning before executing. Scholars support the idea that AI is much more pivotal in this stage of operations' organization, as tools at the tactical level, while practical and effective, are of limited span and scope (for example, offensively hitting an adversarial target). It is at the operational level that influential actions are taken and this is a field where AI is neither actively taken

[45] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022]

[46] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

advantage of nor theoretically promoted by the scientific and research community[47].

The complexity of distinction between defensive and offensive technologies is not only due to the fact that AI technologies are still rather limited on the battlefield or in cyberwars, but also because offensive technologies can be introduced and concealed as defensive, exploiting the knowledge gaps in the field. A system or software which was presented as a defensive one, for example domestic surveillance for security reasons, can actually serve offensive goals, such as illicit surveillance of an adversary. A state realizing this situation can perceive it as a threat, an uncertainty of being able to respond which can lead to an accumulation of even more advanced (counter) technologies, ultimately leading to a constant technological race between the states that will bring uncertainty; a race in acquiring the latest technological innovations and a race in updating safety standards and superiority in critical information infrastructure with uncertainty due to the non-necessarily symmetric acquisition of power. And, falling behind in technological innovations and their acquisition will be impossible to cover with conventional methods and weapons[48].

AI can be fused into already existing weapons and provide them with new capabilities, autonomy or situational awareness, or enhance human capacities in terms of accuracy, effectiveness and speed. In terms of terminology, a lot of talk goes on about "*algorithmic codes"* and "*nano-bio-info-cognitive technologies"*[49].

[47] Steven I. Davis (2022) Artificial intelligence at the operational level of war, Defense & Security Analysis, 38:1, 74-90, DOI: 10.1080/14751798.2022.2031692

[48] Rod Thornton & Marina Miron (2020) Towards the 'Third Revolution in Military Affairs', The RUSI Journal, 165:3, 12-21, DOI: 10.1080/03071847.2020.1765514

[49] Shifting the narrative: not weapons, but technologies of warfare - Humanitarian Law & Policy Blog (2022). Available at: https://blogs.icrc.org/law-and-policy/2022/01/20/weapons-technologies-warfare/ (Accessed: 17 September 2022)

It can also act as an assistant in locating and hitting targets or individuals on the conventional battlefield, while also being able to cause major damage to national command infrastructure systems or important networks in general, through cyberattacks. Enhancing, for example, autonomous weapons or improving missile guidance brings the user one step closer to victory and dominance, but it also pushes the adversary towards creating and developing counterforce technologies, supposedly defensive, yet where the limits with offensive become opaque.

No matter the developments of offensive AI capabilities, the criterium of reliance has to be taken into account. In other words, how AI is incorporated into a function or operation determines the level of dependence on it and, as a result, this dependence is a much safer criterium than the acquisition of a technology per se. For example, rendering AI in charge of final decision-making means a much stronger reliance than simply using it for reconnaissance[50]. As a result, AI applications have to be examined not only as technological tools, rather than in relation with the domain to which they are applied.

7. Types of AI-enabled offensive technologies

A list about all AI-enabled offensive and, generally, weaponized technologies would be both exceedingly lengthy and technical for the scope of this thesis. Be that as it may, some worth mentioning militarized AI capabilities will be listed and explained below. Before that, and to provide a general essence of what AI capabilities are and mean to the military, we could say they are, basically,

[50] Foster, M., 2019. *Artificial Intelligence and Stability in Nuclear Crises*. [online] Usafa.edu. Available at: <https://www.usafa.edu/app/uploads/Space_Defense_Vol12_No01.pdf> [Accessed 16 September 2022

techniques that have been developed in such a way, so as to enable other tools to "think smart" in a human-like way and to operate in a, semi or fully, autonomous way. The technological methods applied to achieve this outcome are, notably, Natural Language Processing and Visual Scenes Interpretation, Machine and Deep Learning and Video Analytics, which allow the systems to conduct a decision-making procedure. Back further, the primary methods that allow all of the above are based on three functions: logical reasoning or symbolic AI, probability and statistical reasoning (data-dependent)[51]. A combination of AI bits introduces new capabilities, such as automated extraction of hierarchies, system control with reinforcement learning, simulation-based prediction, advanced forms of search, all of them revolutionizing the battlefield, whether that be conventional or cyber. All of the previously mentioned technologies and applications render AI an advantage in conflict and especially in three domains: perception, decision-making and action[52].

A primary means of offensive weapon taking advantage of new technologies would be an Artificial Super Intelligence "supercomputer" that makes use of its almost unlimited computing resources, in order to attack targeted military points and infrastructure[53]. This type of technology, however, would require an unimaginable cost and is currently only a theoretical approach and not a military reality. In a more realistic and contemporary sense, as far as cyber operations are concerned, AI applications transform the nature of war, adding more spheres to possible conflict zones. There, tools can remain untraceable and cause excessive

[51] Legal reviews of weapons, means and methods of warfare involving artificial intelligence: 16 elements to consider - Humanitarian Law & Policy Blog (2019). Available at: https://blogs.icrc.org/law-and-policy/2019/03/21/legal-reviews-weapons-means-methods-warfare-artificial-intelligence-16-elements-consider/ (Accessed: 17 September 2022)

[52] Husain, A., 2021. *AI is Shaping the Future of War*. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

[53] Pavel Sharikov (2018) Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination, Bulletin of the Atomic Scientists, 74:6, 368-373, DOI: 10.1080/00963402.2018.1533185

damage to critical systems and infrastructure. Automatically developed cyber weapons and methods, such as espionage and intelligent scanning of vulnerabilities in an adversary's system, identifying paths to be exploited can lead to autonomous conduct of large-scale, high-impact cyber wars[54]. Furthermore, developed for malicious objectives software, such as the strictly harmful AI-enabled Hazardous Intelligent Software, can be used in military cyberwarfare operations and, including trojan horses, spyware, viruses or warms, are able to cause great harm to sensitive and confidential data and systems[55].

Another type of cyber offensive technology enabled by AI are the cyber NC3 "kill switch" attacks, which are a type of attack that tracks, targets and attacks an enemy's nuclear-weapon systems[56]. One can only imagine the consequences a powerful, remote offensive technology can have on nuclear security.

False-flag operations are designed to deflect attribution to a neutral party, while the actor behind the attack takes steps to impersonate or use the distinctive infrastructure, tactics, techniques or procedures to appear as if it had been the work of another party. The Olympic Destroyer cyberattack against the 2018 PyeongChang Winter Olympic Games is regarded a false flag operation, in which Russia's GRU designed its attack to appear as if it had been the work of North Korea. A false flag operation could easily escalate tension between two parties and this is particularly evident in the case of a third-party actor aiming at a state's nuclear systems, known as NC3 (command, control, communication), which due

[54] Husain, A., 2021. AI is Shaping the Future of War. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

[55] Pistono, F., & Yampolskiy, R. V. (2016). Unethical Research: How to Create a Malevolent Artificial Intelligence. *arXiv*. https://doi.org/10.48550/arXiv.1605.02817

[56] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

to their importance could easily trigger an immediate response by the affected state, as the latter considers this act to only be the first of more strikes to come. The situation does not leave much room for diplomacy, research by the intelligence units and careful, strategically built political reactions, quickly leading to an unwanted escalation towards a state that actually is not even to blame[57].

There are AI offensive capabilities that are able to affect public confidence in the state's technological readiness, either through an attack on important systems or a technological attack on personnel in charge of these systems[58]. A characteristic case study in this setting is cyberweapons in "left of launch" operations. Their strategy is based on a preemptive strike with new non-kinetic technologies, such as electromagnetic propagation, cyber, as well as an offensive force to defeat nuclear ballistic missile threats before they are launched, known as "left of launch." They are rumored to have been used by the USA towards Iran and North Korea, with the goal of undermining these countries' confidence in their own nuclear forces and systems, as well as in their technological capabilities[59].

Another type of action that can lead to an escalation is through the deliberate dissemination of relevant or irrelevant information (this is where information is "weaponized") about a crisis, crucial to its continuation and the public's stance[60]. Colonel General Nogovitsyn defined information warfare as the deliberate

[57] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

[58] Ibid

[59] *Left of Launch – Missile Defense Advocacy Alliance* (2022). Available at: https://missiledefenseadvocacy.org/alert/3132/ (Accessed: 5 September 2022)

[60] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

destruction of information systems, processes, and resources, as well as widespread indoctrination of troops and the populace, destabilizing society and an adversary state as a whole[61]. Using software and hardware to break into appropriate systems, gathering intelligence by hacking, intercepting, or decrypting information using specially designed devices (electronic intelligence), harming or compromising these systems and denying the enemy access to some parts of the information infrastructure are all possible goals of an information operation[62]. We will study the act of "information warfare" in the Case Studies Chapter, with the case of the Russian interference in the 2016 USA elections.

USA uses an autonomous AI-enabled Long Range Anti-Ship Missile (AGM-158C), which serves as an extremely accurate and efficient weapon in hitting what are considered high-priority targets[63]. These are used in the Air Force and cost almost 4 million USD[64], while with the current developments it is being incorporated in the Navy too, on the Boeing P-8 Poseidon[65], an integration costing as much as 74 million USD[66].

[61] *Russian Interference in the U.S. Presidential Elections in 2016 and 2020 as an Attempt to Implement a Revolution-like Information Warfare Scheme* (2021). Available at: https://warsawinstitute.org/russian-interference-u-s-presidential-elections-2016-2020-attempt-implement-revolution-like-information-warfare-scheme/ (Accessed: 20 September 2022)

[62] M.T. Kłoda, Stany Zjednoczone Ameryki: przegląd projektów prawa stanowego USA dotyczących badań nad wykorzystaniem technologii blockchain w elekcjach państwowych, „Przegląd Sejmowy" 2020, No. 4 (59), pp. 252–253

[63] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

[64] Trevithick, J. (2020) *Here Is What Each Of The Pentagon's Air-Launched Missiles And Bombs Actually Cost*, *The Drive*. Available at: https://www.thedrive.com/the-war-zone/32277/here-is-what-each-of-the-pentagons-air-launched-missiles-and-bombs-actually-cost (Accessed: 6 September 2022)

[65] Gain, N. (2020) *NAVAIR progressing towards LRASM integration on P-8A MPA - Naval News*, *Naval News*. Available at: https://www.navalnews.com/naval-news/2020/05/navair-progressing-towards-lrasm-integration-on-p-8a-mpa/ (Accessed: 6 September 2022)

[66] *US Navy funds LRASM integration onto P-8A Poseidon MPA* (2021). Available at: https://defbrief.com/2021/04/22/us-navy-funds-lrasm-integration-onto-p-8a-poseidon-mpa/ (Accessed: 6 September 2022)

When it comes to decision-making, a tool that is widely used is the Correlation of Forces calculator (COF). It serves in strategic planning, through determining the result of a clash and uses the calculated capability of blue versus red force to make this prediction[67].

Unmanned Aerial Vehicles (UAVs) are one of the leaders of the AI-enabled offensive technologies used on the battlefield and a domain of high-priority for many countries, even Greece. They have already been deployed in a series of operations and countries, especially in the Middle East[68]. Special focus has been placed on their navigation systems and sensors, which allow them to maneuver in complex, limited-visibility hostile environments and adjust to the enemy's changing moves instantly[69]. UAV types vary in line with the specific functions they support. It is worth mentioning some of these systems, along with the AI technologies they employ.

- High-altitude Long-Endurance (HALE) UAVs: As their name indicates, these UAVs have the capacity for lengthy flight periods and extended terrain surveillance. They are used for Intelligence, Surveillance, Reconnaissance (ISR) operations, intelligence gathering, while also proving useful in electronic warfare via battle network communication. Below, a HALE UAV is depicted, the Baykar Bayraktar Akıncı[70].

[67] Husain, A., 2021. *AI is Shaping the Future of War*. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

[68] MacDonald, N. and Howell, G., 2019. Killing Me Softly: Competition in Artificial Intelligence and Unmanned Aerial Vehicles.. [online] JSTOR. Available at: <https://www.jstor.org/stable/26864279> [Accessed 6 September 2022]

[69] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/>

[70] SABAH, D. (2021) Turkey's Baykar to mass produce Akıncı UCAV soon, Daily Sabah. Available at: https://www.dailysabah.com/business/defense/turkeys-baykar-to-mass-produce-akinci-ucav-soon (Accessed: 8 September 2022)

Manufactured in Turkey, this unmanned combat vehicle has been employed in operations in Syria, Libya and Azerbaijan, and actually holds many advantages compared to US drones, in terms of capabilities, cost and mission profile[71].

Baykar Bayraktar Akıncı HALE UAV

(source: https://en.wikipedia.org/wiki/Baykar_Bayraktar_Ak%C4%B1nc%C4%B1)

- One of China's major exports constitutes MALE (Medium Altitude Long Endurance) UAVs, which are the most notable strike-capable UAVs. This is something extremely favorable for China, as it becomes the market of an important product on which buyers are depending, while also paving the way for its development and usage.

- Tactical Unmanned Aircraft Systems: This particular type acts as an aerial support for forces on the ground, thus providing them with a much more holistic situational awareness. Thus, it indirectly aids the fighter with multidimensional capabilities, as it can fly for a long time, all while inspecting large zones.

[71] Husain, A., 2021. AI is Shaping the Future of War. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

- Loitering munitions: A primary type of directly offensive equipment, this UAV sub-category is able to hit specific targets and self-destruct into them after being programmed to do so. With its light nature, which can be as limited down to 3 kg and the power of being piloted through a cell phone (!), a loitering munition can be extremely precise in its attack and has definitely gained recognition and appraisal among the military. Worth noting that one of the countries developing loitering munitions is Israel, followed by the United States and, then, China.

- Large Rotor-Based Platforms: Another mainly offensive technology, these mini-rotor and mini-helicopter equipment are executing missile launcher, machine gun and small precision bomb operations with great efficacy. China, not oblivious to these benefits and also aiming to minimize costs in military processes, is the current development leader in the game, also exporting them to Middle Eastern and African markets.

Ziyan Blowfish Unmanned Helicopter System (2015)

Source: https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2026#images

- Swarms: A form of operating as a group. In UAVs, the method of operating together, synchronizing their attacks and defenses. Swarms are a pivotal method of practice for AI military applications. Taking into consideration

the capabilities of a single UAV, one can imagine the power of a team working together. The potentials vary: from functioning and hitting targets in a denied airspace to carrying assets or explosives, effectively allocating them on a specified terrain[72]. The latter task has been developed by Russia in small multi-rotor UAVs conveying bombs, with their tiny size maximizing their accuracy. On the same pathway, China is the current leader in drone swarms, with its production firstly introduced as a way to fight against extremism outside the country or for domestic reconnaissance missions, especially maritime, and generally non-lethal activities.

The benefits of UAVs and of their concrete types depend on the Artificial Intelligence technologies they have incorporated, whose level of efficacy must be tested beforehand in war-like scenarios, in order to be practically examined and evaluated. Taking a look into the specific AI applications, UAVs will help better understand just how important they are for enabling these novel capabilities that alter the nature of war.

- Air combat algorithms: As implied by the name, this technology is developed by human pilots training the system, in a way that the latter becomes capable of adapting and operating in an air-to-air battle environment, using a technology known as Deep Reinforcement Learning. This is not just on a theoretical level, as it has been successfully been carried out in tests conducted on an F-16 by the Air Force Research Laboratory and Lockheed Martin Skunk Works in 2017. The great

[72] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

performance of the algorithm on the unmanned F-16 showcased excellent skills and adaptability in air-to-ground strike mission simulations.

- Machine vision: This AI technology aids in target or moving objects/subjects' recognition and identification, via automated classification of data. Its benefits are traced to the enhanced situational awareness capabilities this application offers, even in otherwise limited-visibility environments, and serves as an outstanding vision-based navigator. Among others, facial and gait recognition, as well as license plate reading, constitute forms of machine vision potential.

- Automated missions: Taking advantage of the previous application (machine vision), UAVs are able to autonomously hit specific pre-approved targets. Examples are loitering munitions in Israel and Turkey but also China, which operate in an automatic manner after being given commands, executing them in the most efficient way possible.

- Autonomous flight: Even such technologies as UAVs may come across obstacles that halter their functions. An airspace where remotely controlling the vehicle is not technically feasible, needs a much greater independency and, if possible, full operational autonomy. This is what autonomous flights are about; various AI applications are combined to provide autonomy, such as cognitive visual recognition, image mosaicking and data processing.

On the side of cyber tools and offensive technologies, two promising methods are **infiltration** and the **use of swarms**, which was already mentioned in the field of

UAVs. Infiltration is the ability of storing previous memories acquired by an autonomous agent during reconnaissance missions and later using them to build an infiltration plan. Swarming, as briefly defined above, is a composition of autonomously cooperating agents, without the need for commanding and controlling them in a centralized way[73]. Other widely used methods include **espionage**, **malware planting**, **system destruction**, with most of these enabled after **reconnaissance for vulnerabilities** procedures have been carried out[74]. With stronger systems with enhanced capabilities developed every day, seeking vulnerabilities and hitting targets will become easier and quicker and the damage extremely more difficult or even impossible to repair.

Deepfakes, a new Artificial Intelligence-enabled technology that has been present since 2017, where Machine Learning in neural networks plays the important role of producing the desired fake, audio or visual results in the form of an image, video or voice record[75]. More than ever, deepfakes are influencing the public's opinion and fuel propaganda in a much more intense way than fake news, as this technology affects more senses, making it more believable. In the case studies section, we will examine the use of deepfakes in the recent conflict between Russia and Ukraine and their role in the ongoing war.

Artificial General Intelligence (AGI) is an even more advanced AI technology that displays human-like functions and can be used in executing a substantial range of tasks, with an ability of integrating data-types that are unseen. Naturally,

[73] Pavel Sharikov (2018) Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination, Bulletin of the Atomic Scientists, 74:6, 368-373, DOI: 10.1080/00963402.2018.1533185
[74] Rod Thornton & Marina Miron (2020) Towards the 'Third Revolution in Military Affairs', The RUSI Journal, 165:3, 12-21, DOI: 10.1080/03071847.2020.1765514
[75] Kietzmann, J. et al. (2020) "Deepfakes: Trick or treat?", Business Horizons, 63(2), pp. 135-146. doi: 10.1016/j.bushor.2019.11.006

a technology of this scale calls for advanced programming and coding skills and actually needs self and meta-programming to carry out its goals[76].

Needless to say, the combination of various technologies and AI applications, not only enable a new range of enhanced functions, but also introduce bigger threats. For instance, and citing an example by Michael Horowitz, a missile salvo can use a combination of **AI, Big Data Analytics** and **cyber capabilities**, which, along with an **AI-augmented autonomous weapon**, could be used to (counter) strike an adversary's powers[77].

8. Benefits of employing AI-enabled applications in the military

For their user, AI weapon systems and their technologies, present unprecedented benefits; speed, accuracy, precision in objective measures like blast radius and efficacy increase[78]. Speed in processing information flows from multiple channels operating simultaneously and in moving before your enemy maximizing survival rates is one of the most vital elements one has to have on the battlefield. A commander presented with pre-processed data has a strategic advantage over their adversaries and can incorporate the analyzed data into their decision-making. Speed also appears in machine operation: Between an AI system on a

[76] Steven I. Davis (2022) Artificial intelligence at the operational level of war, Defense & Security Analysis, 38:1, 74-90, DOI: 10.1080/14751798.2022.2031692

[77] Foster, M., 2019. *Artificial Intelligence and Stability in Nuclear Crises*. [online] Usafa.edu. Available at: <https://www.usafa.edu/app/uploads/Space_Defense_Vol12_No01.pdf> [Accessed 16 September 2022

[78] Blanchard, A., Taddeo, M. Autonomous weapon systems and *jus ad bellum*. *AI & Soc* (2022). https://doi.org/10.1007/s00146-022-01425-y

simulated aircraft and a human pilot, AI has a 250 times faster control than the human. The control included, apart from operating the aircraft, choosing between offensive and defensive tactics and calculating counter-firing options[79]. More similar tests have been conducted, such as the "Alpha DogFight" in 2020, a competition organized by the Defense Advanced Research Projects Agency between human pilots operating F-16 and AI agents. AI won by 5-1, yet doubtful was the feedback about the contest that questioned whether its rules were dictated fairly[80]. On a more technical level, AI can process considerable amounts of data without the human tendency to focus on some, while bypassing others. This procedure can almost simultaneously be combined with a further process: developing suggested action plans, according to the analyzed data.

Furthermore, an increase in the lethality of the adversary and maximized possibilities of survival and durability for the user and of the systems they protect, especially if those are of high importance, such as nuclear weapons, is a highly important benefit. Still, what constitutes a benefit can also prove to be a disadvantage; for example, speed leads to quicker decision-making and immediate operation, but this exact speed can also uneventfully lead to an escalation that turns into a crisis, then a conflict and, inevitably, a war or even a nuclear showdown[81].

[79] Steven I. Davis (2022) Artificial intelligence at the operational level of war, Defense & Security Analysis, 38:1, 74-90, DOI: 10.1080/14751798.2022.2031692]

[80] Husain, A., 2021. *AI is Shaping the Future of War*. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

[81] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022]

Incorporating AI on the conventional battlefield provides the actor with new or enhanced capabilities and, to be more specific, some functions include automated classification of sensor information, leading to an increase in target tracking, recognition and hit accuracy rates. Indirect support to the previous service is being offered by other capabilities, such as navigation using 3D maps, the ability to detect concealed objects and obstacles, thus altering their route for safety[82].

AI is of extreme importance for object identification, a vital starting point for a successful military operation. But its benefits extend to more aspects than just that, as it offers increased ISR capabilities and, correspondingly, situational awareness[83]. Combining AI with Big Data Analysis could aid in quickly recognizing a really fragile infrastructure, in other words an easy target, as well as the best timing to make the necessary attack[84].

Pattern recognition, an extremely beneficial application, can also aid in decoupling civilians and allies from enemies and thus assist in better decision-making by military commanders. With Deep Learning technology, a system's algorithm can be trained to analyze and predict territories, the types of attacks and the time estimation that these might take place (predictive analysis), allowing commanders to adjust and quickly prepare their counter-responses. Deep Learning capabilities also prove to be useful away from the conventional

[82] MacDonald, N. and Howell, G., 2019. Killing Me Softly: Competition in Artificial Intelligence and Unmanned Aerial Vehicles.. [online] JSTOR. Available at: <https://www.jstor.org/stable/26864279> [Accessed 6 September 2022]

[83] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022

[84] Pavel Sharikov (2018) Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination, Bulletin of the Atomic Scientists, 74:6, 368-373, DOI: 10.1080/00963402.2018.1533185

battlefield, in cyberspace and during cyber offense/defence and electronic warfare[85].

Above all, technology minimizes or even eliminates the possibility of human losses on the battlefield. Robots would do just that, functioning either with full autonomy using predictive analytics, Machine Learning and 3D navigation systems or with a human operating them from a distance. Their ability to conduct operations for a long duration without any physical or self-protection needs, as well as durability during operations in hostile conditions (chemical, radiological, nuclear environments) that human biology cannot endure, offers an unbeatable advantage against human soldiers. Colonel Daniel Sullivan described it perfectly when he said that, with all these technological possibilities, the "dirty" work of going first during an operation should be done by a robot with lethal capabilities, and not by an "*air breather"*[86].

AI systems, algorithms, software and systems exceed the skills of any human in terms of observation, speed, orientation, navigation and acting. Even when exhibiting a faulty behavior or an error, these are corrected and never again repeated, using feedback accumulated with the help of the pioneer Machine Learning technology. Another benefit can also be found in the asymmetry of power, independently of numbers. What is implied b that is that a single AI-enabled system can "outnumber" an assemblage of conventional means, in terms

[85] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

[86] Ibid

of power and capabilities[87], in simple words one AI tool wins numerous human beings working together.

All in all, AI-enabled weaponized technologies are and will continue to be even more inexpensive and easily, rapidly and massively produced and employed. What is more, they will be able to operate in a much more autonomous and automatic way, without the need for human control or supervision[88].

9. Ethical, legal, political, technological and other challenges

As helpful as it might prove to be, a cutting-edge technology with thinking and acting capabilities in such a fragile environment as a (cyber) battlefield, can turn out as dangerous as a soldier lacking training. The danger threshold is even more extensive when combining these innovative and untested in the military context technologies with other information technologies, such as AI with Cloud Computing, Big Data and the Internet of Things. With this combination, new offense possibilities emerge and, naturally, more threats[89].

Especially in the high-risk field of nuclear security, any advancement and technological breakthrough will follow the rules of the state that produced and introduced it to the rest of the world. Unless common, binding norms are

[87] Husain, A., 2021. *AI is Shaping the Future of War*. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

[88] Ibid

[89] Pavel Sharikov (2018) Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination, Bulletin of the Atomic Scientists, 74:6, 368-373, DOI: 10.1080/00963402.2018.1533185

discussed, agreed upon and drafted, every progress will most likely conflict with the interests of other actors and each state will be left unhindered developing their own, legitimate or not, ethical or not, capabilities. It is a huge risk allowing states to work independently and without any supervision by an external, international organ, as it can turn out that just one nation might have accumulated such great power and capabilities, an Artificial Super Intelligence even, that it would obtain technological, economic and political monopoly. Of course, this state would then be able to prevent further developments from other states, using its newly accumulated power[90].

Another factor that nations have to consider is unpredictable and questionable results in AI-to-AI interactions. No one can be sure how differently developed systems that have not been tested together in a simulated battle scenario would react when converging with each other, especially in an encounter with offensive goals. Unpredicted and unwanted startles confuse at best or end up in an escalation in the worst-case scenario. Apart from technicalities, serious debates and questions are also raised by disputes over legal responsibility for actions executed by the machines; is it the developer or the military commander who bears responsibility for a faulty operation? Is the guilt not born on anyone? If we exclude the latter as impossible and do the same for the developer on the basis of a really distant proximity with the result of the machine's action (unless it is a fault in coding), even then we cannot easily attribute the blame with such a chaotic hierarchy within the military. This absurdity has been confirmed within the US, where there is an ongoing heated debate over authority and responsibility for drone strikes[91].

[90] Carayannis, E.G., Draper, J. Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence. AI & Soc (2022). https://doi.org/10.1007/s00146-021-01382-y

[91] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at:

On a similar note, even when considering completely emotionally-lacking systems that only function to serve set goals, we have to bear in mind that we are still far from reaching a level of total autonomy, without any human supervision, particularly in systems capable of delivering lethal results (LAWS). Therefore, when the human factor is incorporated, it is once again challenging and uncertain just how humans will interact when cooperating or supervising AI systems. Personality and emotions affect the use of AI applications, as much as the technologies themselves and there always exists the possibility of pursuing wrong objectives. Each person cooperating with a system will bring its own dynamic to the way it operates and that is an uncertainty that definitely has to be dealt with by setting some minimum legal norms and acceptable practices.

Apart from the previous point, human thinking is not a function that –at least up to now- has been incorporated into all these AI systems and it definitely constitutes something that will always be necessary, especially in times of conflict. Therefore, in weaponized applications designed for military use, human intervention should always be estimated to exercise at least the minimum amount of necessary supervision and cover legal issues around accountability.

AI systems, despite their beyond-human-limitations capabilities, are themselves vulnerable when there are errors in their coding or faulty/inadequate data inputs and human biases. The latter, seemingly innocent, can actually cause unwanted consequences equipment-wise, diplomatic dysfunction and crisis. Indeed, AI can be used in predicting possible outcomes in a rapid way, so that valuable time is gained for accurate decision-making. However, no decision concerning crisis or

<https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022]

a war should be hasty and based on predictive analytics, as military command, notably during war, will always remain an absolute human-dependent endeavor, as it should. Some aspects that are needed for command and decision-making can indeed be integrated into AI: judgement, willpower and flexibility for example, are objective and easy-to-achieve goals for a system. AI does not suffer from memory limitations and achieves perfect data recall. It is the correlations drawn from experiences and in "non-linear" ways, however, that not even the most powerful Machine Learning algorithm can, at least for now, attain[92]. Even a high-prediction rate up to 90% from a high-end Machine Learning algorithm is not acceptable and cannot be enough to justify such a heavy political decision that bears the risk of human losses, such as war.

Unpredictability is an indispensable outcome of autonomy. As it is being understood, testing and confident validation of the programmed functions is imperative. Until that happens, we cannot be sure that the AI application at hand will act accordingly to its programming and this is a huge risk to take. As Vice-Chairman of the Joint Chiefs of Staff General Paul Selva mentioned, "*In the Department of Defense, we test things until the break. You can't do that with Artificial Intelligence. We're going to have to figure out how to get the software to tell us what is has learned"*. Thus, to fully explore and assess its applications, AI needs to be incorporated into major-scale operations after considerate testing in simulated case-scenarios followed by low-risk real operations. Where big interests and human life risks are at stake, AI will remain an unpredictable weapon that could result in an unwanted aggravation and non-wanted escalation of events and that is true both for semi and fully autonomous systems. The first category has a "*natural fail-safe",* for Paul Scharre, author of the award-winning "Army of None: Autonomous Weapons and the Future of War", which signifies

[92] Steven I. Davis (2022) Artificial intelligence at the operational level of war, Defense & Security Analysis, 38:1, 74-90, DOI: 10.1080/14751798.2022.2031692

the aforementioned uncertainty of human-machine cooperation, whereas the second category of fully autonomous weapons encompasses the serious risk of exhibiting wrong behavior, like hitting civilians as a result of false identification or friendly infrastructure due to expired data in an algorithm. It is evident that, in times of conflict and crisis, removing the human factor only favors confusion[93].

There also exists a question of proportionality concerning the means of an attack or a counter-attack. What this means is that cyber tools are still a novelty as a means of weaponry in the military sphere. An AI-backed or a cyber-attack can be difficult to be dealt with, as what exactly is the necessary, adequate and proportional method to make use of for an offense or a defense is vague. Once again, this causes unpredictability and destabilizes security, as the criteria remain subjective to each state's judgement[94].

It will be mentioned various times throughout the present thesis, but it is compulsory for regionally or, if possible, internationally accepted common schemes to be adopted on an ethical and legal level, which currently are non-existent or inadequate and outdated. On the ethical side, it is indisputable that algorithms carry no ethical barriers, nor are they sentimental and humanitarian in their behavior[95]. This, along with the reduced cost of autonomous weapon systems compared to employing human personnel, could holistically alter the nature of war and make the decision to proceed to one much easier, both for the government but also for the public, which will base such an idea on the perception

[93] Steven I. Davis (2022) Artificial intelligence at the operational level of war, Defense & Security Analysis, 38:1, 74-90, DOI: 10.1080/14751798.2022.2031692

[94] Foster, M., 2019. *Artificial Intelligence and Stability in Nuclear Crises*. [online] Usafa.edu. Available at: <https://www.usafa.edu/app/uploads/Space_Defense_Vol12_No01.pdf> [Accessed 16 September 2022]

[95] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

that lack of need for people to go to war, thus "nothing to actually risk to lose", is enough to support it. Accurately embodying the essence of this paragraph are the words of Keith Abney in "Autonomous Robots and the Future of Just war Theory", that "*autonomous robots, with their promise of fewer casualties, will make war less terrible and therefore more tempting, plausibly enticing political leaders to wage war more readily"*[96]. Nevertheless, it is a common and logical belief that a programmed, algorithmically-based decision to kill a human being, without any human control or ultimate choosing, definitely contravenes basic principles of human dignity[97]. Particularly an ASI would never alleviate from its objective and would definitely not share altruistic and human values; even in the case where it had a positive final goal, such as a simple reconnaissance mission, that would not mean that it would not violate human rights to do so, especially if the human was an obstacle in achieving this positive goal[98].

As explained right before, public perception is, in the cases of diplomatic tension and conflict, extremely critical, as it shapes policies and strategic balances and can be easily affected by fake news, propaganda and deep fakes, all novel technological means of manipulation that were once solely conducted by the Press. These tools can shape a faulty public opinion into a voice so pressuring and absolute, that it can push the leaders to quick, heated, undebated decisions that cause an instability.

[96] "Autonomous Robots and the Future of Just war Theory 1" (2013), pp. 338-351. Available at: https://www.taylorfrancis.com/chapters/edit/10.4324/9780203107164-37/autonomous-robots-future-war-theory-1-keith-abney (Accessed: 17 September 2022)

[97] Blanchard, A., Taddeo, M. Autonomous weapon systems and *jus ad bellum*. *AI & Soc* (2022). https://doi.org/10.1007/s00146-022-01425-y

[98] Carayannis, E.G., Draper, J. Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence. AI & Soc (2022). https://doi.org/10.1007/s00146-021-01382-y

Finally, taking into consideration that, despite their final use by the military, AI systems are and will be developed by private companies or laboratories that are not necessarily supervised by the government, nor will they serve its interests. Big companies that are making deals of millions of dollars would not necessarily prioritize reducing human suffering and ameliorating their position, nor would they necessarily care to develop their codes and algorithms in such a way that the systems would enjoy humanistic values. This is alarming because such technologically advanced weapons with lethal capabilities should not be left completely (or at all) outside public control. Without control, any of these systems could easily and without any trace end up in the hands of non-state actors, extremist and terroristic groups that will exploit them in a foreseeable dangerous way, with the possibility of attributing an attack to a third party or state, blackmailing them.

10. Nuclear stability and AI

Nuclear weapons brought a true revolution to war theory and practice and revolutionized any previously existing concept around international conflicts. Up to now, and despite some minor crises, the nuclear sector has enjoyed stability and peace after the Cold War. Technology and developments in AI may offer easy and quick-to-make and execute decisions, but they can also prove literally catastrophic when nuclear weapons are concerned. In this particular domain, a race between major nuclear states to continuously advance nuclear capabilities through technology encompasses a well-understood political, diplomatic and, undoubtedly, social risk. Indeed, China, Russia and the United States have already publicly supported and encouraged research on AI implementation in nuclear systems. A fear that whoever acquires the relevant knowledge and

benefits will threaten the world with an easily winnable, for them, nuclear war, is more present than ever[99].

AI, incorporated into nuclear systems and subsequent nuclear operations, augments the escalation risk during conflicts or, even earlier than that, in times of crisis in general. Repercussions of tension in this domain are to be taken extremely seriously, as they could produce disastrous effects. For example, in an era where information, its manipulation and effortless dissemination, plays a pivotal role in times of crisis, a party seeking to achieve its personal goals of dominance, could spread fake news around nuclear systems, their detonation or a missile test, causing such an alerting imbalance in diplomatic relations and the public, that the threatened unprepared government can easily take actions otherwise not chosen[100].

Autonomy in the nuclear sector is something that sounds as alarming as it is. Russian "Poseidon", or Status-6 Oceanic Multipurpose System, is an autonomous nuclear-powered and nuclear-armed missile, a robotic submarine, capable of delivering nuclear payloads, apart from conventional ones. Russia has extensively presented this system as a threat both to the United States and to the United Kingdom which, alongside autonomy, does sound disturbing[101].

[99] Foster, M., 2019. *Artificial Intelligence and Stability in Nuclear Crises*. [online] Usafa.edu. Available at: <https://www.usafa.edu/app/uploads/Space_Defense_Vol12_No01.pdf> [Accessed 16 September 2022]

[100] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

[101] Woolf, A., 2022. *Russia's Nuclear Weapons: Doctrine, Forces, and Modernization*. [online] Congressional Research Service Reports. Available at: <https://crsreports.congress.gov/product/pdf/R/R45861> [Accessed 16 September 2022]

Other worrisome and alarming possibilities include unauthorized access and advanced persistent threatening (APT) to control and command nuclear systems, system deception and the sending of false alarm signals. Clearly these incidents, given the gravity of nuclear systems, could result in a nuclear attack based on deceitful data, with repercussions that could be catastrophic not only for diplomatic relations, but for the world in general[102].

As much as specific applications are being developed and used in locating and targeting adversarial assets, apprehension rules the guarding and safety of nuclear systems, which might prove vulnerable to an attack by a much "stronger" AI-enabled system[103].

AI has also been developed in applications that simulate and thus study and give valuable knowledge on how nuclear systems operate. Being able to measure nuclear systems and their effects accurately without the need for actual nuclear testing is an exceptional innovation and extremely beneficial use of Artificial Intelligence, as the results can be used for increasing safety.

The gravity that the nuclear sector holds for nuclear states and their adversaries, worries about technological developments, along with the already mentioned lack of commonly adopted definitions on AI, renders cooperation AI-enabled nuclear capabilities even more unattainable. A three-step approach presented in "Artificial Intelligence and Stability in Nuclear Crises" by Marshall D. Foster in

[102] Pavel Sharikov (2018) Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination, Bulletin of the Atomic Scientists, 74:6, 368-373, DOI: 10.1080/00963402.2018.1533185

[103] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022]

order to preserve and not threaten nuclear stability is, firstly, enhance intelligence gathering methods on intentions and exact capabilities of an adversary, then limit any existing asymmetry of capabilities by the increase of the state's own ones and, finally, work towards building a framework that places controls and sets standards on AI in nuclear weapons[104]. If abode by, these measures could realistically present a solution to the threat of nuclear crisis.

In the words of Zachary Davis, author of "Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise", "*Close is not good enough when it comes to war, especially where nuclear risks are involved*".

11. Case studies

Project Maven, or else "the Algorithmic Warfare Cross-Functional Team", was a project by the United States Department of Defense, with the primary goal of locating the extremist fighters of the Islamic State (ISIL, Daesh). This was achieved by the automated analysis of up to 100,000 Facebook posts per day, with the help of Artificial Intelligence. This mission, along with other important results, was accomplished by AI-backed systems that managed and processed vast amounts of heterogeneous data, surveillance and intelligence, in order to track threats. This task would take even months for humans to complete, but with AI it is only a matter of minutes, or even seconds, to sort out the input and produce a recommended output[105].

[104] Foster, M., 2019. *Artificial Intelligence and Stability in Nuclear Crises*. [online] Usafa.edu. Available at: <https://www.usafa.edu/app/uploads/Space_Defense_Vol12_No01.pdf> [Accessed 16 September 2022

[105] Davis, Z., 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at:

In the United States and in the cyber and information field, the Air Force has been developing its **Advanced Display Core Processor** in avionics, able to process 87 billion instructions per second. Such a rapid data process procedure can lead to significant military advantages, both on the conventional battlefield, but mainly in cyberspace[106].

On the main part, the value of information about the Russian Federation was emphasized. A largely broadcasted topic from a few years ago was the **Russian involvement in the United States' presidential elections of 2016**, where the notion of information warfare was deeply understood. A wide range of proactive measures, including internet operations, were used by Russia to meddle in the U.S. election and, by extension, in its socio-political life. Russian information warfare affected the election process through two interconnected activities of intelligence agencies and affiliated organizations that occurred at the strategic, operational, and tactical levels, according to both theory and practice. Russian officials view democratic elections as a sociopolitical event that should be leveraged to advance Russia's geopolitical objectives in Western nations. Elections are a natural part of information warfare, which also involves disinformation, propaganda, lobbying, manipulation, controlled crisis, and blackmail, given what Russia has done thus far. The widespread use of media channels and other tactics to influence elections has a greater effect on people's consciousness and subconsciousness[107]. Between 2014 and 2017, Russian

<https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/>

[106] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

[107] Russian Interference in the U.S. Presidential Elections in 2016 and 2020 as an Attempt to Implement a Revolution-like Information Warfare Scheme (2021). Available at: https://warsawinstitute.org/russian-interference-u-s-presidential-elections-2016-2020-attempt-implement-revolution-like-information-warfare-scheme/ (Accessed: 20 September 2022)

military intelligence attempted to breach and get access to electoral infrastructure in each of the 50 states. Governmental Russian cyber attackers may have targeted networks connected to the Internet that deal with elections in 21 states. The first reported attack on State electoral infrastructure by Russian operatives during an election took place in Illinois in June 2016. On a website for the voter registry run by the Illinois Board of Elections, election clerks in Illinois noticed unusual network activity, notably a significant spike in outbound traffic. An FBI investigation discovered that 200,000 exfiltrated records, including details on each voter's name, address, social security number, birth date, and either a driver's license or other identification documents, were accessible to hackers thanks to SQL injection attacks. The hackers were able to add, access, update, change, or remove records from databases[108]. In addition, private Russian enterprises, like the Internet Research Agency, engaged in the enormous propaganda effort. Their staff presented themselves as American citizens, generating racially and politically divisive social media groups and pages, as well as created fake news articles but also commentary, in order to incite political animosity among the American people[109].

Taking a look into two historical case-studies related to nuclear weapon systems will aid in understanding the new aspect and gravity AI brings to the field. During the Soviet era, the **Soviet Union acquired ICBMs**, which are intercontinental ballistic missiles, primarily designed for nuclear weapons delivery[110]. As a

[108] Ibid

[109] How the Russian government used disinformation and cyber warfare in 2016 election – an ethical hacker explains (2018). Available at: https://theconversation.com/how-the-russian-government-used-disinformation-and-cyber-warfare-in-2016-election-an-ethical-hacker-explains-99989 (Accessed: 20 September 2022)

[110] Pike, J., 2022. *Intercontinental Ballistic Missiles*. [online] Federation of American Scientists. Available at: <https://nuke.fas.org/intro/missile/icbm.htm> [Accessed 16 September 2022]

counter-response, the USA actively sought to increase its own stockpile of ICBMs. This showcases that the USA did not pursue the development of an even more powerful technology, nor did it attack the Soviet Union. Instead, it embarked on a race of outnumbering the Union, preserving the at the time balance of power as it was. While Ronald Reagan was the United States' president, the country was holding an advantage in intelligence, surveillance techniques and counterforce strategies during the Cold War. The US were using surveillance technologies in submarines and other pioneer technological tools. This prevalence indicates just how competitors and adversaries may react when presented with such a strong technological advancement of another state. They might engage in the race themselves, change their methods of operations or/and develop new counter-technologies, so as to be relevant and become someone to be reckoned with.

The unforgettable **NATO intervention in Kosovo** showed another risk of using new technologies in the military practice. There, high-altitude bombing methods were used, meaning that the danger for NATO forces was limited, while the risk for civilians was augmented. And that is another challenge worth considering about the use of autonomous weapon systems, as it is reasonable that no government would want to take the decision of endangering an increasing number of human and civilian lives[111].

Generally speaking, the Middle East is an area where immeasurable AI-applications and technologies have been tested and employed first. In **Saudi Arabia**, **autonomous drones** have been exploited in a way that attack **oil installations**, critical to Middle Eastern's economy and survival. This is exactly

[111] Blanchard, A., Taddeo, M. Autonomous weapon systems and *jus ad bellum*. *AI & Soc* (2022). https://doi.org/10.1007/s00146-022-01425-y

what happened in 2019 in the country's town of Abqaiq, when the Saudi defense system was not able to halter the swarm drone attack that caused a loss of up to 5% of global production[112].

In the domain of **laser weapons**, **Turkey** seems to hold an advantage, as it has been proved in **Libya**. There and in 2019, Turkey, with its use of laser weapons, was able to target and shoot down the Chinese Wing Loong drone[113]. The ALKA directed-energy weapon system is a dual electromagnetic/laser weapon, yet it is not officially recognized that this was indeed the laser weapon system used in this case[114].

The Wing Loong drone shot down

Source:https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/turkey_uses_laser_weapon_technology_to_shoot_down_chinese_uav_wing_loong_ii_in_libya.html

[112] Husain, A., 2021. AI is Shaping the Future of War. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022

[113] Ibid

[114] *ALKA DIRECTED ENERGY WEAPON SYSTEM – Roketsan* (2022). Available at: https://web.archive.org/web/20200205165711/https://www.roketsan.com.tr/en/product/alka-directed-energy-weapon-system/ (Accessed: 18 September 2022)

In **Nagorno-Karabakh**, a disputed territory between Armenia and Azerbaijan, unprecedented AI-enabled tools have been observed and it may have indicated the end of conventional battlefield tactics and methods, as experts argued. In 2020 there were once again aggressions that led to war, with numerous casualties. Propaganda played its own role, with Azerbaijan's Border Patrol publishing a music video (!), promoting war and hatred for the enemy. In this video, Azerbaijan presented some of its latest and more than promising weaponized technologies. Trucks in the background are seen releasing and launching a loitering munition, the "Harop", manufactured by Israel Aerospace Industries (IAI), the country's major aerospace and aviation manufacturer. Its technology allows it to, after being launched, navigate towards an adversarial target, yet it can also wait and scan before hitting, flying autonomously for hours. When attacking, it hits directly, not by releasing a payload, but by hitting the target itself. This is why such attacks are called, as also mentioned again in this thesis, "kamikaze drones". Azerbaijan presented more than a glorified version for propaganda purposes; the country has been investing years and resources into loitering munitions' research and development. And while it ended up having 200 units across 4 different models, Armenia only had one and with limited capabilities. For these reasons, the Nagorno-Karabakh situation has been described as the first war won, in part, by autonomous weapon systems. The conflict also showed that, in order to win these weapons, you need these weapons[115].

[115] Deutschewelleenglish, director. How AI Is Driving a Future of Autonomous Warfare | DW Analysis. YouTube, YouTube, 25 June 2021, https://www.youtube.com/watch?v=NpwHszy7bMk. Accessed 20 Sept. 2022

 The Israeli-manufactured Harop in action in Azerbaijan

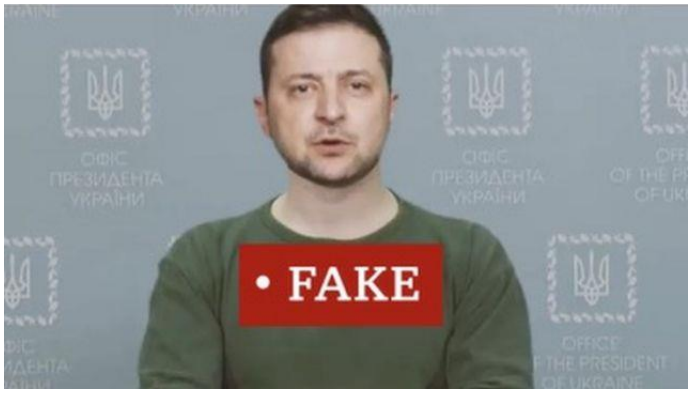
Source: https://www.youtube.com/watch?v=s1Z75jy5TGM&ab_channel=defenseupdate

Not all nations are ready to adapt to a practical level with these capabilities nor are regional and international organizations ready to address the issue with their framework. For Azerbaijan and the developments seen there, the report from the European Council on Foreign Relations stated that "*the advanced European militaries would perform badly against Azerbaijan's current UAS (unmanned aircraft systems)-led strategy"*[116].

Moving on to a more recent situation, the **Russian-Ukraine crisis of 2022**, we will now examine the use of deepfakes, as mentioned in the Definitions Chapter, and their role in the conflict. During the early stages of this war, particularly in March, a video portraying Ukraine's President Zelensky urging his country's population to put their arms down and, thus, surrender was published. It was a suspicious video, since the "president" was using stiff language and it was ultimately the reason it was considered fake. This was an amateur try; nothing however stops the creation of more technically intact videos and audios, with the multitude of real-speech data available, which Deep-Learning algorithms can be trained from and produce the desired outcome. This alarming event is indicative

[116] Husain, A., 2021. AI is Shaping the Future of War. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

of how indirectly offensive technologies can still be adversarial and create public turmoil[117].



Deepfake snapshot from the hacked website of Ukrainian TV network Ukrayina 24

These case studies might be too outdated, taking into consideration just how rapidly technology progresses and how many new capabilities appear. We may have to examine new factors, apart from the technologies themselves, such as questions about intentions that accompany their development and accession[118].

12. A technical consideration

As analyzed above, AI could prove more than beneficial at the operational level of war, with the processing of huge amounts of diverse data, presenting a variety of choices based on millions of facts to commanders. It is advocated, though, that it is safer and more efficient to do so with AI being a multitude made from smaller compounds into a bigger system. This opinion is supported on the following

[117] Centre for Emerging Technology and Security, 'The Information Battlefield: Disinformation, declassification and deepfakes', *CETaS Expert Analysis*, June 2022

[118] Foster, M., 2019. *Artificial Intelligence and Stability in Nuclear Crises*. [online] Usafa.edu. Available at: <https://www.usafa.edu/app/uploads/Space_Defense_Vol12_No01.pdf> [Accessed 16 September 2022]

basis: independently working parts lessens the chances and risks of the system totally collapsing, either due to a bug or a cyber-attack. As a result, the compounds engage with simpler tasks and deliver aggregated results[119].

13. Legal framework creation and relevant policies

With only debates and no international framework at hand, the present is marked by limited results for legal standards concerning AI weapons. In 2018, the United Nations Group of Governmental Experts, consisting of 25 member–states, set the question of the applicability of existing international laws to weaponized AI on the table and generally urged cooperation and escalation prevention. The outcome was a catholic agreement that the ultimate decision-making has to remain a human task on the battlefield and that ethics must be considered in AI employment, yet no agreement was accomplished for Lethal Autonomous Weapon Systems. In the same direction, however, and similarly limited, were the works of the United Nations since 2012, with the debates and conversations held at the United Nations Convention on Certain Conventional Weapons Group of Governmental Experts. Then, the nature and ethics of LAWS were discussed, following the United States executive order publication on them. Questions of responsibility and the imperative need for human control were reviewed, along with the greater question if LAWS and their use comply with the principles set by international humanitarian law and the existing conventions and treaties on the law of war. A basic worry was that this question was difficult and without an absolute answer, as LAWS and, generally new technologies, come with such novel and unexplored capabilities, that we cannot be sure that existing laws apply

[119] Steven I. Davis (2022) Artificial intelligence at the operational level of war, Defense & Security Analysis, 38:1, 74-90, DOI: 10.1080/14751798.2022.2031692

to them[120]. In August 2018, there was also a proposal by a coalition of Austria, Brazil and Chile for the establishment of a binding international organ with the mandate of LAWS, again focusing on human control and surveillance[121]. In the opposite direction, it should also be examined if non-offensive AI applications fall under war law provisions, as there exists the possibility that tools which are not weaponized affect offensive capabilities as much as weaponized ones and, as such, should be treated accordingly. In this direction, there are pivotal international humanitarian law provisions whose obligations have to be taken into account, such as Article 36 of the Additional Protocol I (API) to the Geneva Conventions. This article minimizes freedom of weapon and methods of warfare choice by a state, before deployment, through testing and cared for development. Besides referencing weapons, the review and consideration of the aforementioned tools will revolutionize and bring new meanings to the Protocol and new obligations to the states. This could actually be a realistic scenario, as the Protocol does not define, on purpose, the notion of weapons, means or methods of warfare, in order to be able to include future developments without updating the legal text. The same goes for cyber means, as per Rule 110 of the Tallinn Manual 2.0, which requires member states to legally review the "cyber means of warfare", thus the cyber offensive capabilities. Just like previously, indirect weaponized cyber means are being reviewed under the premise of being able to cause harm and damage[122].

[120] Pavel Sharikov (2018) Artificial intelligence, cyberattack, and nuclear weapons—A dangerous combination, Bulletin of the Atomic Scientists, 74:6, 368-373, DOI: 10.1080/00963402.2018.1533185

[121] Legal reviews of weapons, means and methods of warfare involving artificial intelligence: 16 elements to consider - Humanitarian Law & Policy Blog (2019). Available at: https://blogs.icrc.org/law-and-policy/2019/03/21/legal-reviews-weapons-means-methods-warfare-artificial-intelligence-16-elements-consider/ (Accessed: 17 September 2022)

[122] Shifting the narrative: not weapons, but technologies of warfare - Humanitarian Law & Policy Blog (2022). Available at: https://blogs.icrc.org/law-and-policy/2022/01/20/weapons-technologies-warfare/ (Accessed: 17 September 2022)

An interesting, as well as extremely important issue revolves around the framework on which autonomous (weapon) systems can be complied with. And that is because, while the main tendency is to associate AI offensive technologies with international humanitarian law and the law of armed conflict, yet their norms are actually allowing many more hostilities, destruction and death, as opposed to international human rights law[123]. Therefore, an assessment of intentions has to be decided upon before drafting the relevant provisions and principles.

Carayannis and Draper, in their "Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence", argue that the solution for stability preservation lies in the adoption of a Universal Global Peace Treaty, along with a Convention on Cyberweapons and Artificial Intelligence. In their research paper, they also mention other members of the scientific community that support such a legal measure. Ramamoorhtly and Yampolskiy (2018) suggest a comprehensive UN-backed Benevolent Artificial General Intelligence Treaty, aiming at allowing the development of only beneficial and *"altruistic"* Artificial Super Intelligence. Turchin et al. (2019), as they mention, are also in favor of global standards and norms being set and, more specifically, review the possibilities of either a total ban on ASI through a global treaty, a one-ASI solution or a net of ASIs solution that would include inter-policing among them and, finally, augmented human intelligence[124].

[123] Legal reviews of weapons, means and methods of warfare involving artificial intelligence: 16 elements to consider - Humanitarian Law & Policy Blog (2019). Available at: https://blogs.icrc.org/law-and-policy/2019/03/21/legal-reviews-weapons-means-methods-warfare-artificial-intelligence-16-elements-consider/ (Accessed: 17 September 2022)

[124] Carayannis, E.G., Draper, J. Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence. AI & Soc (2022). https://doi.org/10.1007/s00146-021-01382-y

Apart from discussions on such an official level, it is noteworthy that even the technological colossus of Google has itself published a series of principles regarding AI and its use, which apply to the military use of AI, as well. Among these are the use of AI for beneficial purposes, eliminating human bias in programming, the importance of testing before employing a technology, as well as accountability towards people[125].

Weaponized Artificial Intelligence, able to enable automated hits, has to be addressed by an international legal document, binding in nature, such as an international treaty. Voting in favor, adopting and ratifying a treaty means an expressed preference by the states for a long-term adherence to a set of common rules and restrictions, towards preserving peace. The content of such a treaty definitely has to set some minimum norms of practice in relation to AI systems, but also address and safeguard human rights through international humanitarian law and, perhaps, consider the introduction of a new international body in charge of the treaty's obligations' supervision. All of this has to happen after a total revisal of up-to-today used terms, notions and beliefs, as new technologies have to comply to a newly structured legal and ethical framework. Ensuring that any weapon or weaponized AI-enabled technique will be examined as to its legal compliance before development is pivotal for the sake of stability. Restrictions in the use of weaponized technology would ultimately mean less GDP spent on military operations and more funding available for critical domains, such as health and education[126].

[125] Ai.google. Available at: https://ai.google/principles/ (Accessed: 15 September 2022)

[126] MacDonald, N. and Howell, G., 2019. Killing Me Softly: Competition in Artificial Intelligence and Unmanned Aerial Vehicles. [online] JSTOR. Available at: <https://www.jstor.org/stable/26864279> [Accessed 6 September 2022

The principal complication with setting common rules is the distinctive opinions around AI, technology in general, and its use, as each country presents a different point of view depending on the goals it wants to serve. Different opinions hinder legal universality. For example, the United States have some clear-cut thinking, one however that seems rather contradicting, and that has been expressed during the works of various fora, such as the United Nations Convention on Certain Conventional Weapons. More specifically, despite claiming a position that seemed to be favoring that the ultimate decision must be taken by a human when it came to the use of lethal force by a machine, they also asserted that not every firing decision is to be taken by humans, rather that the systems should act according to "*reasoned human decision-making".* This was supported by the following US interpretation of humanitarian law: "*International humanitarian law does not require that a weapon determine whether the target is a military objective, rather that the weapon be capable of being employed consistent with the principle of distinction by a human operator"*[127]. There exists, however, no technology so advanced today, that it is able to conduct human-like thought processing and take human-like decisions. And, besides that, it seems irrational wanting to replace everything with a super-intelligence, especially in a field so critical and frail as the military in times of crisis. Developing human-thinking capabilities and consciousness will cost millions and, at the end of the day, it would not serve any imperative needs; experts should then ideally focus on automating otherwise time-consuming or harmful and potentially lethal tasks for humans.

With the aim of setting a primary, binding legal ground of AI deployment in a militarized context, arms control and verification procedures, unilateral

[127] Ray, B., Forgey, J. and Mathias, B. (2020) *Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions*, *DTIC*. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

international measures are vital for a stabilized international world, rather than a technologically competitive arena. Nevertheless, it is more than clear-cut that such a novel situation requires a search for an innovative and more than adequate legal framework, with approaches much different to the ones used when addressing matters concerning conventional weapons used up until now. Furthermore, technology is always in a race with itself, continuously and rapidly evolving. Thus, a framework able to catch up with advancements, without the need for constant updates and discussion, is also imperative. Such a framework has to take into consideration the capabilities that AI-enhanced conventional weapons present, their correlation with nuclear systems, as well as the role of information and its use in conventional or/and cyber battlefields[128].

Should AI technology in weapons systems or some specific types (eg. LAWS) be restricted or completely prohibited (total ban)? The opinion of this thesis' author is that we can neither halter nor prohibit the development or use of a technology and tool that is already out there, being used and advanced. When offensive AI-enabled capabilities are already a part of national agendas, we simply cannot expect states to give up their work and already distributed funding. Even if states officially agreed on such an agreement, the threat caused by the uncertainty of another state keeping up with developing weaponized technologies, would mean the practical continuation of the race.

Especially when it comes to nuclear security, a top priority as it is, the major nuclear powers have to come to the table and agree on commonly adopted norms and binding principles of practice; the direction should always be safeguarding NC3 systems, preventing a nuclear crisis at all costs and comply with explicit

[128] Johnson, J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age," European Journal of International Security. Cambridge University Press, 7(3), pp. 337–359. doi: 10.1017/eis.2021.23

uses of technology in this field, all embodied within a consistent and mandatory framework of international law. To be more specific, it is within the mandate of the United Nations Convention on Certain Conventional Weapons, under the auspices of the UN Conference on Disarmament or the DISEC Committee, to regulate discussions and papers on the matter.

With such a technical matter at hand, any solution has to incorporate both the political, but also the technological part. Policymakers should work closely with technology experts, who are the ones with the actual knowledge on how these systems function and what they are able to accomplish. In order to achieve even broader safety standards, coalitions of countries should use the same international teams of experts who will operate under the same guidelines and norms, so that uniformity is achieved.

It is certain that offensive and defensive technological skills are being developed in parallel, in a constant race to catch up and surpass each other. Hence, a viable answer to this situation that can address and prevent a crisis or/and a conflict would be collaboration on research and analysis; a coalition for the development of AI defence capabilities would create a common threshold of beneficial AI use, strategic alliances and investment partnerships[129]. Such initiatives currently exist, yet in a limited context. For example, the Defense Technology and Trade Initiative between USA and India on UAV swarm developments, focuses on the aforementioned goal: retreating from the "buyer-seller" approach and

[129] MacDonald, N. and Howell, G., 2019. Killing Me Softly: Competition in Artificial Intelligence and Unmanned Aerial Vehicles.. [online] JSTOR. Available at: <https://www.jstor.org/stable/26864279> [Accessed 6 September 2022]

emphasizing on technological collaboration, mutual production and development[130].

The US Department of Defense has suggested, with is 3000.09 Instruction that it is the commander of an autonomous weapon and the government the ones that should hold accountability for their behavior when in use. As the Instruction indicates, the operation of an autonomous weapon must be completed "*in a timeframe consistent with commander and operation intentions and, if unable to do so, terminate engagements or seek additional human operator input before continuing the engagement".* This American guideline may affect the questions and relevant debates on legal issues of responsibility and pave the way for a broader, multinational agreement on it.

Most of the time, the law follows logic and this should be the case for the legal framework around AI and autonomous systems and weapons in the military. Logic indicates that when a soldier, a commander or another person is in charge of an AI system and takes a decision or issues an order based on the AI's suggestions, they therefore accept and choose it and, consequently, accept liability from it, shall an unfavorable outcome arise. In order to fairly judge the person in charge, however, the law has to distinguish and define the lines between accidental malfunction of the machine, prediction and acceptance of an unfavorable result from the commander or the soldier and, finally, deliberate action. Consequences and sanctions have to vary accordingly[131].

[130] Webmaster, O. (2022) IC - US | India Defense Technology and Trade Initiative, Acq.osd.mil. Available at: https://www.acq.osd.mil/ic/dtti.html (Accessed: 7 September 2022)

[131] Blanchard, A., Taddeo, M. Autonomous weapon systems and *jus ad bellum*. *AI & Soc* (2022). https://doi.org/10.1007/s00146-022-01425-y

Foremost, however, should be the fact that weaponized systems have to be legally classified as a means of ultimate resort *(ultimum refugium*). This provision complies with major principles of international law, such as the principle of proportionality, explained above. Differently put, other means have to be exhausted first before deciding to engage with autonomous weapon systems, AI capabilities and applications. Diplomatic dialogue has to remain the first and major tool for resolving conflict.

No matter the accomplishment of an international treaty or not, AI and cyber offense will continue to grow regardless. Hence, with technology advancing expeditiously, AI and cyber defence must progress accordingly, to prevent precarious and perilous prospects. In this way, the race that has been mentioned in this thesis so many times will be ongoing, but for a beneficial intention. And, for stability to be maintained, states have to keep transparency in their work, acquisition and intentions on AI deployment.

14. Future prospects and possibilities

Forecasting a situation as fragile as the political field with its surrounding conflicts is difficult as it is. But it is needless to say that, not within an extended period of time, regional stability and security, as well as the indispensable diplomatic relations that follow the aforementioned, will be affected and reshaped by AI progress, adoption and practice in the military field.

Currently, it is the United States that have a typical superiority on the matter and, logically, this indicates that Russia and China will remain behind and, maybe, left behind for good. It is left to be seen how they will react to such a scenario and

whether they will choose to showcase their capabilities by forming an escalation policy, the use of their own powerful systems or even with the use of nuclear power.

With countries developing distinct theories and practices in military AI and with the need for being the most technologically advanced and prepared turning into a race, both the essence of war and conflict, but also the balances of power change. In this risky new mise en scène, where no previous history can teach us how to act, some things must remain steady and guide all actions taken. One of these is deterrence, abstaining from actions that can lead to a conflict, a condition that can be reinforced by increasing incentives for abstinence, especially through strengthened alliances and cooperations on common technological research and innovation. Abstinence from adversarial AI use and notably nuclear deterrence will prove extremely beneficial in the ever-changing strategic environment of today and tomorrow. AI applications and uses that are primarily developed for beneficial uses give hope that stability will continue to prevail. Because, in any case, advantages in individual systems may offer temporary dominance to one nation, but definitely not lasting authority.

According to the opinion of Amir Husain, author of "AI is Shaping the Future of War", Artificial Intelligence will play the following four roles in the near future; Firstly, it will automate the process of strategic planning. Secondly, it will transform sensor technology, through fusing and interpreting signals in a much more efficient and rapid way. Thirdly, it will alter space-based systems,

especially in information fusion. Finally, and more importantly, it will empower the next generation of cyber (and information) warfare competences[132].

15. Conclusion

Above all, according to the author of this thesis, it is imperative that AI does not reach the point where it totally substitutes human presence and decision-making on the military battlefield, whether that be the conventional or the cyber one. And that is mentioned because human control over AI is most prevalent at its initial development stages, whereas it begins to fade away as much as autonomy is obtained[133].

Today, the principal need is found in a focused discussion on the specific characteristics and technicalities of AI weaponized technology, so that every part clarifies the intentions and points of view of the others. Artificial Intelligence and related technologies, such as Machine and Deep Learning, present the military with too many capabilities to prohibit their holistic adoption and use, therefore the basis of negotiation has to start from the point of indented uses rather than a prohibition that would be unrealistic, since these capabilities are already being available out there.

[132] Husain, A., 2021. AI is Shaping the Future of War. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022]

[133] Carayannis, E.G., Draper, J. Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence. AI & Soc (2022). https://doi.org/10.1007/s00146-021-01382-y

Today's conflicts that older generations were used to are evidently far, further away from the conventional battlefield. Now, the battlefield is, most of the time (not all times, as reality has proven in 2022 in Europe), unlikely and the ultimate war is being conducted through the manipulation, deceit and exploitation of cyber systems. Even on the conventional battlefield, more and more autonomous systems are starting to replace human soldiers and conduct tasks in a much more efficient and rapid way. It comes, then, with no surprise that any future large-scale war will actually be over in a few minutes or less, as many scholars argue, as it will take place in cyberspace and its goal will be taking over critical cyber or nuclear control and command systems of a nation or a coalition of states[134]. Nevertheless, first-mover is not always an advantage here. Quoting the words of Paul Schare of "Robotics on the Battlefield", "*The winner of this revolution will not be who develops these technologies first, or even who has the best technologies, but who figures out who to best use them"*[135].

Bibliography and references

1. Ai.google. Available at: https://ai.google/principles/ (Accessed: 15 September 2022)

2. Algorithmic Warfare or Algorithmic Warfare and Focal Point Analysis | Small Wars Journal (2022). Available at:

[134] Rod Thornton & Marina Miron (2020) Towards the 'Third Revolution in Military Affairs', The RUSI Journal, 165:3, 12-21, DOI: 10.1080/03071847.2020.1765514

[135] Joint Concept Note 1/18, HumanMachine Teaming (London: United Kingdom Ministry of Defence, May 2018), iii, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/709359/20180517-concepts_uk_human_machine_teaming_jcn_1_18.pdf

https://smallwarsjournal.com/jrnl/art/algorithmic-warfare-or-algorithmic-warfare-and-focal-point-analysis (Accessed: 20 September 2022)

3. ALKA DIRECTED ENERGY WEAPON SYSTEM – Roketsan (2022). Available at: https://web.archive.org/web/20200205165711/https://www.roketsan.com.tr/en/product/alka-directed-energy-weapon-system/ (Accessed: 18 September 2022)

4. Andrei Ilnitsky and Aleksandr Losev 'Iskusstvennyy Intellekt – Eto i Riski i Vozmozhnosti' ['Artificial Intelligence – Here Are the Risks and Opportunities'] Krasnaya Zvezda [Red Star] 24 June 2019 accessed 15 September 2022

5. Autonomous Robots and the Future of Just war Theory 1 (2013) pp. 338-351. Available at: https://www.taylorfrancis.com/chapters/edit/10.4324/9780203107164-37/autonomous-robots-future-war-theory-1-keith-abney (Accessed: 17 September 2022)

6. Blanchard A. Taddeo M. Autonomous weapon systems and jus ad bellum. AI & Soc (2022). https://doi.org/10.1007/s00146-022-01425-y

7. Carayannis E.G. Draper J. Optimising peace through a Universal Global Peace Treaty to constrain the risk of war from a militarised artificial superintelligence. AI & Soc (2022). https://doi.org/10.1007/s00146-021-01382-y

8. Centre for Emerging Technology and Security 'The Information Battlefield: Disinformation declassification and deepfakes' CETaS Expert Analysis June 2022

9. Davis Z. 2019. Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. [online] National Defense University Press. Available at: <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1979401/artificial-intelligence-on-the-battlefield-implications-for-deterrence-and-surp/> [Accessed 10 September 2022]

10. Davison N. (2022) A legal perspective: Autonomous weapon systems under international humanitarian law | United Nations iLibrary Un-ilibrary.org. Available at: https://www.un-ilibrary.org/content/books/9789213628942c005 (Accessed: 19 September 2022)

11. Defence Artificial Intelligence Strategy (2022). Available at: https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy (Accessed: 11 September 2022)

12. Deutschewelleenglish director. How AI Is Driving a Future of Autonomous Warfare | DW Analysis. YouTube YouTube 25 June 2021 https://www.youtube.com/watch?v=NpwHszy7bMk. Accessed 20 Sept. 2022

13. Forrest E. Morgan Karl P. Mueller et al. “Dangerous Thresholds: Managing Escalation in the 21st Century (Santa Monica CA: Rand Cooperation 2008) p. 8.

14. Foster M. 2019. Artificial Intelligence and Stability in Nuclear Crises. [online] Usafa.edu. Available at: <https://www.usafa.edu/app/uploads/Space_Defense_Vol12_No01.pdf> [Accessed 16 September 2022]

15. Gain N. (2020) NAVAIR progressing towards LRASM integration on P-8A MPA - Naval News Naval News. Available at: https://www.navalnews.com/naval-news/2020/05/navair-progressing-towards-lrasm-integration-on-p-8a-mpa/ (Accessed: 6 September 2022)

16. Harding T. 2022. Russia's KUB-BLA kamikaze drone intercepted in Ukraine. [online] The National News. Available at: <https://www.thenationalnews.com/world/uk-news/2022/03/14/russias-kub-bla-kamikaze-drone-intercepted-in-ukraine/> [Accessed 15 September 2022]

17. Horowitz M. (2018) Artificial Intelligence International Competition and the Balance of Power - Texas National Security Review Texas National Security Review. Available at: https://tnsr.org/2018/05/artificial-intelligence-

international-competition-and-the-balance-of-power/ (Accessed: 16 September 2022)

18. How the Russian government used disinformation and cyber warfare in 2016 election – an ethical hacker explains (2018). Available at: https://theconversation.com/how-the-russian-government-used-disinformation-and-cyber-warfare-in-2016-election-an-ethical-hacker-explains-99989 (Accessed: 20 September 2022)

19. Husain A. 2021. AI is Shaping the Future of War. [online] Ndupress.ndu.edu. Available at: <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-3/prism_9-3_50-61_Husain.pdf?ver=7oFXHXGfGbbR9YDLrnX3Fw%3D%3D> [Accessed 18 September 2022

20. Intelligent design: inside France's €1.5bn AI strategy - Global Defence Technology | Issue 88 | June 2018 (2022). Available at: https://defence.nridigital.com/global_defence_technology_jun18/intelligent_design_inside_frances_15bn_ai_strategy (Accessed: 19 September 2022)

21. Johnson J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age" European Journal of International Security. Cambridge University Press 7(3) pp. 337–359. doi: 10.1017/eis.2021.23

22. Johnson J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age" European Journal of International Security. Cambridge University Press 7(3) pp. 337–359. doi: 10.1017/eis.2021.23

23. Johnson J. (2022) "Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age" European Journal of International Security. Cambridge University Press 7(3) pp. 337–359. doi: 10.1017/eis.2021.23.)

24. Joint Concept Note 1/18 HumanMachine Teaming (London: United Kingdom Ministry of Defence May 2018) iii available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/709359/20180517-concepts_uk_human_machine_teaming_jcn_1_18.pdf

25. Kietzmann J. et al. (2020) "Deepfakes: Trick or treat?" Business Horizons 63(2) pp. 135-146. doi: 10.1016/j.bushor.2019.11.006

26. Layton P. (2018) "Algorithmic Warfare: Applying Artificial Intelligence to Warfighting" Air Power Development Centre p. Available at: https://www.academia.edu/36620913/Algorithmic_Warfare_Applying_Artificial_Intelligence_to_Warfighting (Accessed: 20 September 2022)

27. Left of Launch – Missile Defense Advocacy Alliance (2022). Available at: https://missiledefenseadvocacy.org/alert/3132/ (Accessed: 5 September 2022)

28. Legal reviews of weapons means and methods of warfare involving artificial intelligence: 16 elements to consider - Humanitarian Law & Policy Blog (2019). Available at: https://blogs.icrc.org/law-and-policy/2019/03/21/legal-reviews-weapons-means-methods-warfare-artificial-intelligence-16-elements-consider/ (Accessed: 17 September 2022)

29. Lethal Autonomous Weapons Systems: Recent Developments (2019). Available at: https://www.lawfareblog.com/lethal-autonomous-weapons-systems-recent-developments (Accessed: 19 September 2022)

30. M.T. Kłoda Stany Zjednoczone Ameryki: przegląd projektów prawa stanowego USA dotyczących badań nad wykorzystaniem technologii blockchain w elekcjach państwowych „Przegląd Sejmowy" 2020 No. 4 (59) pp. 252–253

31. MacDonald N. and Howell G. 2019. Killing Me Softly: Competition in Artificial Intelligence and Unmanned Aerial Vehicles.. [online] JSTOR.

Available at: <https://www.jstor.org/stable/26864279> [Accessed 6 September 2022]

32. Machi V. 2022. France approves final phase of Artemis big-data processing platform. [online] Defense News. Available at: <https://www.defensenews.com/global/europe/2022/07/11/france-approves-final-phase-of-artemis-big-data-processing-platform/> [Accessed 19 September 2022]

33. Pavel Sharikov (2018) Artificial intelligence cyberattack and nuclear weapons—A dangerous combination Bulletin of the Atomic Scientists 74:6 368-373 DOI: 10.1080/00963402.2018.1533185

34. Petrella S. Miller C. and Cooper B. (2021) "Russia's Artificial Intelligence Strategy: The Role of State-Owned Firms" Orbis 65(1) pp. 75-100. doi: 10.1016/j.orbis.2020.11.004

35. Pike J. 2022. Intercontinental Ballistic Missiles. [online] Federation of American Scientists. Available at: <https://nuke.fas.org/intro/missile/icbm.htm> [Accessed 16 September 2022]

36. Pistono F. & Yampolskiy R. V. (2016). Unethical Research: How to Create a Malevolent Artificial Intelligence. arXiv. https://doi.org/10.48550/arXiv.1605.02817

37. Ray B. Forgey J. and Mathias B. (2020) Harnessing Artificial Intelligence and Autonomous Systems Across the Seven Joint Functions DTIC. Available at: https://apps.dtic.mil/sti/citations/AD1104964 (Accessed: 13 September 2022)

38. Rod Thornton & Marina Miron (2020) Towards the 'Third Revolution in Military Affairs' The RUSI Journal 165:3 12-21 DOI: 10.1080/03071847.2020.176551

39. Russian Interference in the U.S. Presidential Elections in 2016 and 2020 as an Attempt to Implement a Revolution-like Information Warfare Scheme (2021).

Available at: https://warsawinstitute.org/russian-interference-u-s-presidential-elections-2016-2020-attempt-implement-revolution-like-information-warfare-scheme/ (Accessed: 20 September 2022)

40. SABAH D. (2021) Turkey's Baykar to mass produce Akıncı UCAV soon Daily Sabah. Available at: https://www.dailysabah.com/business/defense/turkeys-baykar-to-mass-produce-akinci-ucav-soon (Accessed: 8 September 2022)

41. Shifting the narrative: not weapons but technologies of warfare - Humanitarian Law & Policy Blog (2022). Available at: https://blogs.icrc.org/law-and-policy/2022/01/20/weapons-technologies-warfare/ (Accessed: 17 September 2022)

42. Steven I. Davis (2022) Artificial intelligence at the operational level of war Defense & Security Analysis 38:1 74-90 DOI: 10.1080/14751798.2022.2031692

43. Trevithick J. (2020) Here Is What Each Of The Pentagon's Air-Launched Missiles And Bombs Actually Cost The Drive. Available at: https://www.thedrive.com/the-war-zone/32277/here-is-what-each-of-the-pentagons-air-launched-missiles-and-bombs-actually-cost (Accessed: 6 September 2022)

44. US Navy funds LRASM integration onto P-8A Poseidon MPA (2021). Available at: https://defbrief.com/2021/04/22/us-navy-funds-lrasm-integration-onto-p-8a-poseidon-mpa/ (Accessed: 6 September 2022)

45. Webmaster O. (2022) IC - US | India Defense Technology and Trade Initiative Acq.osd.mil. Available at: https://www.acq.osd.mil/ic/dtti.html (Accessed: 7 September 2022)

46. Woolf A. 2022. Russia's Nuclear Weapons: Doctrine Forces and Modernization. [online] Congressional Research Service Reports. Available at:

<https://crsreports.congress.gov/product/pdf/R/R45861> [Accessed 16 September 2022]

47. Yen Koh T. n.d. Intelligent Machines vs. Human Intelligence. [online] Ebsco.com. Available at: <https://www.ebsco.com/apps/landing-page/assets/POVRC_Intelligent_Machines_vs_Human_Intelligence.pdf> [Accessed 19 September 2022]