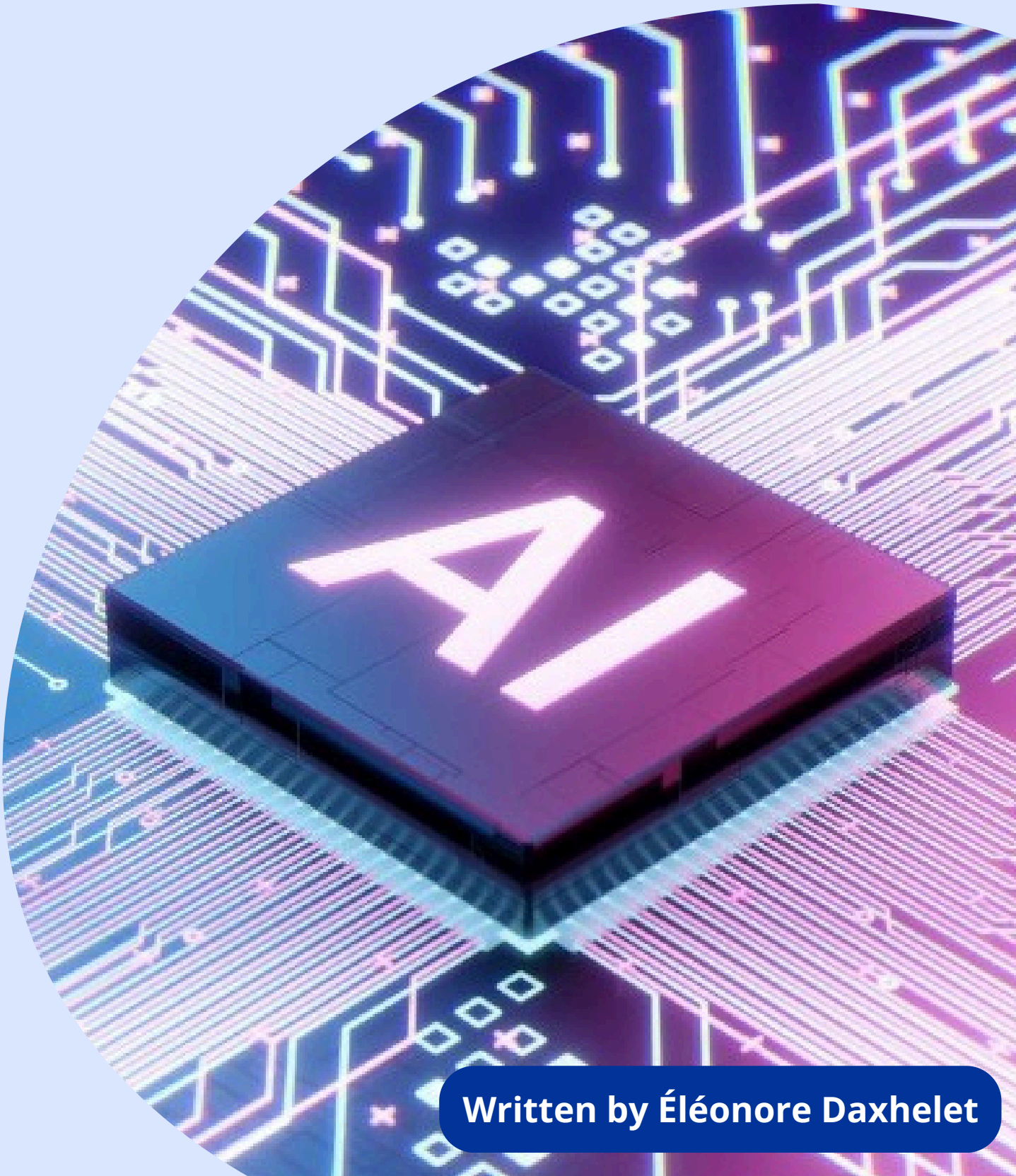
Food For Thought 2023

Artificial Intelligence and the Future of Warfare

FINABEL - The European Land Force Commanders Organisation

AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953



Written by Éléonore Daxhelet

Written by Éléonore Daxhelet
Supervised by Ginevra Bertamini

This Food For Thought paper is a document that gives an initial reflection on the theme. The content is not reflecting the positions of the member states but consists of elements that can initiate and feed the discussions and analyses in the domain of the theme. All our studies are available on www.finabel.org

Director’s Editorial

As the managing director of Finabel, it is my privilege to present this strategic analysis of "Artificial Intelligence and the Future of Warfare" by Éléonore Daxhelet. In an era where technological advancements rapidly transform every facet of our operational environment, the defense sector is no exception. This paper examines the profound impacts that Artificial Intelligence (AI) is poised to have on modern warfare, with a particular focus on its applications in cyber warfare, military operations, and the broader geopolitical landscape.

AI's integration into military strategies signifies a paradigm shift. Its capacity to process vast amounts of data, facilitate rapid decision-making, and enhance operational efficiency introduces both unprecedented opportunities and challenges. This duality is a recurring theme throughout the paper, reflecting the complex nature of AI technologies that can simultaneously act as powerful force multipliers for defense and potential instruments of offense.

The paper starts by defining AI and exploring its applications in cyber warfare, highlighting both offensive and defensive AI. It then transitions into discussing AI's role in military operations, from enhancing tactical decisions to the deployment of unmanned systems. The geopolitical implications of AI, particularly its potential to incite a new arms race, are critically examined, along with the ethical considerations that must guide its development and deployment.

Our aim at Finabel is to develop a nuanced understanding of these emerging technologies and their implications for military strategy and international security. This paper underscores that mission, offering valuable insights into how AI can shape the future battlespace while emphasizing the need for careful and ethical integration of these technologies.

I extend my gratitude to Éléonore Daxhelet for her meticulous research and analysis. It is my expectation that this paper will serve as a vital resource for military professionals, policymakers, and scholars as we navigate the complexities of AI in the defense sector.

Sincerely,

Mario Blokken

Director

TABLE OF CONTENTS

Introduction

The field of Artificial Intelligence (AI) is evolving quickly. New artificially intelligent technologies are being developed continuously, and sometimes they can be ground-breaking. These technologies are increasingly incorporated into diverse aspects of everyday life and are becoming crucial for commercial, economic and scientific development and innovation. It is not surprising that the defence sector is also seeking to take advantage of AI and introduce these new technologies into the security arena. As explained by Murugesan (2022, p. 4), AI can be used, among other things, "for repetitive tasks to free up security staff for projects that require human ingenuity." Furthermore, testifying to the benefits of AI, "NATO Member States have already started to invest in this technology and have incorporated it in their defence strategy" (Carlo, 2021, p. 269).

Despite its benefits, AI is expected to bring "dramatic changes in the strategy, operational art, tactics and doctrines of the warring sides" (Ploumis, 2022, p. 1). On this line, changes need to be carefully considered and studied to prevent the risks they could engender. For example, AI technologies "have a substantial impact on cyber warfare, but could have an adverse effect and significantly increase the number and threat level of cyber-attacks in the future" (Kline et al., 2019).

AI systems are thus expected to impact "the conduct of warfare, bring new capabilities into being, and alter power equations" (Singh Gill, 2019, p. 169). Drawing from these assumptions, this paper aims to study how AI can impact the nature of conflicts. In particular, the paper seeks to better understand the benefits and risks associated with the introduction of AI technologies in the security sector for military joint operations, considering technological compatibility and ethical considerations. How do developments of Artificial Intelligence Systems in the defence sector affect military cooperation? What are the benefits and risks associated with the inclusion of Artificial Intelligence in the defence sector?

What is Artificial Intelligence?

Before exploring in more detail the core questions of this paper, there is a need to define the main concept which is the focus of this research: Artificial Intelligence. Defining AI is a challenging task. There is indeed "no widely accepted definition of Artificial Intelligence" (Wang, 2019, p. 1).

Broadly defined, AI is "the science and engineering of making intelligent machines, especially intelligent computer programs" (McCarthy, 2007, p. 2). It refers to a set of techniques and distinct disciplines, such as "machine learning, computer vision, natural language processing (NLP), deep learning and cognitive computing" (Carlo, 2021, p. 270), with the particular goal "of developing systems endowed with the intellectual processes characteristic of humans" (Copeland, 2023).

At the heart of the definition of AI lies thus the notion of 'intelligence'. Struggles to properly define the former comes primarily from a lack of universal definition for the latter (Wang, 2019). The definition of AI also changes according to the aim of each research project. Therefore, each of "the different working definitions of AI correspond to not only different ways to abstract from human intelligence but also different expectations about the destination of this research" (Wang, 2019, p. 14). Many types of AI therefore exist. However, they all have the ultimate objective "to make computer programs that can solve problems and achieve goals in the world as well as humans" (McCarthy, 2007, p. 5).

As per Forrest et al. (2020, p. 9), the Defense Science Board's Summer Study on Autonomy in 2016 endorsed the prevailing definitions, stating that AI pertains to "the capacity of computer systems to execute tasks that typically necessitate human intelligence." However, this definition might describe different computer programmes across time. AI as a field of academic study has been around since the 1950s, but its roots go back to the 1940s (Haenlein & Kaplan, 2019, p. 5).

During the early stages of computer development, the tasks accomplished by computers were focused on replacing human intelligence through computer programs. However, in the present day, many of these tasks, such as calculations, have become routine for computers and are no longer considered as necessitating human intelligence. Consequently, some computer programs once considered as 'intelligent' are no longer classified as such due to the evolution of technology, in the idea that "what may now seem a 'revolutionary' technology will eventually become the new 'conventional'" (Kello, 2013, p. 38). In brief, the interpretation of tasks demanding human intelligence shifts as they are substituted by computers to the extent that it becomes customary.

Given the diversity of definitions and the variety of AI systems, in this document, a machine will be considered intelligent based on the results of its behaviour (Kaloudi & Li, 2020, p. 29). Therefore, AI will be here defined as "a system's ability to interpret external data correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation" (Kaplan & Haenlein, 2019 IN: Haenlein & Kaplan, 2019, p. 5). This definition offers indeed practicality and adaptability by capturing AI's dynamic problem-solving capabilities and accommodating evolving technological advancements.

Structure of the Paper

Having addressed the issue of defining AI, this paper will then seek to discuss the many implications of the inclusion of AI technologies in the defence sector. What are the benefits and drawbacks of military AI applications? What are the security consequences of AI? To answer these important questions, this paper is divided into four main parts.

The first section addresses the issue of cyberwarfare. It focuses on the impact of AI on cyber security. After defining the concept of cyber warfare and explaining the relevance of the topic, two main applications of AI will be analysed according to their main objective: offensive and defensive AI. The first aims at improving cyber-attacks, while the second aims at enhancing the defence capabilities of a particular actor in cyberspace.

The second section focuses on the application of AI in the physical space. AI can bring significant tactical benefits to military operations on the field in the form of surveillance, reconnaissance and improved organisation. AI can also be implemented in unmanned systems and vehicles, also known as drones and robots. However, it is not without risk, as AI systems are not infallible and can be the target of cyber-attacks, encompassing serious consequences for military operations.

The third section analyses the geopolitical impact of AI. This technology provides major strategic advantages to state actors. These benefits attract them towards increasing investment in AI and strengthen its inclusion in their defence capabilities. This runs the risk of sparking a new arms race, weaponising AI technologies. The inclusion of AI systems in the defence sector also bears challenges for military cooperation, especially in terms of technological compatibility. Finally, the last section will conclude by tackling the main ethical considerations of the inclusion of AI in the security sector.

AI and Cyberwarfare

What is Cyberwarfare?

In an era defined by interconnectedness and digital dependency, the emergence of cyberwarfare has introduced a new dimension of conflict where battles are fought not only on physical battlefields but in the vast expanse of cyberspace too. Since the popularisation of the Internet in the 1990s, the virtual space has grown into a new international space. In contrast to other recognised international spaces, the definition of cyberspace is still being developed (Barnard-Wills & Ashenden, 2012, p. 112). The situation is further complicated by the nature of cyberspace, as it is undergoing unprecedented, rapid and constant evolution (Barnard-Wills & Ashenden, 2012, p. 117). Unlike air, land, sea and space, cyberspace is a man-made dimension with its own characteristics, offering new opportunities and challenges (Lehto, 2018).

Accordingly, the development of cyber technologies has, through their interconnectivity, eroded the presence of well-defined digital boundaries, forcing nations to rethink traditional notions of territoriality online. Consequently, the imperative to oversee and regulate this dynamic sphere extends globally. This need is accentuated by the worrisome trend of individuals, subnational entities, and governments exploiting cyberspace for potentially destructive pursuits in order to advance their interests (Reveron, 2012). In brief, it is evident that cyberspace is quickly developing into a contemporary battleground (AL-Durrah & Sadkhan, 2021). However, the precise contours of the definition of cyberwarfare remain the subject of ongoing scholarly debate. The absence of a generally acknowledged interpretation of cyber warfare is evident in the literature and underscored by several scholars (Lehto, 2018; AL-Durrah & Sadkhan, 2021).

Assuming that war is invariably extensive and includes all types of warfare, cyberwarfare can be broadly understood as "one form of waging war, used alongside kinetic attacks" (Lehto, 2018, p. 3). Its distinctive feature is that it is conducted in the virtual domain. More specifically, cyberwarfare can be defined as "a digital attack orchestrated by a state or government with the intention of damaging computer systems and networks, committing acts of espionage, or mangling the critical infrastructure of an adversary or ally" (Kline et al., 2019). Cyber operation, therefore, entails the use of digital tools and technologies to launch strategic attacks on a nation's critical infrastructure, information systems, or even its socio-political fabric. It is, in sum, a "politically motivated hacking for sabotage and espionage" (AL-Durrah & Sadkhan, 2021, p. 125).

As this concept continues to evolve, it underscores the need to re-evaluate traditional notions of warfare and security in an increasingly interconnected world. Cyberattacks not only pose a threat to the military but also to society's vital functions (Lehto, 2018). Moreover, because of the low costs of entering the cyberspace and the difficulty of attributing an attack, anyone has the possibility to affect a state's security and cause widespread harm (Lehto, 2018). In an unprecedented manner, cyberattacks have granted state and non-state actors the ability to exert influence at the international level (Kello, 2013). As such, "cyber warfare may be the greatest threat that nations have ever faced" (Lehto, 2018, p. 5).

While cyberattacks do not fundamentally change the nature of warfare, they have enabled non-traditional actors to cause significant economic and social damage, thereby raising important new security concerns (Kello, 2013). These concerns are even more troubling considering defensive systems' vulnerability to cyberattacks and the features of cyberspace. In fact, cyberattacks evolve rapidly, shifting the warfighting "from the day/hour scale to the minute/second scale" (Lehto, 2018, p. 17). In this regard, cyberwarfare differs substantially from kinetic warfare and, accordingly, requires unique considerations when applying traditional laws of conflict to the online domain (AL-Durrah & Sadkhan, 2021). As a result, and given the lack of clear and purposeful regularity and stable or known interacting logics, it seems that "the present cyber condition deviates from the routinized patterns of competition that characterize much of international anarchy" (Kello, 2013, p. 39). In other words, the development of cyberspace as an international space subject to competition between different actors is outpacing the development of strategies to mitigate the associated risk (Kello, 2013).

Present cyber strategies primarily employ a defensive approach. However, an offensive aspect is lacking (Kim et al., 2019). Since they lack an offensive dimension, these systems do not effectively consider and adapt to the evolving cyber warfare landscape, which could be revolutionised by technologies like AI. (Kim et al., 2019). For example, while the vast majority of cyber-attacks are currently planned and launched by humans, AI has the potential to take over such tasks in the future, assessing and penetrating a system more quickly and efficiently. Applied to cyber operations, this technology has the ability to disrupt systems on a much larger scale, posing significant security challenges that militaries need to prepare for (AL-Durrah & Sadkhan, 2021).

Offensive AI

As AI's capabilities grow increasingly sophisticated, its potential to revolutionise the dynamics of conflicts in cyberspace raises both intriguing possibilities and daunting risks. Indeed, AI can be used in a variety of ways to facilitate human activities, including malicious and illegal ones (Kaloudi & Li, 2020). Despite its benefits, AI has the potential to be weaponised. As a matter of fact, AI-driven attacks appear to have increased recently (Guembe et al., 2022).

Offensive AI can be broadly defined as the "use [of] AI as an effective tool and aid to create intense, harmful cyberattacks that are more difficult to detect" (Murugesan, 2022, p. 4). A novel form of cyberattack is arising, characterised by the incorporation of artificial intelligence methods during the attack process, in parallel with conventional methods, amplifying their potential to inflict significant harm (Kaloudi & Li, 2020). As cyber warfare refers to "a digital attack orchestrated by a state or government with the aim of damaging computer systems and networks, conducting espionage, or disrupting the critical infrastructure of an adversary or ally" (Kline et al., 2019), the implications of AI-driven cyber-attacks are significant. Cyberattacks are indeed pervasive and nowadays represent one of the most prominent security challenges (Guembe et al., 2022). Since "the potential of AI to enhance a cyberattack is boundless" (Meinert, 2018, p. 43), this last challenge seems even greater when coupled with the possibility of using AI to conduct cyber operations in an unprecedentedly efficient and rapid manner. AI has increased the feasibility of cyberwarfare, enabling nations to transcend their domestic and global boundaries and have a significant impact on an adversary's military, political, economic and social systems (Kline et al., 2019).

While AI has demonstrated its immense value and capacity for innovation, its most remarkable strengths on the global platform paradoxically unveil its greatest dangers (Kline et al., 2019). An exemplification of the perilous nature of malicious AI deployment lies in its potential to exploit intricate systems like smart cyber-physical infrastructures – encompassing domains such as smart cities, automated vehicles, healthcare devices, and intelligent residences (Kaloudi & Li, 2020). While AI can bring many benefits to the development of these smart systems, it can also be weaponised in a harmful way. Their interconnectivity, to each other and to the Internet of Things (IoT), and their autonomy can become a significant weakness, as a single vulnerability in one of these smart objects can spread to the entire system (Kaloudi & Li, 2020). In short, "the malicious use of AI is altering the landscape of potential threats against a wide range of beneficial applications" (Kaloudi & Li, 2020, p.1).

Delving deeper into the technicalities, there are several ways in which AI can enhance the cyber-attack process of hackers. Kaloudi and Li (2020) divide AI-driven cyberattacks into five main categories: "next-generation malware, voice synthesis, password-based attacks, social bots and adversarial training". The first aims to use AI to create advanced malware with self-learning capabilities, allowing it to adapt to its environment, evade detection and evolve to exploit vulnerabilities. AI can indeed collect vast amounts of data, which allows it to learn other skills from the rules or patterns in the data that build the algorithms (Kline et al., 2019).

Second, AI-powered voice synthesis allows attackers to imitate the voices of individuals to create convincing fraudulent messages and trick victims into divulging sensitive information or performing actions they would not normally do. Third, AI-enhanced password attacks provide a more efficient way to crack passwords, using algorithms to analyse patterns in large datasets of leaked passwords to predict and crack passwords, bypassing traditional security measures.

AI can also be used to generate social bots to amplify disinformation campaigns on social media platforms and manipulate public opinion by mimicking human behaviour and interacting with real users. In the last category, AI is employed to train systems to circumvent defences by exploiting their own vulnerabilities. In addition, AI can improve spear phishing attacks, i.e. "emails sent to specific people that may include a malicious software attachment or a link to a malicious software download" (AL-Durrah & Sadkhan, 2021, p. 125). In this area, AI text generators, such as Chat GPT, can be manipulated to write more convincing emails to trick the victim.

Using these techniques, malicious actors, such as state-sponsored hackers or criminals, will increasingly be able to use these AI-enabled techniques to improve their performance, attacking at unprecedented speed, scale and efficiency (Guembe et al., 2022; Kaloudi & Li, 2020). This will also give them the ability to avoid most traditional detection measures, and so go undetected (Guembe et al., 2022). As a result, existing cybersecurity infrastructures need to be improved. They currently appear inadequate to deal with this type of advanced cyber weaponry, and unviable given the complexity of AI-driven attacks (Guembe et al., 2022). In particular, cybersecurity technologies are presently unable to adequately detect and mitigate AI-based attacks (Guembe et al., 2022). The reason for this is mainly a lack of understanding of how to defend against offensive AI (Kaloudi & Li, 2020).

Defensive AI

Although it can enhance cyberattacks, AI can simultaneously be used to fight offensive AI (Guembe et al., 2022). In the face of the growing threat of AI-driven attacks, AI appears and will become "a significant ally against intensifying cyber threats" (Murugesan, 2022, p.7). Cybersecurity professionals and cybercriminals can leverage AI and machine learning technologies. Cybersecurity refers to a set of technologies, protocols and strategies designed to protect networks, computers, software applications and information from potential attacks, disruptions or unauthorised access (Murugesan, 2022). These security processes can also benefit from the technological development called defensive AI. In a nutshell, this concept encompasses cybersecurity strategies that harness AI systems to tackle challenges that traditional methods struggle to resolve or manage effectively (Murugesan, 2022).

In fact, this technology is expected to play a key role in future cybersecurity processes, with intelligent and automated security services and products based on its unique capabilities (Murugesan, 2022). AI offers significant benefits to defenders. Overall, "these techniques can be applied for identifying malicious activities, fraud detection, predicting cyber-attacks, access control management, detecting cyber-anomalies or intrusions, etc" (Sarker et al., 2021, p.2).

Moreover, while traditional and human-based systems rely on static rules and data to identify suspicious patterns, behaviours and activities, AI uses machine learning algorithms to continuously evolve. In this way, AI-based defences can identify new attack techniques and use this knowledge to grow their datasets, allowing them to detect future attacks faster and with greater accuracy (Meinert, 2018).

Furthermore, AI can be employed for monotonous and time-consuming tasks, thereby releasing security personnel to focus on projects demanding human creativity and innovation (Murugesan, 2022). Similarly, AI can operate around the clock without rest, in contrast to humans, enhancing the security capabilities and readiness of a system.

As recalled by Murugesan (2022), despite its unique features and capabilities, "AI is not a silver bullet". Humans are still needed in the cybersecurity process and cannot be fully replaced by automated and intelligent systems. AI can strengthen the robustness of a system's defences in cyberspace, but for now these technologies are still far from being able to match human intelligence and innovation. Worse still, as cyber technologies themselves, AI systems are vulnerable to being hacked and compromised, with implications for the entire cybersecurity strategy (Murugesan, 2022). Ultimately, it appears that the integration of AI systems into their respective procedures will offer advantages to both offensive and defensive tactics. Nevertheless, "as long as computers are moving into activities that are traditionally done well by humans, it might create new asymmetries in the attack-defense balance" (Kaloudi & Li, 2020, p.29).

AI Applications in Military Operations

Tactical, Operational and Organisational Improvements

In the realm of military operations, the integration of AI systems has brought about a paradigm shift, ushering in a new era of tactical enhancements. Machine learning, deep neural networks, and reinforcement learning empower machines to uncover valuable insights from training data using approaches that might elude human programmers (Singh Gill, 2019). Furthermore, these techniques empower machines to manage much larger amounts of data during operations. This transition has led to a shift from rule-based deterministic systems to approaches that are driven by data and oriented towards achieving specific outcomes (Singh Gill, 2019).

Therefore, with AI's capacity to process vast amounts of data, rapidly analyse complex scenarios and facilitate informed decision-making, its integration into military strategies has unlocked unprecedented opportunities to revolutionise the way armed forces approach planning, execution and adaptation on the modern battlefield. In fact, AI provides military planners with a powerful tool capable of achieving speed, precision and flexibility to adapt the military force to meet the desired objectives (Singh Gill, 2019). Particularly, it can be applied to jobs deemed "dull, dirty, and dangerous" (Sisson, 2019, p. 4). Firstly, it provides the chance to prevent endangering human lives (Pereira Mendes, 2021; Sisson, 2019), particularly by using unmanned systems, as elaborated in the following section. These systems can be used "closer to the front line where the combat is taking place", replacing human operators or remote-controlled drones (Singh Gill, 2019, p. 170). This in turn eliminates "the need to transmit data on vulnerable high bandwidth channels back to home base", averting the disruption or interception of critical information by an adversary (Singh Gill, 2019, p. 170).

Secondly, it can replace human workers in arduous and repetitive tasks, freeing them to focus on tasks that require creativity and human intelligence (Sisson, 2019; Pereira Mendes, 2021). AI systems have finally the potential to resolve several manpower issues, such as mitigating shortages or allowing the armed forces to sustain or improve their combat capabilities without increasing their manpower (Pereira Mendes, 2021). AI systems can lower labour costs in the defence sector, especially in logistics and detection while enhancing productivity. These technologies can also optimise processes, enabling better communication and transparency in complex systems (Pereira Mendes, 2019; Sisson, 2019).

AI proves to be a fascinating tool in supporting data analysts and enhancing the effectiveness of the workforce (Vogel et al., 2021), especially in the sectors of intelligence and defence where it can enhance the decision-making process. As explained by Sisson (2019, p. 4), "the ability of AI to support capturing, processing, storing, and analysing visual and digital data has increased the quantity, quality, and accuracy of information available to decision makers". AI has the capability to process vast amounts of data and is consequently effective in handling the problem of information overload (Pereira Mendes, 2021). It is especially interesting in cyberspace. The internet and social media platforms generate a tremendous amount of data and information daily, which are increasingly fundamental to intelligence gathering. The value of big data and open source intelligence (OSINT) has considerably increased in recent years, to the level that some consider it to have become '"the new oil of the 21st century', 'the world's most valuable resource'" (van Puyvelde et al., 2017, p. 1397).

Nevertheless, as the name implies, databases based on OSINT are too extensive, making it challenging to acquire and analyse them solely with manual labour. In this scenario, AI technology can serve as a primary filter for data before being analysed by human analysts (Carlo, 2021).

Furthermore, as Hallaq et al. (2017) illustrated, AI might be advantageous for intelligence analysis by automating the scanning of satellite images. This function diminishes the workload of military analysts, who would otherwise have to scrutinise vast amounts of data. Contextually, the implementation of AI technologies in data analytics platforms may provide valuable information, expedite early threat detection, and enable the formulation of various strategic scenarios (Hallaq et al., 2017).

Ultimately, this helps the decision-making process. AI can be employed to create 'Intelligent Virtual Assistants' for battlefields, to scan multiple databases and images to identify particular threats, and to choose methods for safeguarding against or conducting cyber warfare (Hallaq et al., 2017). This can assist leaders by providing calculated inputs that are detached from emotion and other human judgement-affecting factors, thus enabling them to make informed decisions in real-time (Hallaq et al., 2017; Carlo, 2021). Moreover, "AI can be used to create simulations and models that allow for different strategies to be tested and evaluated" (Carlo, 2021, p. 269).

Unmanned Systems

Unmanned systems are one particular example of military applications of AI in operations. In other words, unmanned systems refer to systems that operate partially or entirely without human intervention or supervision. This can be achieved through the integration of AI techniques, for example. They can take diverse forms, such as autonomous vehicles, aircraft, tanks or submarines, Unmanned Aerial Vehicles (UAVs) also known as drones, or even lethal autonomous weapons systems (Artificial Intelligent Weapons Systems – AIWS). To summarise, "such robots, which could be in the air, on the ground, or in and under water, theoretically incorporate 'artificial intelligence' (AI) that would make them capable of executing missions on their own" (Cummings, 2017, p. 2).

Autonomous systems are of great interest to military ground operations for various reasons. They are capable of conducting missions in environments that are inaccessible to humans. This capability enables them to collect significant data that would have been otherwise inaccessible (Sisson, 2019). Similarly, they can carry out missions that would pose a risk, or even a lethal threat, to human operators (Russell, 2023). AI robots provide the military the ability to pursue its missions and objectives, while in the long run only putting "mangled metal and fried computers" at risk, instead of human lives (Singh Gill, 2019, p. 169). In fact, as they are made of articulated and lifeless materials, they are able to function in inhospitable environments, like underwater. They can also have super-human abilities and do things that are not possible for humans, such as "withstand higher g-forces in flight" (Russell, 2023, p. 622). Furthermore, they can react faster than human operators and remotely controlled systems, as they operate on the basis of autonomous algorithms and calculations (Russell, 2023). Since they are autonomous, they also do not require a communication system to function.

Therefore, they can operate even when electronic communication is rendered impossible due to jamming or other attacks (Russell, 2023). Ultimately, these systems are "cheaper, faster, more manoeuvrable and have longer range than their crewed counterparts" (Russell, 2023, p. 622).

However, more attention should be given to AIWS in particular. The ethical implications of their use are numerous and controversial. This section will concentrate on the advantages of such systems to military operations, while the disadvantages will be discussed in the following section.

The United Nations defines 'lethal autonomous weapons systems' as "weapons that locate, select, and engage human targets without human supervision" (Russell, 2023, p. 622). It is crucial to clarify that in this definition, 'engage' is actually a euphemism for 'kill', as AISWs are real weapons. As stated previously, the main reason behind the creation and introduction of such systems in military operations is to spare military lives. They provide the possibility of war without fatalities, fought solely by autonomous machines and computers, which is an appealing prospect for countries with populations that are increasingly reluctant to engage in armed conflict (Singh Gill, 2019, p. 169).

Another benefit of AIWS is to reduce collateral casualties. Autonomous weapons should be able to identify and distinguish civilians and combatants with better efficacy, only targeting the latter according to the rules of war. AI is less prone to errors than human operators (Russell, 2023). Additionally, it lacks the capacity to disregard the rules programmed into its system to commit a fault, unlike humans who can intentionally violate them. AIWS thus provide the military with a tool that can "rapidly evaluate threats, decide on and execute war strikes in real time, without the engagement of human will" (Ploumis, 2022, p. 2). Ultimately, in the future AIWS might probably be used "in essentially the same scenarios as human-controlled weapons such as rifles, tanks and Predator drones" (Russell, 2023, p. 622).

AI Vulnerabilities

As Forrest et al. (2020, p. 24) explain, concerns regarding high-intelligence robots have been raised by writers and filmmakers. Films such as Terminator, The Matrix, and I, Robot underscore the potential extreme risks of Artificial General Intelligence systems (AGI) for humanity. However, AI technologists and experts have also expressed concerns, as demonstrated by the open letter signed by over a thousand tech leaders. The letter called for a halt to AI research and development citing profound risks for society (Metz & Schmidt, 2023). One particular issue raised is the insufficient legal and ethical regulation, lagging behind sector developments and creating a significant regulatory gap.

The autonomy of AI systems, their most notable characteristic and advantage, might paradoxically present itself as their primary ethical vulnerability. AI does indeed present the risk of human control loss, bringing forth an array of unprecedented challenges (Singh Gill, 2019). In fact, as stated by Cummings (2017, p. 1), "while computers and AI can be superior to humans in some skill- and rule-based tasks, under situations that require judgment and knowledge, in the presence of significant uncertainty, humans are superior to computers". Human emotions and cognition, often portrayed as untrustworthy, irrational, and barriers to the efficient execution of military operations, are, in fact, crucial to exhibiting restraint in armed conflict (Human Rights Watch, 2012). Machines should therefore not operate without incorporating human intelligence, to guarantee that emotions are not entirely eliminated from military operations; this is also known as the 'centaur approach' (Pereira Mendes, 2021). Furthermore, from an ethical standpoint, it is difficult to justify the capability of machines to independently terminate human lives. Indeed, "human life would be devalued if robots take life-or-death decisions, raising moral and justice concerns" (Russell, 2023, p. 622).

From a legal standpoint, this issue raises apprehensions as it introduces an accountability gap. When a machine independently causes harm, such as taking a life without human oversight, attributing responsibility becomes a challenge. In such cases, it becomes imperative to ascertain the responsible entity objectively to establish liability. Failing to do so could potentially grant AIWS the capability to allow states to breach international humanitarian law without facing the threat of legal repercussions (Pereira Mendes, 2021). The lack of oversight may allow individuals or non-state actors and terrorist groups to obtain weapons capable of swiftly and effectively eradicating entire populations (Russell, 2023). The issue of AI systems adhering to international law must therefore be examined.

Other significant vulnerabilities of AI systems are operational in nature. These risks can be divided into three categories: (1) hacking, data poisoning, and adversarial attacks; (2) accidents; and (3) trust and reliability (Forest et al., 2020, p. 24). AI systems can be ideal targets for a hacking attack, particularly considering their capability and the potential advantage they can give an adversary if control is taken over them. AI systems are also susceptible to accidents or miscalculations, for instance, in cases of malfunctions or errors in their programming or algorithms. These issues could then unintentionally trigger conflicts or lead to their escalation (Russell, 2023, p. 622). Regarding trust and reliability, the sophistication of AI systems is making them less transparent to human operators. It is becoming less evident to identify when the system is not working as intended. This has potentially dangerous consequences if human operators cannot properly recognise when an AI system has become defective and it is still being used in military operations, therefore increasing the potential for accidents or hacking. Human operators working with AI systems must be sufficiently experienced in this particular tech domain to understand these specific systems and trust their reliability.

This last point exposes a final vulnerability in the integration of AI within the military sector, specifically the insufficient governmental proficiency in AI, in contrast to the commercial sector. While the commercial sphere has seen an explosion in the development of autonomous systems, military autonomous systems have been progressing slowly (Cummings, 2017). In comparison to the advances made in commercial autonomous systems like drones and driverless cars, military development has been at best incremental (Cummings, 2017). This shift of research and development efforts from the public and military to the private sector presents various problems. Firstly, the budgetary differences between the two sectors have enticed many experts, especially the most talented, to join the commercial sphere where they can obtain more funding and benefits (Cummings, 2017). This defines a private sector more proficient in the AI domain compared to the military. The situation presents another crucial issue, namely that the systems being created are primarily intended for private and civilian use. The standard of autonomy being developed may not meet the necessary levels and quality required for military purposes (Cummings, 2017). Additionally, as the defence sector must rely further on commercial progress in this area, it results in difficulty in distinguishing between commercial drone autonomy and that of military UAVs. In conclusion, an uneven commercial autonomous system market development could lead to governments and militaries lacking expertise, potentially compromising and rendering autonomous systems, whether fully or semi-autonomous, unsafe (Cummings, 2017, p. 2).

Geopolitical Implications

Strategic Advantage and the Emergence of a New Arms Race

The swift progress of sophisticated technologies like AI and their widespread implementation have resulted in a scenario where nations can attain strategic benefits only if they are at the forefront of innovation and technological progress. Although AI is still in the early stages of development particularly in the military sphere, it is increasingly being acknowledged as a considerable strategic advantage (Carlo, 2021; Thornton & Miron, 2020). Russia, for instance, is placing great emphasis on what the Kremlin considers a significant tool in cyberwarfare, capable of producing "truly game-changing strategic effects against state adversaries" (Thornton & Miron, 2020, p.12). Moreover, in a speech given in September 2017 to pupils about AI, Russian President Vladimir Putin stated that "the one who becomes the leader in this sphere will be the ruler of the world" (Asaro, 2019). Due to the technology's importance, particularly in the field of cyber warfare, and its implementation in military robotics, a global competition towards AI appears to have begun in recent years (Carlo, 2021). This has led to the emergence of a new arms race, driven not only by the traditional security imperatives of states but also by the fear of falling behind in the technological domain. The increasing importance of technology as a source of strategic advantage has put pressure on states to invest heavily in research and development and to acquire and deploy new technologies quickly.

In fact, for players like Russia and China, AI not only provides tactical and organisational advantages but "the ability to disrupt US military superiority" (Thornton & Miron, 2020, p.20). Other Western countries have also fallen victim to electoral interference, notably through online information warfare, using bots and other tactics to influence opinions.

In this field, AI could indeed become a game-changing tool, launching even more compelling information campaigns. According to Thornton and Miron (2020, p.20), "the threat to Western interests from Russian AI-enhanced cyber warfare is not notional; it is clear". The challenges are likely to increase in the foreseeable future as the technology continues to improve and enhance its performance and capabilities. However, Western militaries envisage utilising AI primarily at a tactical level rather than a strategic one, potentially overlooking the possible weaponisation of AI systems and its impact on the global competition arena (Thornton & Miron, 2020). It can indeed be expected that AI will play a progressively pivotal role in international competition in the upcoming years. As stated by Carlo (2021, p. 277), it is therefore "critical that organisations such as NATO maintain their superiority and react to the challenges posed by this new technology".

Furthermore, an AI arms race can be framed in various ways, depending on the context, whether it be from an economic or military perspective (Asaro, 2019). This could have repercussions for the conduct of the global technological race, as it outlines the objectives, allocation of resources, and actors involved. In a race to gain economic and political control, investments are primarily directed towards the commercial and private sectors rather than the military, impacting the capacity and quality of AI systems for military applications (Asaro, 2019). Additionally, IT platforms and companies are integral players in this competition, alongside states, with their own interests and objectives. These firms are increasingly in possession of vast amounts of data - a new and critical resource - and are capturing large amounts of economic wealth.

All of this is providing them with increasing political influence. They can use this newly acquired influence and the big data they are able to collect to deploy AI technologies able to predict and control human behaviour (Asaro, 2019). This explains why for Asaro (2019), "the greatest threat to the political hegemony of nation-states could become the technology companies themselves, rather than other nation-states".

Therefore, given the complexity of the international security environment and the risks associated with the proliferation of advanced technologies like AI, it is vital that states adopt a careful and measured approach to the development and deployment of new technologies, including all potential actors. Ultimately, the aim should be to guarantee the widespread sharing of the benefits of technological innovation, contributing to a peaceful and stable international security environment.

Impact on Military Cooperation

Technological compatibility is an important aspect of successful military operations. In fact, technological improvement has always played a key role in military equipment. As a result, the defence industry is attempting to become increasingly important in developing new and emergent technologies, to adapt to society's wider technological advances and evolution (Fuilmartin, 2023). Today's technological advancements are such that we seem to have entered the 'third revolution in military affairs', characterised by the rise of computing science and the emergence of numerous groundbreaking technologies, like AI (Thornton & Miron, 2020; Kroenig, 2021).

In parallel, military operations are nowadays increasingly conducted jointly by several countries. Considering the expected growing role of AI systems in the defence sector, technological compatibility in this domain is crucial for military interoperability.

In short, interoperability can be defined as a "measure of the degree to which various organisations or individuals are able to operate together to achieve a common goal" (Huraet al., 2000, p. 7). In other words, it means that "my radio can talk to your radio, your ammo fits my gun [...], my computer understands your computer, your fuel nozzle fits in my filler tube, and on and on" (Saunders & Koczanski, 2013, p. 2). It is interesting to note that, like AI military applications, interoperability concerns every level of military operations, from the tactical level to the strategic, passing by organisational and operational.

Scholars and military experts extensively agree that interoperability is a 'force multiplier' (Ciocan, 2011, p. 66; Saunders & Koczanski, 2013, p. 2) and is a must-have for the success of joint operations and response to international security crisis (Ciocan, 2011). In the context of increasing multi-dimensional and international security issues, interoperability is increasingly perceived as a necessity. Furthermore, the concept relates not only to relations between states but also with other relevant international actors, such as international organisations and private industries (Munk, 2002). This latter is particularly important in the context of AI as most of the research and development is funded by private actors and IT firms.

In this context, AI presents both opportunities and challenges to military interoperability. In terms of logistics, AI, as explained by Schütz and Stanley-Lockman (2017, p. 1), holds the potential to liberate valuable resources, readjust the makeup of forces, and provide operational advantages such as enhanced distributed manoeuvrability. AI integrated into military systems can aid in faster handling of large data sets, improve decision-making, ease communication, and enhance transportation (Abadicio, 2019). This, in turn, increases troops' readiness as it relies on efficient logistics (Schütz, Stanley-Lockman, 2017).

Intelligence agencies can benefit significantly from AI for reconnaissance and surveillance operations. In particular, UAVs can acquire critical sensitive information about a target or challenging terrain that is difficult to access, without risking the lives of any operators. Finally, AI can be utilised as an essential strategic asset within the increasingly militarised cyberspace, providing agents from various armed forces with shared defensive and offensive capabilities.

However, for joint military forces to fully capitalise on the advantages of AI, their systems must be interoperable. Inadequate interoperability, notably within the IT sector, may lead to data loss and impede real-time sharing of vital information, thereby hindering the decision-making process. Unfortunately, this issue persists within the realm of AI integration. For example, there are at least thirteen distinct battle tracking systems across NATO countries, such as drone technologies, to assist in constructing operational situational awareness (NATO, 2015). The absence of uniformity among these systems presents a challenge to interoperability and exposes the difficulty of harmonising digital technologies. Incorporating diverse defence systems within the realm of AI requires amalgamating disparate hardware and software modules, often originating from dissimilar manufacturers. Discordances in system architecture, interfaces, and software protocols could result in integration challenges that may diminish the ultimate efficiency of AI-driven operations. It is therefore important for standardisation agreements aimed at addressing interoperability to consider the numerous challenges of AI systems and ensure their interoperability starting from the design phase. This is necessary to avoid mismatches that can significantly affect the success of joint operations and hinder the army from fully benefiting from AI.

Concluding Remarks

Ethical Considerations

With the increasing use of AI to take over various tasks from human operators within the security sector and broader society, numerous ethical issues must be considered. As explained by Bellaby (2021, p. 86), "autonomous weapons are not full ethical agents due to the restrictions of their coding". Although AI systems may appear to be capable of making decisions in a similar fashion to humans, their actions are ultimately determined by programmed instructions. They do not relieve human operators from responsibility for any harm that may result from the deployment of these systems (Bellaby, 2021).

The integration of AI systems in military operations creates an "asynchrony between decision-making and decision-execution" (van Diggelen et al., 2023, p. 4). The use of machines can distance decision-makers and operators from the moral impact of their decisions. However, it does not absolve them of ethical responsibility for the behaviour and actions of the system. Therefore, humans bear responsibility for actions that are "increasingly distant from their own decision-making, forcing them to assume the moral weight, blame, and, if necessary, punishment for an eventual action" they cannot directly control or reasonably expect to predict (Bellaby, 2021, p. 87). As a result, AI raises important questions regarding accountability that the military must consider when incorporating intelligent systems into their operations.

In addition, the increasing reliance on machines in military operations risks 'dehumanising' wars and conflicts. (van Diggelen et al., 2023, p. 1). AI systems are not conscious beings and do not include emotions in their calculations as humans do. Traits like empathy, compassion, and remorse are absent from the algorithms, that rely solely on deterministic and probabilistic calculations (van Diggelen et al, 2023).

However, these emotions play a crucial role in guiding appropriate moral decisions and judgments, as they signify an individual's values and establish their motivation and engagement in the decision-making process. AI systems cannot currently comprehend and replicate the complex thought processes of humans. Therefore, to guarantee ethical decision-making, human oversight is necessary to consider factors that machines are unable to grasp (van Diggelen et al., 2023).

AI and the Nature of Conflicts

This paper focused on the implications of incorporating AI across various facets of military operations, with a specific emphasis on its relevance within cyber warfare. The investigation encompassed the advantages and security implications linked to the integration of AI systems within defence contexts. It also highlighted the potential benefits offered by AI in bolstering defence capabilities, particularly in cyberspace and diverse military domains, it concurrently underscored the novel challenges and vulnerabilities arising from these emergent technologies.

Initiating with a precise definition of AI as a system capable of comprehending external data, learning from it, and applying insights for achieving preset goals through adaptable mechanisms, the first section scrutinised AI's cybersecurity consequences. It delineated AI's dual role in enhancing both cyberattacks and the fortification of countermeasures against them.

Transitioning to the realm of physical AI applications, the analysis highlighted AI's capacity to confer military advantages across tactical, operational, and strategic levels of military operations.

Additionally, AI is applicable in unmanned systems, offering soldiers novel capabilities whilst safeguarding human lives. However, this does not come without risks, as analysed in the paper, AI systems are not impervious to errors and vulnerabilities, making them vulnerable to cyber-attacks that could have significant repercussions on military operations. AI systems also raise moral and legal considerations concerning decision-making accountability. Moreover, without formal training, their use may be difficult to understand, resulting in transparency and error prevention concerns.

Furthermore, the paper examined the geopolitical implications of AI, elucidating its potential to provide significant strategic leverage to nations and possibly incite a new arms race through its militarisation. The integration of AI into defence systems also poses challenges for international military cooperation in terms of technological interoperability.

In conclusion, this paper provided a comprehensive exploration of AI's implications within both the physical and cyber dimensions of military operations, dissecting their associated security considerations. As stated by Ploumis (2022, p. 14), the integration of artificially intelligent machines is likely to fundamentally transform the nature of warfare into an impersonal phenomenon. The integration of AI systems is expected to diminish the human element in decision-making and execution in combat scenarios, possibly detaching fighters from the immediate repercussions of their actions. This shift could redefine the traditional emotional and moral dimensions associated with warfare, ushering in a new era in which strategic decisions and engagements may be predominantly influenced by algorithms and automated processes rather than human experience and instinct.

Bibliography

Abadicio, M. (2019, April 30). Artificial Intelligence for Military Logistics – Current Applications. Emerj Artificial Intelligence Research. https://emerj.com/ai-sector-overviews/artificial-intelligence-military-logistics/.

AL-Durrah, Q. & Sadkhan, S. B. (2021). Cyberwarfare Techniques: Status, Challenges and Future Trends. 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM-2021), 124-129. https://doi.org/10.1109/ICCITM53167.2021.9677861.

Asaro, P. (2019). What is an artificial intelligence arms race anyway. ISJLP, 15, 45. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/isjlpsoc15&section=5.

Barnard-Wills, D. & Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. Space and Culture, 15:2, pp. 110–123. https://doi-org.ezproxy.lib.gla.ac.uk/10.1177/1206331211430016.

Bellaby, R. W. (2021). Can AI Weapons Make Ethical Decisions? Criminal Justice Ethics, 40(2), 86–107. https://doi-org.dcu.idm.oclc.org/10.1080/0731129X.2021.1951459.

Carlo, A. (2021). Artificial Intelligence in the Defence Sector. In: Modelling and Simulation for Autonomous Systems (pp. 269–278). Springer International Publishing. https://doi-org.dcu.idm.oclc.org/10.1007/978-3-030-70740-8_17.

Ciocan, F. (2011). Perspectives on Interoperability Integration within NATO Defense Planning Process. Journal of Defense Resources Management (JoDRM), 2(2), 53-66. https://www.ceeol.com/search/article-detail?id=78253.

Copeland, B. J. (2023, June 21). Artificial Intelligence. Encyclopaedia Britannica. www.britannica.com/technology/artificial-intelligence.

Cummings, M. L. (2017). Artificial intelligence and the future of warfare. London: Chatham House for the Royal Institute of International Affairs. https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings.pdf.

Forrest, E. M., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K. & Grossman, D. (2020). Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RR3139-1.html.

Fuilmartin, J.F. (2023). Military Technology. Britannica. https://www.britannica.com/technology/military-technology.

Guembe, Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L. & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. Applied Artificial Intelligence, 36(1). https://doi.org/10.1080/08839514.2022.2037254.

Haenlein, M. & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. California Management Review, 61(4), 5 – 14. https://doi-org.ezproxy.lib.gla.ac.uk/10.1177/0008125619864925.

Hallaq, B., Somer, T., Osula, A. M., Ngo, K. & Mitchener-Nissen, T. (2017, June). Artificial intelligence within the military domain and cyber warfare. In: Eur. Conf. Inf. Warf. Secur. ECCWS (pp. 153-157). https://core.ac.uk/download/pdf/132201697.pdf.

Human Rights Watch and International Human Rights Clinic. (2012). Losing Humanity: The Case Against Killer Robots. https://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf.

Hura, M., McLeod, G., Larson, E. V., Schneider, J., Gonzales, D., Norton, D. M., Jacobs, J., O'Connell, K. M., Little, W., Mesic, R. & Jamison, L. (2000). Interoperability: A Continuing Challenge in Coalition Air Operations. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/monograph_reports/MR1235.html.

Kaloudi, N. & Li, J. (2020). The AI-Based Cyber Threat Landscape: A Survey. ACM Computing Surveys, 53(1), Article 20, 1–34. https://doi-org.dcu.idm.oclc.org/10.1145/3372823.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security, 38:2, pp. 7-40. https://www.jstor.org/stable/24480929.

Kim, S.-K., Cheon, S.-P. & Eom, J.-H. (2019). A leading cyber warfare strategy according to the evolution of cyber technology after the fourth industrial revolution. International Journal of Advanced Computer Research, 9(40), 72 – 80. http://dx.doi.org/10.19101/IJACR.SOC6.

Kline, K., Salvo, M. & Johnson, D. (2019 March 27). How Artificial Intelligence and Quantum Computing are Evolving Cyber Warfare. Cyber Intelligence Initiative – The Institute of World Politics. https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/.

Kroenig, M. (2021). Will Emerging Technology Cause Nuclear War?: Bringing Geopolitics Back In. Strategic Studies Quarterly, 15(4), 59-73. https://link.gale.com/apps/doc/A689824415/AONE?u=glasuni&sid=summon&xid=e72dd5de.

Lehto, M. (2018). The Modern Strategies in the Cyber Warfare. In: Lehto, M., Neittaanmäki, P. (eds.) Cyber Security: Power and Technology. Intelligent Systems, Control and Automation: Science and Engineering, vol 93. Springer, Cham. https://doi.org/10.1007/978-3-319-75307-2_1.

McCarthy, J. (2007). What is Artificial Intelligence? http://www-formal.stanford.edu/jmc/whatisai.pdf.

Meinert, M. C. (2018). Artificial Intelligence: The Next Frontier of Cyber Warfare? ABA banking journal, 110 (3), p.43-43. https://web-p-ebscohost-com.dcu.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=0&sid=86c959a0-a1a2-41d0-a52b-bdef68a1bf20%40redis.

Metz, C. & Schmidt, G. (2023, March 29). Elon Musk and Others Call for Pause on A.I., Citing 'Profound Risks to Society'. The New York Times. https://www.nytimes.com/2023/03/29/technology/ai-artificial-intelligence-musk-risks.html.

Munk, S. (2002). Interoperability in the Infosphere. Challenges, Problems, Solutions. Jan Kamenícek. Obrana a Strategie, 2005:1, pp. 103-140. https://www.proquest.com/openview/379adfcc7a3dcc0739399085938cb0e7/1?pq-origsite=gscholar&cbl=236259.

Murugesan, S. (2022). The AI-Cybersecurity Nexus: The Good and the Evil. IT Professional, 24(5), 4–8. https://doi.org/10.1109/MITP.2022.3205529.

NATO. (2015, June 16). Enhancing interoperability: the foundation for effective NATO operations. North Atlantic Treaty Organisation. https://www.nato.int/docu/review/articles/2015/06/16/enhancing-interoperability-the-foundation-for-effective-nato-operations/index.html.

Pereira Mendes, L. (2021). Artificial Intelligence in the Military. Info flash. Finabel European Army Interoperability Centre. https://finabel.org/artificial-intelligence-in-the-military/.

Ploumis, M. (2022). AI weapon systems in future war operations; strategy, operations and tactics. Comparative Strategy, 41(1), 1–18. https://doi-org.dcu.idm.oclc.org/10.1080/01495933.2021.2017739.

Reveron, D. S. (2012). Chapter 1. An Introduction to National Security and Cyberspace. Reveron, D. S. et al. (eds). Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press, pp. 3-19. https://ebookcentral.proquest.com/lib/gla/detail.action?docID=1029588.

Russell, S. (2023). AI weapons: Russia's war in Ukraine shows why the world must enact a ban. Nature, 614, pp. 620-623. https://www-nature-com.ezproxy.lib.gla.ac.uk/articles/d41586-023-00511-5.

Sarker, I. H., Furhad, M. H. & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science, 2(173). https://doi.org/10.1007/s42979-021-00557-0.

Saunders, G. E. & Koczanski, T. (2013). Interoperability. Defense Standardization Program Journal.

Schütz, T. & Stanley-Lockman, Z. (2017). Smart Logistics for Future Armed Forces. European Union Institute for Security Studies. https://www.jstor.org/stable/resrep17454.

Singh Gill, A. (2019). Artificial Intelligence and International Security: The Long View. Ethics & International Affairs, 33(2), 169–179. https://www-cambridge-org.dcu.idm.oclc.org/core/journals/ethics-and-international-affairs/article/artificial-intelligence-and-international-security-the-long-view/4AB181EAF6485014222579349 82A4DD5.

Sisson, M. (2019). Multistakeholder Perspectives on the Potential Benefits, Risks, and Governance Options for Military Applications of Artificial Intelligence. The Militarization of Artificial Intelligence. Technical report. United Nations Office for Disarmament Affairs, pp. 3-5.

Thornton, R. & Miron, M. (2020). Towards the "Third Revolution in Military Affairs": The Russian Military's Use of AI-Enabled Cyber Warfare. The RUSI Journal, 165(3), 12–21. https://doi-org.dcu.idm.oclc.org/10.1080/03071847.2020.1765514.

van Diggelen, J., Metcalfe, J. S., van den Bosch, K., Neerincx, M. & Kerstholt, J. (2023). Role of emotions in responsible military AI. Ethics and Information Technology, 25(1), 17–20. https://doi-org.dcu.idm.oclc.org/10.1007/s10676-023-09695-w.

van Puyvelde, D., Coulthart, S. & Hossain, M. S. (2017). Beyond the Buzzword: Big Data and National Security Decision-Making. International Affairs (London), 93(6), pp. 1397-1416. https://doi-org.ezproxy.lib.gla.ac.uk/10.1093/ia/iix184.

Vogel, K. M., Reid, G., Kampe, C. & Jones, P. (2021). The impact of AI on intelligence analysis: tackling issues of collaboration, algorithmic transparency, accountability, and management. Intelligence and National Security, 36(6), 827–848. https://doi-org.dcu.idm.oclc.org/10.1080/02684527.2021.1946952.

Wang, P. (2019). On Defining Artificial Intelligence. Journal of Artificial General Intelligence, 10(2), 1–37. https://doi.org/10.2478/jagi-2019-0002.