Leo Heng

STRATEGIC OVERVIEW OF APPLYING ARTIFICIAL INTELLIGENCE ON THE FUTURE BATTLEFIELD

UNIVERSITY OF JYVÄSKYLÄ
DEPARTMENT OF INFORMATION TECHNOLOGY
2024

TIIVISTELMÄ

Heng, Leo
Strategic Overview of Applying Artificial Intelligence on the Future Battlefield
Jyväskylä: Jyväskylän yliopisto, 2024, 125 s.
Turvallisuus ja strateginen analyysi, pro gradu -tutkielma
Ohjaajat: Lehto, Martti; Halunen, Kimmo

Tämä tutkimus tarjoaa kattavan strategisen katsauksen tekoälyn (AI) soveltamisesta tulevaisuuden sodankäynnissä ja konfliktitilanteissa. Tutkimus syventyy tekoälyn teknologisiin perusteisiin, mukaan lukien suuret datamäärät, suorituskykyinen laskenta ja koneoppimisalgoritmit, ja tarkastelee kognitiivisia prosesseja, jotka mahdollistavat tekoälyjärjestelmien havainnoinnin, päätöksenteon ja toiminnan sotilaallisessa kontekstissa. Tutkimus käsittelee myös tekoälyn integrointia fyysiseen maailmaan, korostaen mahdollisuuksia parantaa toiminnallista tehokkuutta ja päätöksentekokykyä.

Lisäksi tutkimus hahmottelee strategisen maiseman, joka muovaa uusien tekoälyteknologioiden omaksumista tulevaisuuden sodankäynnissä. Maisema määritellään 1) teknologisen kehityksen ja globaalien dynamiikkojen, 2) yhteiskunnallisten ja sääntelyyn liittyvien tekijöiden, 3) sotilaallisen strategian ja konfliktien johtamisen, sekä 4) edistyneiden teknologioiden ja niiden vaikutusten kautta.

Tutkimus luokittelee tekoälyn tulevaisuuden mahdolliset sovelluskohteet eri toiminta-alueisiin, joihin kuuluvat 1) parannettu tiedustelu, päätöksenteko ja ennustuskyvyt; 2) operationaalinen tehokkuus ja toimitusketjun optimointi; 3) edistynyt ihmisen ja koneen välinen vuorovaikutus ja suorituskyvyn parantaminen; 4) kyber- ja informaatiosodankäynnin tehostaminen; sekä 5) autonomiset järjestelmät ja robotiikka.

Tutkimus korostaa tekoälyn muuntavaa potentiaalia sodankäynnissä ja tuo esiin tarpeen eettisille pohdinnoille, vastuullisuudelle ja kansainväliselle yhteistyölle. Sen tavoitteena on varustaa puolustus- ja turvallisuusalan ammattilaiset strategisella ymmärryksellä tekoälyn mahdollisuuksista ja haasteista, ja se kannustaa jatkamaan tutkimusta, politiikan kehittämistä ja eettistä hallintoa varmistaakseen tekoälyn positiivisen vaikutuksen kansalliselle ja kansainväliselle turvallisuudelle.

Asiasanat: tekoäly, sodankäynti, taistelukenttä, tulevaisuus, strateginen, sovelluskohde, käyttötapaus

ABSTRACT

Heng, Leo
Strategic Overview of Applying Artificial Intelligence on the Future Battlefield
Jyväskylä: University of Jyväskylä, 2024, 125 pp.
Security and Strategic Analysis, Master's Thesis
Supervisors: Lehto, Martti; Halunen, Kimmo

This study provides a comprehensive strategic overview of the application of artificial intelligence (AI) in future warfare and conflict scenarios. It delves into the technological foundations of AI, including big data, high-performance computing, and machine learning algorithms, and explores the cognitive processes that enable AI systems to observe, decide, and act within a military context. The study also examines the integration of AI into the physical world, highlighting the potential for enhanced operational efficiency and decision-making capabilities.

Furthermore, the study outlines the strategic landscape that shapes the adoption of new AI-enabled technologies in the future conduct of warfare. The landscape is characterized by 1) technological evolution and global dynamics, 2) sociopolitical and regulatory factors, 3) military strategy and conflict conduct, and 4) advanced technologies and their implications.

The future applications of AI in the battlespace are categorized into various domains consisting of 1) enhanced intelligence, decision-making, and predictive capabilities; 2) operational efficiency and supply chain optimization; 3) advanced human-machine interaction and performance enhancement; 4) cyber and information warfare enhancement; and 5) autonomous systems and robotics.

The study emphasizes AI's transformative potential in warfare, highlighting the need for ethical considerations, accountability, and international cooperation. It aims to equip defense and security professionals with a strategic understanding of AI's opportunities and challenges, advocating for continued research, policy development, and ethical governance to ensure AI's positive impact on national and international security.

Keywords: artificial intelligence, warfare, battlefield, future, strategic, application, use case

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Artificial intelligence is currently bringing about significant changes in all areas of society, and even the most knowledgeable experts have only educated guesses about the outcome of this process (Hunter, Albert, Rutland, et al., 2023). As part of this transformation, artificial intelligence is very likely to have a significant impact on warfare as well (J. Johnson, 2019). Building defense capabilities over decades requires anticipatory consideration of the threats and opportunities brought about by AI to maintain a credible deterrent effect (J. Johnson, 2020b).

The most vigorous development of artificial intelligence is currently taking place in major corporations such as Microsoft, Alphabet (Google), Meta (Facebook), and NVIDIA in the United States, as well as in China with companies like Alibaba, Baidu, Huawei and Tencent. The forefront of technological development is not within the military or defense industry, but it is reasonable to assume that especially the business sectors in these two countries also support efforts to utilize technology for military purposes. (Duggan, 2024; glass.ai, 2023.)

Military applications can be widespread across all dimensions of the battlespace (land, sea, air and space, but also including cyber and information environments that intersect the physical dimensions). AI can be utilized in weapon systems (with the biggest concern being lethal autonomous weapon systems, LAWS), logistics, data collection, as well as in support of leadership and decision-making. (Metz & Cuccia, 2011.) Ethical and moral considerations unite all these various applications (Arandjelović, 2023; Trusilo & Danks, 2023).

AI has become a central factor in NATO's digital transformation strategy, and several alliance member states are increasing their investments in its development (Giordano, 2023). At the same time, there are global efforts to restrict the military use of such technologies (*AI and Autonomous Weapons Arms Transfers*, 2022; *AI Weaponry Should Be Banned from the Battlefield*, 2023; Boodhoo, 2024; Gibbs, 2015; O'Connell, 2023; Russell, 2023; *Stop the "Stop the Killer Robot" Debate*, 2022; Wareham, 2020). However, limitations are not a credible way to prevent AI from reaching the battlefield for three key reasons:

1. Major states, such as the United States and China, have not expressed support for the ratification of such agreements.
2. States acting autonomously outside the international legal system and various non-state entities, such as terrorist organizations, have no reason to adhere to international agreements.
3. Many AI application methods are openly available and simple to use, allowing even a technically competent individual to independently build an autonomous weapon system.

Since the use of AI on future battlefields cannot be prevented, democratic states in particular must familiarize themselves with its possibilities, at least for defensive and counteraction purposes.

1.1 Earlier research

Both artificial intelligence and future warfare have been extensively researched. There is also a considerable amount of non-fiction literature on the topic, along with policy papers from public entities and forecasts from think tanks and research institutes. Overall, the field is characterized by an abundance of interesting material. Much of the material delves deep into the subject, making it practically impossible even for an expert in the field to fully comprehend due to the breadth of the topic. Therefore, the goal of this study is to conduct a strategic-level overview that would assist defense and security professionals in gaining insights into the subject.

Public documents such as Strategic guidelines for developing AI-solutions by the Finnish Ministry of Defense (2020), Data, Analytics, and Artificial Intelligence Adoption Strategy by the U.S. Department of Defense (2023) or NATO 2022 Strategic Concept (2022) give often a limited overall view of the topic, while being heavily influenced by local constraints. Military organizations conduct voluminous research, but the full results are not usually publicly available. However, there is even a wealth of writing on predicted developments and strategic effects. Authors such as Johnson (2019, 2020a, 2020b, 2021, 2022b, 2024), Shiekh (2022), Schmertzing (2018), Ruppert (2024), Rajagopalan (2022), Payne (2018) and O'Hanlon (2018) among many others have contributed greatly to the general understanding.

Some of the most important books published on the topic include Latiff's Future War: Preparing for the New Global Battlefield (2017), Lonsdale's The Nature of War in the Information Age: Clausewitzian Future (2004), Scharre's Army of None: Autonomous Weapons and the Future of War (2018) and Four Battlegrounds: Power in the Age of Artificial Intelligence (2023), Sanger's The perfect Weapon: War, Sabotage, and Fear in the Cyber Age (2018), Lee's AI Superpowers: China, Silicon Valley, and the New World Order (2021), Lee and Chen's AI 2041 (2021), Lovelock and Appleyard's Novacene: The Aoming Age of Hyperintelligence (2019), Kaku's Quantum Supremacy: How the Quantum

Computer Revolution Will Change Everything (2023), Bradford's Digital Empires: The Global Battle to Regulate Technology (2023) and The Age of AI and Our Human Future by Kissinger et al. (2021).

1.2 Key concepts and definitions

As the study touches such a wide field of different concepts, a number of concepts need to be defined. By defining the concepts here it is possible to also set limitations and boundaries, and to focus on studying the actual topic, use of artificial intelligence in warfare. Some of the concepts defined here are very complex and others seem mundane, but it is important to lay out some key understanding to be able to discuss the topics in sufficient detail later.

1.2.1 Military concepts

Battlefield and battlespace: Panwar (2017) discusses the evolution of the concept of the battlefield in the context of modern warfare, which has become increasingly complex and multifaceted. The traditional term "battlefield" has been largely replaced by "battlespace" to reflect the multi-dimensional nature of contemporary military operations that extend beyond physical domain (land, sea, air, space) to include cyberspace domain. Cebrowski (2000) adds the physical, information, cognitive, and social domains. While the five-dimensional model is widely accepted in military doctrines, there may be a need to evolve a more comprehensive model that includes the human dimensions of cognitive and social domains (Cebrowski, 2000; Panwar, 2017). In many current usages the now already traditional five-domain model has been updated to include the information domain, which summarizes the cognitive and social domains. In the more modern six-domain model both the cyber and information domains are ubiquitous in the physical domain, meaning that they are present everywhere in the land, sea, air and space domains.

Petranick (2015) focuses on the realities of the 21st-century battlefield environment, particularly in the context of asymmetric warfare and terrorism. He defines asymmetric warfare as the blurring of lines between various aspects such as politics, economics, combatants, and civilians, and includes dynamics like cyber warfare, communications, and the use of civilians as shields and weapons. He argues that conventional warfare is becoming obsolete and is being replaced by asymmetric warfare, which has been present throughout history but is now being applied in totality as a means to fight. The document also criticizes the current rules of engagement and military doctrines, suggesting that they may favor the enemy and hinder the effectiveness of military operations. (Petranick, 2015.) In more modern light we can see that the Russian invasion of Ukraine has proven, that conventional warfare has not become obsolete, but that the other less conventional forms of warfare complement it. It seems unlikely that any

method or form of warfare ever released from the Pandora's box could be put back there. Even though we wouldn't have seen a certain strategy, tactic or method used, all the suitable known methods will be used when there is need for them.

To complement Petranick, Münkler (2003) explores the characteristics of "new wars" in the 21st century, focusing on three main phenomena: asymmetry, demilitarization, and privatization and commercialization of war. He highlights the asymmetry between parties in conflicts, the trend towards wars being fought partly by soldiers and not primarily against military targets, and the increasing role of private and commercial interests in conflicts. He suggests that these trends will continue to shape future wars unless there are significant geopolitical and economic changes. (Münkler, 2003.) This has been proven correct by Russia's use of private military companies (PMCs) in Ukraine.

Megret (2012) discusses the social construction of the battlefield and its evolution. He suggests that the battlefield is both an idea and a space, with its purpose and rules shaped by a series of understandings. He argues that the definition of the battlefield has always been central to the conduct of war and that the regulatory role of the battlefield has been increasingly challenged, complicating the waging of war and potentially heralding its end. (Megret, 2012.) The International Committee of the Red Cross (*War & Law*, 2014) confirms this. Israel's recent bombings in Gaza and Russia's bombings in Ukraine are grim examples of using weapons of war designed for open battlefields in populated areas. The weapons have wide-area effects and cause major harm to civilians. However, similar bombings were used in WWII by all the parties, so this is not a new phenomenon.

In summary, the concept of the battlefield is an evolving and increasingly complex construct that extends beyond traditional operations in the physical domain to encompass multiple dimensions, including the human aspects of conflict. This reflects a shift from conventional warfare to a broader, more inclusive understanding of battlespace that takes into account the realities of asymmetric warfare, the role of non-state actors, and the impact of technology and privatization on the conduct of war. Warfare is not conducted only on a physically limited battlefield, but it touches on all aspects of both civilian and warfighter existence.

In addition to the six domains military activities are described to take place in, there are other ways of making sense out the complexity of the real world battlespace. Competing acronyms such as PMESII (Political, Military, Economic, Social, Infrastructure or Information) and DIMEFIL (Diplomacy, Information, Military, Economics, Finance, Infrastructure, and Legal) (Eikmeier, 2019) are equally well suited to the task. The domains and other systems depicted with acronyms overlap partially, as they are mostly used to describe only slightly different things or the same things in different usage or contexts. For the purpose of this study, activities taking place in battlespace could be viewed through any of the listed tools. This, in turn, opens the scope to cover everything an aggressor

could do to affect any part in the society of a target, much in the way hybrid threats are seen.

FAW: Fully Autonomous Weapon, autonomous weapon system capable of causing physical harm. The term LAWS is usually preferred due to both the difference in complexity between an individual weapon and a weapon system (individual weapons are rarely autonomous), and because most weapon systems have a human oversight instead of being fully autonomous.

Hybrid threat: Unwelcome interventions of one sort or another to a country's internal space, with hybrid warfare being the most extreme form of a hybrid threat. Individual activities can't be classified as being "hybrid", the hybrid effect comes from concerted use of different activities for a unified malign purpose. Such synchronized action targets deliberately the systemic vulnerabilities in democratic societies with malign intent, combines the use of multiple tools, creates ambiguity, manipulates the detection and response threshold deliberately, exploits the seams of democratic society and often includes a distracting element. (*The Landscape of Hybrid Threats*, 2021.)

Some threats enhanced or enabled by information technology fall squarely within the hybrid threat umbrella, while others do not. In many cases the tool is the same, but it depends on the wielder or the intent whether the effect can be classified as a hybrid threat or not. Quite often the actors behind the threat employ the services of other organizations or middlemen to carry out the actual deed. And a number of tools employed to build hybrid threats, such as diplomatic sanctions, military exercises, foreign investments or military operations, do not fall in the field of threats enhanced or enabled by information technology.

Hybrid activities are often described to create an effect in Political, Military, Economic, Social, Infrastructure or Information (PMESII) spheres as described by Hillson (2009). For the purpose of this study, any hybrid activities can be seen to take place in a battlespace, and thus should be viewed as something relevant to this study.

Kill chain: The sequence of events starting from target detection and ending with a kinetic effect.

Kinetic effect: The use of lethal force to destroy a military target.

LAW: Lethal Autonomous Weapon, autonomous weapon capable of causing physical harm. The term LAWS is usually preferred due to the difference in complexity between an individual weapon and a weapon system. Individual weapons are rarely autonomous.

LAWS: Lethal Autonomous Weapon Systems, autonomous weapon systems capable of causing physical harm.

OODA Loop: Observe, Orient, Decide, and Act Loop. A model developed by Colonel John Boyd in the 1970s based on his experiences in aerial combat in the U.S. Air Force. The model describes an individual's or organization's reaction to a perceived event. In summary, according to the model, the actor who can go through observation, orientation, decision, and action the fastest will gain an advantage.

1.2.2 Social and legal concepts

Terrorism and cyber terrorism: The Office of the United Nations (*Fact Sheet No. 32*, 2008) defines terrorism as any intentional criminal action which, through death, serious bodily injury, taking of hostages or serious damage to public or private property aims to intimidate a population or to pressurize the authorities to act in a particular way. When drawing the line between other criminal activity and terrorism the key distinguishing factor is the intentional aim to intimidate or pressurize. A catastrophic nuclear plant malfunction can be caused by criminal negligence or by an intentional cyberattack. Likewise, the financial sector might be affected by a large-scale theft or a hacker bringing down the electronic funds transfer system. In both examples, the first act is seen as "regular" crime (accidental or committed for personal gain) while the second act can be argued to be terrorism (if the perpetrator aims for societal impact).

Terrorist organizations: Terrorist groups aim to instill fear and exert political influence through violence. Their tactics often target civilians or non-combatants. Al-Qaeda and ISIS (Islamic State of Iraq and Syria) are prominent examples of terrorist organizations involved in conflicts across the Middle East and beyond. (*Fact Sheet No. 32*, 2008.)

1.2.3 Technological and operational concepts

AGI: Artificial general intelligence or general artificial intelligence also known as strong AI or deep AI, refers to systems that are capable of solving multiple diverse problems, as opposed to narrow AI (ANI). AGI describes the capacity of machines to engage in cognitive processes akin to humans, encompassing thinking, comprehension, learning, and problem-solving abilities. Strong AI employs a theory of mind AI framework to perceive emotions, beliefs, and thought processes in other intelligent systems. A theory of mind-level AI aims to imbue machines with a genuine understanding of human aspects, moving beyond mere replication or simulation of human cognition. While AGI remains unrealized, it has attracted significant interest from leading tech companies. (Kanade, 2022.)

ANI: Artificial narrow intelligence or narrow artificial intelligence, also known as weak AI or narrow AI. ANI systems are designed for specific applications or tasks in one narrow and very specific area only as opposed to general AI (AGI). These systems are programmed to excel in singular tasks like facial or speech recognition, or driving vehicles. ANI operates within predefined parameters, constraints, and contexts, simulating human behavior in a limited scope. Common examples of ANI include Siri's speech and language recognition on iPhones, vision recognition in self-driving cars, and recommendation systems like Netflix's suggestions based on user activity. Google's RankBrain is another instance of narrow AI, utilized for sorting search results. These systems are trained or learn to perform specific tasks efficiently. (Kanade, 2022.)

Automated system: Automatic systems are pre-programmed to act in a certain way, and the way they operate is entirely predictable, without potential

for interpretation (*Texts Adopted - Autonomous Weapon Systems - Wednesday, 12 September 2018*, 2018).

Autonomous system: Autonomous systems operate independently or with minimal human oversight, leveraging artificial intelligence to perform tasks ranging from surveillance to lethal engagements (*Texts Adopted - Autonomous Weapon Systems - Wednesday, 12 September 2018*, 2018).

Autonomous vehicles and robots: The terms "autonomous vehicle" and "robot" both refer to systems equipped with advanced technologies that allow for operations with minimal or no human intervention, but they differ primarily in their design purposes, operational environments, and functionalities.

- An autonomous vehicle is specifically designed for transportation purposes. This includes a variety of platforms such as cars, drones, ships, and aircraft that can navigate and operate independently in their respective environments. The primary function of an autonomous vehicle is to move from one location to another without human control, utilizing technologies like GPS, lidar, radar, and computer vision to safely navigate and handle tasks related to transportation and mobility. Autonomous vehicles are often specialized to operate in specific environments—such as roads, air, or water—and focus on tasks such as route planning, obstacle avoidance, and traffic navigation. (Ioniță, 2020a)
- A robot is a broader and more versatile concept that encompasses any machine capable of carrying out a complex series of actions automatically, especially one programmable by a computer. Robots are designed for a wide range of applications beyond transportation, including manufacturing, surgery, service provision, and exploration. They can interact with their environment in more complex ways, including manipulating objects, performing specific operational tasks, and adapting to varied situations using sensors and programmable actions. Robots are not confined to movement or transportation but are also used for tasks like assembly in factories, medical procedures, or domestic chores. (Raj & Kos, 2022.)

While an autonomous vehicle is a type of robot specialized for transport and navigation tasks, robots as a broader category encompass a wide variety of forms and functionalities that extend well beyond the scope of transportation, highlighting their diverse applications across different sectors and environments (Hoppes et al., 2024; Raj & Kos, 2022).

Autonomous vehicles may be utilized in any physical domains, and are often named to indicate the appropriate environment. The most distinctive types include unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and unmanned maritime vehicles (UMVs, or, separately uncrewed surface vessels (USVs) and unmanned underwater vehicles (UUVs)). Additionally, while the word "drone" often refers to an unmanned aerial vehicle (UAV), it can also be seen to refer to any autonomous vehicle or robot. Thus, the classification of a

drone as either an autonomous vehicle or a robot depends on its intended use and capabilities (Ioniță, 2020a; Raj & Kos, 2022). Since very few UAVs are used for transport, strictly speaking they are robots.

Cyber operations vs. information operations: Military cyber operations (or cyber warfare) target computers, information systems and networks, while information operations (or warfare) target people by using the information as a weapon (Lin, 2020; Mbuthia, 2017; Williams, 2017). In other words, in a cyber operation you could penetrate the servers of a social media platform and delete the contents. In an information operation you could use the platform as it is meant to be used, possibly through several different user accounts, and post disinformation or hate speech in discussions. An information operation can be carried out entirely without information technology, for example by using a printed newspaper or airdropped leaflets as the medium. Then again, it can also be carried out through a cyberattack: the servers of the social media platform could be breached and all the contents could be replaced with disinformation or hate speech.

For the purpose of this essay (and the proposed model) I follow the military usage and define cyber as being technical activity targeting computers, information systems and networks. This approach allows for more exact granularity and wider area of applications. Thus, online crime and cybercrime are not the same thing, neither are information operations and cyber operations.

GAI, GenAI: Generative Artificial Intelligence, an AI system capable of generating text or images.

Human in the loop: An automated system where a human manually approves each step.

Human off the loop: An automated system whose operation does not require human approval or supervision.

Human on the loop: An automated system where a human monitors the steps carried out by the automated system.

Human-machine teaming: The collaboration between a human and a machine as a team.

LLM: Large Language Models, large AI models that can interpret and generate natural language across various application areas. LLMs may sometimes give the impression of AGI but, in reality, they are not.

Remotely and tele-operated systems: Remotely and tele-operated systems are under human control and require constant human input. In many cases the terms are used interchangeably, but they can also be seen as having a slight difference. When tele-operating a system, the operator is in complete real-time control of the full system, usually receiving the required information to do so from the system's sensors such as cameras. In a remote operation setup, on the other hand, the system could be operated with the operator's own senses, usually within a line of sight. Simple real-life examples could be operating a flying drone through a camera and a laptop (tele-operation) and a recreational radio-controlled car standing next to it (remote operation). (Chintamani et al., 2008; Ranganeni et al., 2023; Yu et al., 2013)

1.3 Limitations

The field of technological developments and potential applications of AI in the field of conflicts, security and warfare is vast. To make it possible to conduct this study at all, significant limitations had to be made. First, the focus of the study is on the strategic level, dwelling more on the large-scale effects of utilizing AI, instead of the details or the technology itself. Next, the question of potential problems with ethics, international agreements, regulation and laws is purposefully left mostly unaddressed. Authors such as Trusilo (2023), Tóth et al. (2022), Teo (2022), Shereshevsky (2022), Schraagen (2023), Ryan (2020), again together with Stahl (2020), and Pavlidis (2024) have covered it well, and the discourse continues. This study focuses on outlining the potential possibilities, without making ethical claims on what should and should not be done. It is important to see all the possible applications when preparing to future conflicts, instead of naively disregarding ones deemed unethical based on a democratic nations' standards—it is well possible that the adversary might not have such qualms.

AI research is blooming. ProQuest databases alone list 792 255 documents on artificial intelligence during the past 12 months. The material of the literature review had to be narrowed down with some strict queries. Likewise, the time period studied was set to be from 2022-01-01 to 2024-04-04 (the time of the query) to limit the number of hits. The short time span is not detrimental in this field, since the technology is changing so fast, that studies any older than this run the risk of obsolescence. Although the literature review is not exhaustive, the method utilized provides a reasonably comprehensive overview of the up-to-date literature on the research topic.

2 GOALS AND METHODS

This section describes in detail the goals, the methods and the structure of this study.

2.1 The goal

The goal of the study is to provide a strategic-level overview of warfare-related AI technology available in the near future, and it's use cases in the future battlespace. The overview should serve both technology professionals and career military officers who don't have a deep technological understanding. This study aims to offer a framework through which the development and applications of artificial intelligence can be understood within the two respective fields. The framework should act as a bridge combining the two separate spheres of competence.

It is crucial for defense and security authorities to both grasp the threats and opportunities that technology creates in their field, and be able to use AI-based systems and tools in fulfilling their missions. Additionally, the study aims to offer an easily understandable publication for public discourse, providing readers with better foundational knowledge to understand the ongoing discussions.

Most of the public discourse focuses on autonomous weapon systems (LAWS, often referred to with the deliberately polarizing term killer robots) since it is usually the first thing that comes to mind regarding AI's military applications. However, this study aims to broaden the understanding.

The impact of technology on performance will be more significant the earlier it can be utilized in a process. The OODA Loop theory supports this perspective: comprehensive data gathering, forming a situational assessment based on it, making the best decision, and acting according to the decision before the opponent has a greater impact on the outcome than just having a more accurate weapon.

The research questions for this study were the following:

- What are the artificial intelligence applications that are likely to have the most impact on future warfare and the battlefield between 2024 and 2030?
    - What kind of developments in global trends and technology are likely to have most impact on the development of artificial intelligence systems for defense and security in 2024-2030?
    - What kind of artificial intelligence use scenarios are likely on the future battlefield in 2024-2030?

2.2 The method

The study is a strategic-level review of existing research literature. The scope has been limited by regulating the depth of exploration rather than narrowing down the research field into a single topic, since there is a significant demand for an easily understandable comprehensive description of the domain. Additionally, AI has numerous application areas worth examining, and often the areas overlap, so it would be counterproductive to rule out particular domains.

The key uses of literature reviews are identifying what knowledge is available, determining whether the research reveals any trends or patterns, aggregating findings to support evidence-based practice, generating new frameworks and identifying topics that require more research (Paré & Kitsiou, 2017). For this study identifying the available knowledge, recognizing trends and patterns, and generating a new framework are all applicable uses in order to reach the overall goal. TABLE 1 Literature review types (Grant & Booth, 2009) outlines the potential types below.

TABLE 1 Literature review types

Critical Review	Aims to demonstrate extensive research and critical evaluation of the literature, often resulting in a hypothesis or a model rather than an answer. It is used for conceptual innovation and evaluating the value of previous work.
Mapping Review or Systematic Map	Maps out and categorizes existing literature on a particular topic, identifying gaps in research literature. It is used for identifying research evidence and informing further reviews or primary research.
Meta-analysis	A technique that statistically combines the results of quantitative studies to provide a more precise effect of the results. It is used to assimilate small or inconclusive studies into a composite evidence base.
Mixed Studies Review or Mixed Methods Review	Combines quantitative effectiveness reviews with qualitative reviews on attitudes or implementation

	issues. It is used for a holistic understanding of interventions or conditions.
Overview	A generic term used for any summary of the literature that attempts to survey the literature and describe its characteristics. It is used for broad summation of a topic area.
Qualitative Systematic Review or Qualitative Evidence Synthesis	Integrates or compares findings from qualitative studies, often leading to the development of a new theory or narrative. It is used to explore barriers, facilitators, and user views.
Rapid Review	Provides a quick assessment of what is already known about a policy or practice issue by using systematic review methods. It is used for evidence-based decisions within a policymaker's time frame.
Scoping Review	Provides a preliminary assessment of the potential size and scope of available research literature. It is used to inform policymakers if a full systematic review is needed.
State-of-the-Art Review	Addresses more current matters in contrast to other combined retrospective and current approaches. It is used to offer new perspectives on issues or point out areas for further research.
Systematic Review	Seeks to systematically search for, appraise, and synthesize research evidence, often adhering to guidelines on the conduct of a review. It is used to draw together all known knowledge on a topic area.
Systematic Search and Review	Combines the strengths of a critical review with a comprehensive search process, typically addressing broad questions to produce 'best evidence synthesis'. It is used for exhaustive, comprehensive searching and recommendations for practice.
Systematized Review	Attempts to include elements of the systematic review process while stopping short of a systematic review. It is typically conducted as a postgraduate student assignment and is used to model the systematic review process.
(Traditional) Literature Review	Describes published materials that provide an examination of recent or current literature. It may include research findings and is generally used for summarization and consolidation of previous work.
Umbrella Review	Compiles evidence from multiple reviews into one accessible and usable document, focusing on a broad condition or problem with competing interventions. It is used to aggregate findings from several reviews that address specific questions.

(Grant & Booth, 2009)

Choosing the right approach for the study proved to be complicated. Both the Traditional Literature Review and the Systematic Review were initially considered, but due to the scope of the topic (the whole battlespace) and the aim (to create a conceptual model for understanding the potential use scenarios of AI) they were deemed inadequate. Traditional Literature Review lacks the structure and focus needed for this study, and might have introduced biases. Systematic Review runs the risk of introducing a far too large body of material, which could only have been remedied by narrowing the study scope so much that it wouldn't fulfil the original purpose anymore.

Out of the fourteen different literature review types outlined in TABLE 1 Literature review types, Critical Review rose to the top, because:

1. It aims to demonstrate extensive research and critical evaluation of the literature, but allows for flexible material selection (in this case to limit the amount of material chosen).
2. It often results in a model rather than a single answer, supporting the goal of creating a model of the use case landscape.
3. It is useful for conceptual innovation, again, supporting the model creation in a flexible way.

Critical reviews offer also some additional benefits useful in this study (Grant & Booth, 2009; Jesson & Lacey, 2006; Kibbee, 2023):

4. Acts as a foundation to gathering knowledge by providing a detailed background for understanding the evolution of concepts, theories, and methodologies related to the topic.
5. Helps in identifying gaps by highlighting areas where questions remain unanswered, literature reviews guide researchers toward valuable and original research contributions.
6. Provides theoretical contribution through analysis and synthesis, and can propose new theoretical frameworks or models, offering fresh perspectives on the topic.
7. Gives methodological insights by revealing methodological trends, strengths, and limitations in existing research, guiding the methodological approach of future studies.

Because of these reasons, the study was conducted as a Critical Literature Review as described by Grant and Booth (2009). A critical review enables the researcher to evaluate the existing work to find out what is valuable and should be included. It may also be used to resolve conflicts between competing theories and views, and may act as the first step in a new phase of conceptual research and understanding. (de Klerk & Pretorius, 2019.)

Grant and Booth (2009) use the framework of Search, Appraisal, Synthesis, and Analysis (SALSA) to ensure all the review types contain methodological

accuracy, systematization, exhaustiveness, and reproducibility. TABLE 2 Critical review in the SALSA framework, outlines the method chosen for this study.

TABLE 2 Critical review in the SALSA framework

Search	Seeks to identify most significant items in the field.
Appraisal	No formal quality assessment. Attempts to evaluate according to contribution.
Synthesis	Typically narrative, perhaps conceptual or chronological.
Analysis	Significant component: seeks to identify conceptual contribution to embody existing or derive new theory.

(Grant & Booth, 2009)

2.3 The process

The study by de Klerk and Pretorius (2019) outlines a seven-step process for conducting critical reviews in research. The guideline aims to provide a structured and systematic approach to conducting critical reviews in research, addressing a gap in the literature for clear guidelines on this process:

1. Selecting and defining the review topic
2. Identifying sources of relevant scientific literature
3. Selecting and deselecting prominent literature
4. Data extraction
5. Analyzing and synthesizing extracted data
6. Presenting the review findings and discussion
7. Conclusion and recommendations

2.3.1 Selecting and defining the review topic

The first step involves selecting a focused review topic to manage the volume of literature. It includes considering the type of literature to be included and defining a specific research angle informed by the review question. The more focused the research topic is, the easier it is to limit the amount of the literature included. (de Klerk & Pretorius, 2019.) However, alternatively, for a wide scope, it is possible to try to limit the depth of the research.

For this study, using material from different types of sources is necessary to answer the research question. The material can be methodologically very diverse, including theoretical or conceptual research, and can also consist of gray literature such as conference publications and editorials. (Kangasniemi et al., 2013, p. 296.) It is also useful to complement research data with materials such as official policy documents (e.g., the U.S. Department of Defense's AI strategy or NATO Allied Command Transformation's digitalization strategy) as well as future research institute and think tank future scenarios, which would not be included in a purely systematic database search.

2.3.2 Identifying sources of relevant scientific literature

De Klerk and Pretorius (2019) propose a systematic approach to identifying relevant scientific literature, which includes peer-reviewed documents. This includes strictly defining keywords for a bibliographic database search. However, Grand and Booth (2009) also describe flexibility as one of the advantages of the critical review method. For the purpose of this study, the data was collected both implicitly and explicitly.

In implicit data collection, the research question actively guides the selection. Collection occurs in an information-centric and understanding-oriented manner, where the selection is made partially simultaneously with the analysis, and the report does not include details on the selected databases or evaluation criteria. The reliability and relevance of the data selection are addressed within the research text, reflecting on literature in relation to the research question. (Grant & Booth, 2009; Kangasniemi et al., 2013, p. 295.)

Explicit selection, on the other hand, closely resembles the reporting style of a systematic literature review, meaning it is done precisely and formally. Searches are manually conducted from selected publications and databases, utilizing time and language restrictions. Unlike a systematic literature review, predetermined limits can be deviated from during the process if necessary to answer the research question. The main characteristic of the selected data is its content and its relation to other collected data. The selection involves an ongoing two-way dialogue with the research question; both refine throughout the entire process. (Kangasniemi et al., 2013, p. 296; McCombes, 2023.)

For an overarching coverage through the explicit selection, 18 online databases were used. Taylor & Francis Online provides a one unified database of over 2700 journals, and ProQuest provides 17 different databases covering over 13000 scholarly journals. (*ProQuest*, 2024; *Taylor & Francis*, 2024.) Out of all of the databases available through University of Jyväskylä agreements these two provided the most accessible and usable combination.

2.3.3 Selecting and deselecting prominent literature

This step involves considering factors such as databases, time range, target participants, and methods for determining relevance. Inclusion and exclusion criteria are outlined, and literature is selected or deselected based on the presence of keywords in titles, abstracts, and full texts. (de Klerk & Pretorius, 2019.)

De Klerk and Pretorius (2019) propose an iterative selection pattern where first the title is searched for selected keywords, then the abstract and the full text. Each of the stages would be a deselecting criterion. Narrowing the literature this way has the risk of creating various false negatives, i.e., ruling out articles with usable content that is not mentioned in the title or the abstract. Admittedly for a well-focused and written study this should be low, but it can't be ruled out for grey literature. To mitigate this issue the initial searches were conducted from a broader perspective, i.e., searching for the relevant terms in the abstract first, and narrowing down from that.

The initial searches used and the subsequent deselection processes for the literature are described below in TABLE 3 Search queries and deselection. The search functionality available on Taylor & Francis and ProQuest differs slightly, so the exact queries used had to be adapted to be as closely identical as possible. Most notably, in ProQuest it is possible to define the query to include only documents with full text available, and to select only documents from scholarly journals. In Taylor and Francis this was not possible. Also, Taylor & Francis search didn't function correctly with nested AND and OR queries, so the search had to be split into separate queries to achieve the same results that could be achieved with a single search in ProQuest.

TABLE 3 Search queries and deselection

Taylor & Francis		**ProQuest**	
Operation	**Number of articles**	**Number of articles**	**Operation**
Search text "artificial intelligence" in Abstract AND Search text "military" in Abstract AND Publish date from 2022-01-02 to 2024-04-04	28	193	Search text "artificial intelligence" in Abstract AND (Search text "military" OR "warfare" OR "defense" OR "battlefield" OR "battlespace" in Abstract) AND Publish date from 2022-01-02 to 2024-04-04 AND Peer reviewed = Yes AND Full text = Yes AND Language = English AND Source type = Scholarly Journal
Search text "artificial intelligence" in Abstract AND Search text "warfare" in Abstract AND Publish date from 2022-01-02 to 2024-04-04	9		
Search text "artificial intelligence" in Abstract AND Search text "defense" in Abstract AND Publish date from 2022-01-02 to 2024-04-04	16		
Search text "artificial intelligence" in Abstract AND Search text "battlefield" in Abstract AND Publish date from 2022-01-02 to 2024-04-04	259		
Search text "artificial intelligence" in Abstract AND Search text "battlespace" in Abstract AND Publish date from 2022-01-02 to 2024-04-04	0		

Taylor & Francis in total	**312**	**193**	**ProQuest in total**
After removing duplicates and clear negatives based on title	74	172	After removing duplicates and clear negatives based on title
After removing incomplete records	74	170	After removing incomplete records
Total number of documents	**244**		**Total number of documents**

2.3.4 Data extraction

De Klerk and Pretorius propose that organizing the literature systematically is crucial for easy retrieval and use of data. They recommended a data extraction table to outline the components to be extracted and analyzed. They also propose that it would be important to provide clear criteria on why and which specific data components are extracted. (de Klerk & Pretorius, 2019.) This is more applicable to quantitative critical reviews, and due to the qualitative nature of this study and the amount of research material available the data extraction was carried out in a different manner.

The data was extracted by using an AI tool called Docalysis (www.docalysis.com), which was used to run a batch process on the 244 files collected. Docalysis is an AI-powered platform that analyses documents and answers questions about them. Users can upload PDF, TXT, CSV, or DOCX files and converse with Docalysis to get answers. It supports multiple languages and file types, including English, Spanish, Portuguese, French, Italian, Chinese, Japanese, Korean, Arabic, Indonesian, Hindi, Urdu, and more. The accuracy of the answers is surprisingly high, thanks to Docalysis' training on billions of lines of text, allowing it to provide answers with human-level intelligence. (*Docalysis - Frequently Asked Questions*, n.d..) The exact question used for the extraction was the following:

> I am looking for some ideas on how AI could be used in future conflicts, defense, warfare, crime and other security related matters. List the potential uses proposed in this document as a bulleted list, describe how AI is used in each case, and include the number of the page where you found the information. Do not include any other generic explanations in your answer.

The batch processing returned a CSV file with 2401 individual references to different potential uses. Some of the references included multiple items, so in practice the number of applications found in the documents was slightly higher. An example of the batch contents can be found in Appendix 1, Docalysis export sample.

2.3.5 Analyzing and synthesizing extracted data

De Klerk and Pretorius then propose a structured approach for analyzing and synthesizing data. They recommend either thematic analysis or content analysis

for qualitative synthesis, and meta-analysis is suitable for quantitative synthesis. (de Klerk & Pretorius, 2019.) Since this study is qualitative in nature, and aims for identifying strategic scale themes, thematic analysis was chosen as the analysis method.

Braun and Clarke (2006) give an excellent overview of running a thematic analysis in six steps:

1. Familiarizing yourself with your data
2. Generating initial codes
3. Searching for themes
4. Reviewing themes
5. Defining and naming themes
6. Producing the report

The process initiates when the analyst starts observing and actively seeking patterns of meaning and potential points of interest within the data, a stage that may coincide with data collection. The endpoint involves presenting the substance and significance of identified patterns (themes) in the data. These 'themes' are abstract, often somewhat vague constructs that investigators identify before, during, and after the analysis. Analysis requires a continual movement between the entire dataset, the coded extracts of data being examined, and the analysis of the data being generated. In contrast to statistical analyses, writing is an integral and ongoing aspect of the analysis, commencing in phase one with the initial jotting down of ideas and potential coding schemes and persisting throughout the entire coding/analysis process. (Braun & Clarke, 2006.)

The process is started by familiarizing yourself with the data (phase 1) and generating initial codes systematically (phase 2), identifying interesting features in each data item. It is important to code for numerous potential themes and patterns, to inclusively code data extracts to avoid losing context and to remember that an extract can be coded into multiple themes as relevant. (Braun & Clarke, 2006.)

Next, in phase 3, the analysis shifts to a broader focus on themes rather than codes. The process includes organizing various codes into potential themes and gathering all pertinent coded data extracts under these identified themes. Essentially, you begin to scrutinize your codes and explore how different codes might merge to create an overarching theme. (Braun & Clarke, 2006.)

In phase 4 Braun and Clarke (2006) propose to begin establishing potential themes and involves refining them. Some themes may lack support or merge, requiring adjustment or creation. Themes should cohere internally but maintain distinctions. They employ two review levels: level one assesses coherence within coded data extracts, and if the themes align, level two assesses the entire dataset's validity. The extracted data should be reread for theme validation, and any overlooked data should be coded within themes.

Phase 5 begins after establishing a satisfactory thematic map. This is the time to articulate and refine the analysis themes, focusing on their essence and

specific aspects within the data. It is good practice to avoid overloading themes or making them too complex. Each theme should be analyzed in detail, highlighting its unique contribution to the broader narrative around the research questions, ensuring minimal overlap. By the phase's end, each theme should have clear boundaries. This is tested by summarizing each theme in a couple of sentences; if clarity is lacking, further refinement is needed. (Braun & Clarke, 2006.)

Phase 6, 'Producing the report' in Braun and Clarke's (2006) description of the thematic analysis, and phase 6, 'Presenting the review findings and discussion', in de Klerk and Pretorius's (2019) description of critical review overlap, both describing presenting the review findings.

The actual process of how the analysis was conducted is described below in TABLE 4 Processing the data.

TABLE 4 Processing the data

Phase	**Steps conducted**
Phase 1	Getting familiar with 2401 items of the batch process results and cross-checking with the source files when the context of the entries was unclear.
Phase 2	Generating approximately 50 initial codes and coding the whole batch material with them (and with multiple codes when relevant). Again, also cross-checking with source files when the context of the entries was unclear.
Phase 3	Organizing various codes into potential themes and gathering all pertinent coded data extracts under these identified themes.
Phase 4	Refining the themes, with the final result of 27 themes.
Phase 5	Articulating and refining the analysis themes, focusing on their essence and specific aspects. Each theme was analyzed in detail, highlighting its unique contribution to the potential applications of AI while ensuring minimal overlap.

2.3.6 Presenting the review findings and discussion

The findings are presented to answer the original review question. The structure of the findings should be logical and critical, summarizing the impact and contribution of the included literature. (de Klerk & Pretorius, 2019.)

Furthermore, Braun and Clarke elaborate that it is crucial that when writing the final report and analysis, the text, including data extracts, presents a concise, coherent, logical, non-repetitive, and engaging account of the data story within and across themes. It is beneficial to offer ample evidence of the themes for example by using vivid examples or extracts that capture the essence of the demonstrated point without unnecessary complexity. The possible extracts are embedded within an analytic narrative that should compellingly illustrate the data story, going beyond mere description. The narrative should make a persuasive argument related to the research question. (Braun & Clarke, 2006.)

2.3.7 Conclusion and recommendations

The final step involves proposing new models, theories, hypotheses, or definitions based on critical thinking and analysis. Recommendations are derived from the critical analysis and synthesis of the included literature. (de Klerk & Pretorius, 2019.)

2.4 The structure of the study

The study opens up by describing the goals and methods used. The next section describes briefly what artificial intelligence is, the technology behind it, and the related cognitive aspects, physical world integrations and societal interactions. Following that, the study outlines what kind of developments are most likely going to have an effect on how AI is going to be utilized, including geopolitical and environmental forces, technological innovations and doctrinal and strategic paradigm shifts.

The final parts of the study describe how AI will most likely be going to be utilized in the battlespace and conflicts, some analysis and discussion outlining the model built for understanding the strategic effects and developments in the field of technology and warfighting, and in the end, conclusions.

3 WHAT IS ARTIFICIAL INTELLIGENCE?

Defining Artificial Intelligence (AI) in the modern context is very complex. According to Abbass (2021) AI is a multidisciplinary field that intersects with biology, philosophy, mathematics, metaphysics, and psychology, and that it is challenging to formulate a universal definition that gains consensus across these disciplines. He argues that while definitions should be concise and provide clear guidance, they also need to be flexible to allow for the growth of the field, and to foster meaningful discussions and reflections, even if they provoke disagreement or discomfort.

Abbass (2021) proposes two definitions of AI. The first definition is "*Artificial Intelligence is the automation of cognition*", which focuses on the technological aspect of AI, distinguishing it from mere software development and classic industrial automation. The second definition expands the scope to include social and ethical considerations:

> Artificial Intelligence is social and cognitive phenomena that enable a machine to socially integrate with a society to perform competitive tasks requiring cognitive processes and communicate with other entities in society by exchanging messages with high information content and shorter representations. (Abbass, 2021)

This definition views AI not just as technology or a product but as a social and cognitive phenomenon. FIGURE 1 AI in the surrounding society, illustrates the key domains that AI relates to, and the following chapters will outline the current capabilities, challenges and potential future developments on a high level in each of the domains.

The core of an AI solution is the technology used to create the solution itself, and the cognitive capability of the system, i.e., the capability to observe and orient, make decisions and to gather feedback. The solution is used for something by people, possibly in an organization. The people interact with the solution through a user interface, which could consist of text, images and/or speech. The solution itself interacts with the surroundings using different types of sensors, such as audio, video and others, but also could be able to manipulate the

surroundings using robotics. All of this has effects to the wider surrounding society in legal, ethical, economical, scientific, educational and other aspects.

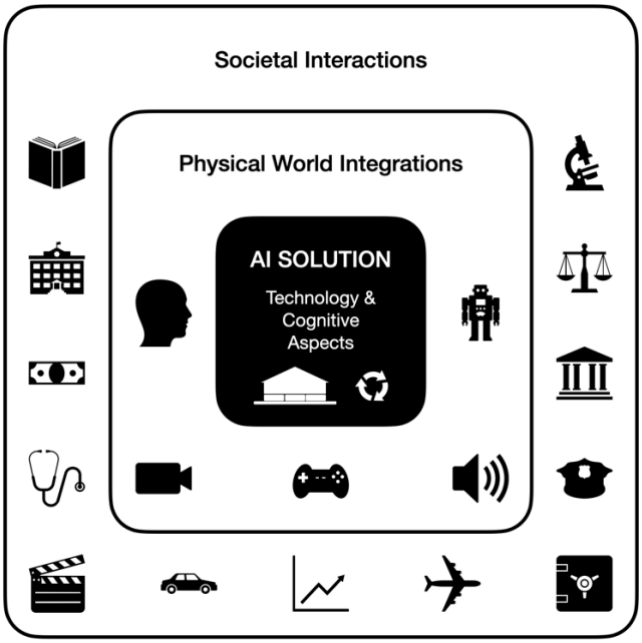

FIGURE 1 AI in the surrounding society

The overview of the domains surrounding AI solutions presented in this chapter is presented on a general, strategic level, and as such, is far from exhaustive and complete. The context of this work does not allow for deeper study in the topics, as each of them could be the topic of a thesis of its own. However, in order to provide the reader with a basic understanding of the landscape, even a limited overview such as this is useful.

3.1 Technology behind artificial intelligence

Van Assen et al. (2020) list the key technological enablers of artificial intelligence as big data, high-performance computing (HPC), and algorithms, as described below in FIGURE 2 House of artificial intelligence. Mathematics and computer science are the land the house is built on, and big data, HPC and algorithms are the foundation, with the house itself containing all the AI capabilities available.

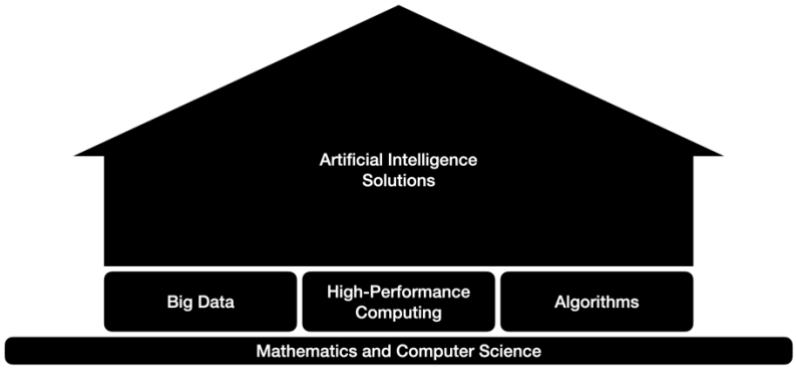

FIGURE 2 House of artificial intelligence

3.1.1 Big data

Big data refers to the large and rapidly expanding datasets that are now collected by various information-sensing devices such as mobile devices, aerial cameras, microphones, and sensor networks. Big data is essential for AI modeling, especially when using deep learning techniques that require large heterogeneous training datasets. (van Assen et al., 2020.)

3.1.2 High-performance computing

HPC infrastructure is critical for handling big data sets. Typical local computing infrastructure with limited resources cannot cope with the demands of big data. AI algorithms need powerful processes across computer, networking, and storage systems, and usually the most cost-effective way to secure those is through different cloud computing providers. In the context of this study, it is important to note that public cloud services cannot be used for all defense and security applications. However, most large-scale on-premise AI implementations benefit from similar HPC architecture and implementations. The availability of HPC cloud computing has been a game-changer for AI adaptation and scientific discoveries. It has allowed a broader range of people to train AI algorithms with extremely large datasets, democratizing access to AI development. (van Assen et al., 2020.)

3.1.3 Machine learning

The true capabilities of AI come from machine learning (ML) algorithms, which are broadly categorized into supervised and unsupervised learning algorithms. Supervised learning involves learning associations from classified and labeled training datasets, while unsupervised learning explores the internal structure of the data without targeted outcomes (van Assen et al., 2020). Complementing the two main types there is semi-supervised learning that combines qualities from both supervised and unsupervised learning algorithms (Dang et al., 2022), and reinforcement learning where the algorithm utilizes structured learning methods to adapt through trial and error (Militani et al., 2021). The different types of ML

algorithms are described in more detail in TABLE 5 Main machine learning algorithm types below.

TABLE 5 Main machine learning algorithm types

Supervised learning	The machine learns from examples provided by the operator. The operator furnishes the machine learning algorithm with a labeled dataset containing input-output pairs, and the algorithm endeavors to discern patterns that link these pairs. Although the operator possesses the correct solutions, the algorithm learns through observation and prediction. The algorithm predicts outcomes and receives corrections from the operator, iterating until it achieves a satisfactory level of accuracy or performance. (van Assen et al., 2020.)
Unsupervised learning	Algorithms that analyze data to uncover patterns without the aid of an answer key or human guidance. Instead, the machine autonomously discerns correlations and relationships within the available data. Through this process, the algorithm attempts to organize the data to reveal its underlying structure, which may involve clustering similar data (grouping similar data sets based on predefined criteria, facilitating the segmentation of data into distinct clusters for pattern analysis) or reducing dimensions (by reducing the number of variables under consideration while retaining crucial information, aiding in simplifying complex data sets) to extract essential information. (van Assen et al., 2020.)
Semi-supervised learning	Utilizes both labeled and unlabeled data, with the former containing meaningful tags for the algorithm's comprehension, while the latter lacks such information. By leveraging this combination, machine learning algorithms can learn to assign labels to unlabeled data, as an intermediary method between unsupervised and supervised learning. (Dang, 2022.)
Reinforcement learning	Focuses on structured learning paradigms, providing machine learning algorithms with predefined actions, parameters, and desired outcomes. By establishing rules, the algorithm explores various options and evaluates each outcome to determine the most favorable course of action. Through trial and error, reinforcement learning allows the machine to adapt its approach based on past experiences, aiming to achieve optimal results in varying scenarios. (Militani et al., 2021.)

With the advancements in big data and HPC, ML algorithms have become more complex. Deep learning (DL) approaches can be utilized in all the above-mentioned types of ML algorithms, creating a subset of DL algorithms. DL algorithms utilize several layers of neural networks, which feature, in turn, millions of densely connected processing nodes (neurons) that attempt to replicate the functionality of the human brain. These algorithms have multiple layers of processing and can perceive nonlinear structures within the data. Both deep and shallow types of ML have their own strengths and weaknesses, and

each should be used in the right contexts. (Pouyanfar et al., 2018; Robles Herrera et al., 2022.)

3.2 Cognitive aspects

Cognitive aspects of AI arise from Abbass's (2021) second definition. He describes how AI is a cognitive phenomenon that integrates with a society, performs tasks requiring cognitive processing and communicates with others. The first key phase of a cognitive process of an AI is observing and orienting, which covers things like acquiring information and rules for both representing and using it. Based on that, the system is ready to start reasoning and making decisions, i.e., using algorithms and rules to reach approximate or definite conclusions. This phase also includes handling uncertainty and probabilities. The final phase of the cognitive cycle is gathering feedback for self-correction, covering adapting behavior over time, leveraging knowledge from one domain to another, and generalizing learnings to new tasks or environments. This is illustrated in FIGURE 3 AI cognitive process.

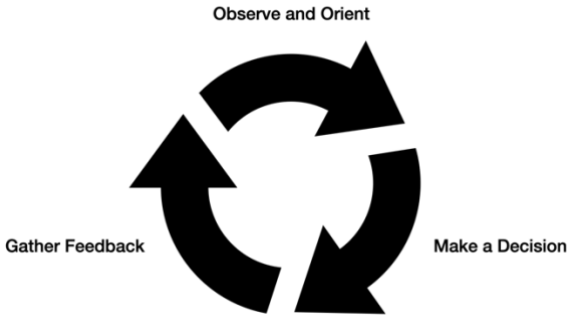

FIGURE 3 AI cognitive process

3.2.1 Observing and orienting

In addition to the initial learning used to create and to teach the AI system described above in section 3.1, Technology behind artificial intelligence, the system also learns about the surroundings using different sensors, described in more detail below in section 3.3, Physical world integrations. The cognitive aspects most focused on in this section include rules for both representing and using the information in a given context. The topic is very wide, but a few interesting developments outline the directions research is currently taking.

Wang (2020) discusses technologies that map logical relations into neural network structures. This model enables dynamic construction and adjustment of neural network structures based on logical relations, offering potential applications in fields like medical diagnosis and robotics. Despite its strengths,

the model faces challenges such as computational complexity and interpretability issues. (Wang, 2020.)

On the other hand, Skarding et al. (2021) focuses on dynamic networks, which provide a framework for representing complex systems that evolve over time. These networks encode both structural and temporal patterns, allowing for accurate modeling and prediction of changes in various domains. Again, they come with computational complexity and a cold start problem, necessitating further research to fully leverage these technologies. (Skarding et al., 2021.)

Both of the studies highlight interesting current possibilities of storing and representing information. These advancements offer promising avenues for understanding and predicting the behavior of dynamic systems, though challenges remain to be addressed for optimal utilization of these technologies. The foundation for the full cognitive cycle depends on the work done in this step.

3.2.2 Making a decision

AI engages the environment in intricate processes of reasoning and decision-making, emulating human cognitive functions to deduce conclusions, forecast outcomes, and formulate strategies based on existing knowledge. This capacity is fundamental to AI's diverse applications, such as expert systems, natural language processing, autonomous vehicles, and healthcare diagnostics. At the core of AI reasoning is its adeptness at sifting through vast data sets, employing algorithms and rules to arrive at either approximate or definitive conclusions, even amidst conditions of uncertainty.

AI reasoning encompasses various types, each characterized by distinct methodologies and domains of application. Deductive reasoning, for example, follows a top-down approach, commencing with general statements or hypotheses to derive specific conclusions. Rooted in the logical structure of statements and the validity of premises, deductive reasoning is prominent in domains like mathematics and logic, where it constructs indisputable theorems from foundational axioms and rules. (Calimeri et al., 2021.)

Conversely, inductive reasoning employs a bottom-up strategy, drawing generalizations from specific observations. While premises support conclusions, they do not ensure their absolute truth, rendering inductive reasoning prevalent in scientific exploration and hypothesis generation. This form of reasoning empowers AI systems to glean patterns from data, facilitating predictions about future events or behaviors. (Spelda, 2020.)

Abductive reasoning diverges from both deductive and inductive reasoning by commencing with an incomplete set of observations and seeking the most plausible explanation. Particularly valuable in diagnostic contexts, abductive reasoning aids AI systems in inferring potential causes for observed symptoms or conditions, significantly benefiting fields like medicine. (Garbuio & Lin, 2021.)

A significant hurdle in AI reasoning and decision-making lies in navigating uncertainty. While traditional models such as Markov Decision Processes (MDPs) effectively handle the aleatoric uncertainty related to data and outcome

randomness, they falter in addressing epistemic uncertainty arising from incomplete system or environmental knowledge. (Hoey et al., 2016.)

Recent AI research strides focus on developing models and algorithms adept at managing both forms of uncertainty. Decision theory offers a framework for decision-making under uncertainty, integrating subjective degrees of belief (probabilities) with outcome preferences. This systematic approach enables the evaluation of different actions based on their anticipated outcomes and the decision-maker's inclinations. (Garbuio & Lin, 2021; Hoey et al., 2016; Jiang et al., 2022; Lochner & Smilek, 2023.)

Furthermore, the distinction between aleatoric and epistemic uncertainty spurs exploration into uncertainty models offering more robust interpretations. These models endeavor to capture the inherent unpredictability of complex systems and environments, equipping AI systems to make well-informed and dependable decisions. (Garbuio & Lin, 2021; Hoey et al., 2016; Jiang et al., 2022; Lochner & Smilek, 2023.)

AI reasoning and decision-making epitomize the capacity of artificial intelligence to emulate human cognitive processes effectively. By leveraging diverse forms of reasoning and confronting challenges in decision-making under uncertainty, AI systems can make informed decisions, assimilate experiential insights, and adapt to evolving information landscapes. Ongoing research endeavors aim to augment AI's capabilities, cementing its status as a dependable and potent tool across diverse domains.

3.2.3 Gathering feedback

Integral to AI reasoning and decision-making is the capacity for learning from errors and self-correction. This capability fosters continual improvement and adaptation of AI systems to evolving information and environments. Recent studies delve into the concept of self-correction in AI, particularly evident in large language models like ChatGPT. However, these models face limitations due to static data uploads hindering the unlearning of outdated or erroneous information. (Lochner & Smilek, 2023.)

Efforts to imbue AI systems with the ability to unlearn and self-correct emulate human learning processes. The self-correction mechanisms may be automatic, or they may operate in conjunction with the human operator, requesting for feedback and corrections. Human input is usually accurate but limited in scope. Automatic systems such as streaming workflows enable real-time data processing and updating, allowing AI systems to independently rectify inaccuracies and biases in their knowledge base, thereby enhancing reliability and performance. (Hasanujjaman et al., 2023; Ryan, 2020.)

Autonomous self-correction holds particular significance within decision support systems, where trustworthiness and accuracy are paramount. The study conducted by Lochner and Smilek (2023) delves into the dynamics of trust formation in autonomous systems, investigating how self-correction influences human trust in such systems. Their experiments reveal that the impact of self-correction on trust varies based on the system's accuracy and response speed.

While high accuracy generally fosters trust, the introduction of self-correction may paradoxically diminish trust, potentially due to heightened awareness of errors. This underscores the importance of judiciously implementing self-correction to avoid unintended consequences on user trust. (Lochner & Smilek, 2023.)

In the realm of medical imaging, Wang et al. (2023) present a deep semi-supervised multiple instance learning framework that incorporates self-correction. Their approach integrates a small set of labeled data with a larger pool of unlabeled data, employing a self-correction strategy to refine the system's performance iteratively. This strategy involves confidence-based pseudo-labeling and consistency regularization, enabling the system to enhance its accuracy over time by focusing on high-confidence predictions. The study showcases the feasibility of employing semi-supervised learning with self-correction to achieve heightened classification accuracy at a reduced annotation cost. (X. Wang et al., 2023.)

The demonstrated capabilities of self-correction in AI systems hold promise for enhancing the reliability and trustworthiness of automated decision-making processes. By facilitating systems to learn from errors and adapt their behavior autonomously, self-correction can drive continuous performance improvement over time, particularly beneficial in fields like healthcare, where data labeling costs and expertise constitute significant barriers. Using the autonomous self-correction mechanisms together with operator feedback enable the system to reliably improve in the given context.

3.3 Physical world integrations

Abbass (2021) also describes several real-world AI integrations in his second definition: a machine integrates with a society to perform competitive tasks, and to communicate with other entities. Real-world integration involves incorporating AI into existing systems and businesses. It spans domains like computer vision, robotics, speech to text, natural language processing (NLP), perception, human-machine interaction, emotion recognition, and human-machine teaming. Deployment and integration ensure AI systems seamlessly fit into real-world workflows with scalability and reliability.

3.3.1 Automatic speech recognition

Speech is the most natural communication and interaction medium for humans, which is why automatic speech recognition (ASR) is a key focus area in real-world interactions with AI systems. Recent years have witnessed remarkable advancements in ASR technology, largely propelled by deep learning and neural network methodologies. ASR systems now exhibit a remarkable ability to convert human speech into readable text with ever-improving accuracy, nearing

human-level performance in specific contexts. (Arachchi Dimuthu Maduranga & Dinesh Samarasinghe, 2023.)

These advancements have paved the way for diverse applications of ASR technology, ranging from real-time captioning on social media platforms to transcription services in video conferencing and customer service interactions. ASR systems play a pivotal role in the functionality of smart speakers, conversational AI, and autonomous vehicles, enabling them to comprehend and respond to human commands accurately. Here, speech recognition technology not only enhances user experience but also contributes to safety by reducing distractions for drivers. This application underscores the transformative potential of speech recognition in refashioning various industries, making interactions more intuitive and systems more efficient. (Arachchi Dimuthu Maduranga & Dinesh Samarasinghe, 2023; Xu, 2022.)

A significant milestone in ASR development has been the transition from traditional machine learning techniques to deep learning approaches. This shift has led to substantial accuracy enhancements, with some ASR systems achieving error rates comparable to those of human transcribers in specific benchmark tests. (Beaver, 2022.)

However, despite these strides, ASR technology encounters several challenges. Variability in speech patterns, including accents, dialects, and individual styles, poses a significant hurdle to recognition accuracy. Particularly, non-native speakers of a language often experience higher error rates when utilizing ASR systems. Moreover, environmental factors such as background noise and recording equipment quality can adversely affect ASR performance. Another limitation lies in the reliance on benchmarks that may not fully represent the diversity and complexity of real-world speech. ASR systems still grapple with speech disorders, technical jargon, and non-standard speech patterns. (Arachchi Dimuthu Maduranga & Dinesh Samarasinghe, 2023; Beaver, 2022.)

Nevertheless, the current state of ASR technology is already impressive, and the future holds more promise. Innovations such as self-supervised learning systems and end-to-end deep learning models are anticipated to bolster accuracy and diminish the necessity for extensive labeled training data. These advancements could foster more robust and adaptable ASR systems capable of navigating the intricacies of human speech. (Beaver, 2022; Xu, 2022.)

While ASR technology has made remarkable strides and is increasingly ubiquitous in various applications, achieving universal human parity remains elusive. The efficacy of the technology varies widely depending on context and speakers involved. Ongoing research and development endeavors aim to address these challenges, aspiring to create ASR systems adept at reliably understanding and transcribing human speech across diverse conditions and use cases. Continued research and innovation in areas such as natural language processing and understanding will be essential for unlocking the full potential of speech recognition in enabling more natural and meaningful interactions between humans and machines. Overall, the future of speech recognition holds promise

for delivering enhanced user experiences, improved efficiency, and greater accessibility across a wide range of applications and industries.

3.3.2 Computer vision

AI systems can be integrated to a wide array of different types of sensors. All of the sensors can provide vital information for real-world integration in a particular application, but as one of the most prevalent sensor technologies, computer vision boasts a wider array of capabilities than other sensor types. There has been substantial progress in enabling computers to see, interpret and comprehend information from the world around us. Fueled by advancements in machine learning, particularly deep learning techniques, and the availability of vast datasets, current computer vision systems possess extensive capabilities that continue to evolve. (Matsuzaka & Yashiro, 2023; Sagodi et al., 2022; Sharma et al., 2022.)

Modern computer vision systems excel at tasks traditionally performed by humans, often surpassing human speed and accuracy. These tasks encompass image classification, object detection, facial recognition, and real-time video analysis. The utilization of convolutional neural networks (CNNs) and recurrent neural networks (RNNs) has been particularly instrumental in advancing these capabilities. CNNs are proficient in recognizing patterns and categorizing images, while RNNs excel in understanding temporal dynamics in videos, making them suitable for tasks involving motion or temporal changes. (Bhatt et al., 2021; Cuhadar & Tsao, 2022.)

The applications of computer vision span across multiple industries, impacting manufacturing, healthcare, retail, agriculture, autonomous vehicles, and interactive entertainment. In manufacturing, AI-powered computer vision systems ensure quality control by meticulously inspecting parts and identifying imperceptible defects (Sagodi et al., 2022). In healthcare, these systems aid in medical imaging analysis, aiding in disease diagnosis by detecting abnormalities in X-rays, MRIs, and CT scans (Esteva et al., 2021). Retail benefits from automated checkouts enabled by computer vision, which recognizes items in shopping carts without manual barcode scanning (Wei et al., 2020). In agriculture, computer vision monitors crop health and optimizes farming practices (Ouhami et al., 2021).

Computer vision is integral to the development of autonomous vehicles, enabling interpretation of traffic environments and detection of pedestrians, vehicles, and traffic signs (Chuprov et al., 2023; Hasanujjaman et al., 2023; Sarvajcz et al., 2024; Yessenbayev et al., 2022). In interactive entertainment, it offers immersive experiences by responding to user movements and expressions (Bermejo-Berros & Gil Martínez, 2021; Chen et al., 2020).

Despite their remarkable capabilities, computer vision systems encounter challenges and limitations. One significant challenge is their reliance on extensive labeled datasets for training, which can be laborious and resource-intensive to create (Sagodi et al., 2022). Additionally, these systems may struggle with image

processing under varying conditions such as changes in lighting or occlusions (Cuhadar & Tsao, 2022).

Another challenge lies in the requirement for specialized expertise to develop and maintain computer vision systems effectively. Furthermore, hardware or software issues can lead to system failures, potentially disrupting critical operations. Computer vision systems are also sensitive to deployment environments, necessitating careful consideration during design and deployment to ensure reliable operation (A. Sharma et al., 2022).

The literature underscores the transformative potential of computer vision while acknowledging practical challenges. While computer vision systems continue to evolve impressively, addressing issues such as data management, system reliability, and the need for specialized expertise remains critical. Various sources emphasize the importance of cross-functional collaboration, expectation management, and continuous improvements in algorithm efficiency and hardware technologies.

In conclusion, computer vision holds promise for remodeling diverse industries, but its full potential hinges on overcoming significant challenges. As technology advances, addressing these challenges will be pivotal for widespread adoption and successful integration across different sectors. Future progress will likely involve a combination of architectural innovations, improved training methodologies, and endeavors to enhance interpretability and explainability in AI systems.

3.3.3 Sensor fusion

Sensor fusion has emerged as a critical technology in AI systems, enabling more accurate, reliable, and comprehensive environmental perception by integrating data from multiple sensors. This technology is pivotal across various domains, including autonomous vehicles, robotics, smart cities, and healthcare, enhancing decision-making processes and operational efficiency.

The current capabilities of sensor fusion in AI systems are multifaceted, focusing on improving the accuracy and reliability of environmental perception. AI-based sensor fusion, as discussed in the work of Zoghlami et al. (2021), leverages deep neural networks to analyze combined data from different sensors, such as cameras, lidar, radar, and ultrasonic sensors, to create a bi-functional system that evaluates single sensor contributions in classification tasks. This approach not only enhances classification accuracy but also evaluates the robustness and contribution of each sensor, enabling a more interpretable and smart decision-making process. Similarly, Leung et al. (2019) highlight the use of AI in integrating transportation data from GNSS/GPS, accelerometers, and GIS for better urban mobility analysis, aiming towards smarter city management. These capabilities underscore the potential of sensor fusion in creating more intelligent and responsive systems. (Zoghlami et al., 2021.)

The possibilities of sensor fusion technologies are vast, with ongoing advancements promising even more sophisticated and reliable fusion techniques. Future developments are expected to yield AI and machine learning

algorithms that can process data more efficiently, with a focus on energy-efficient sensor systems and greater environmental adaptability (A. Sharma et al., 2022). Such advancements could significantly impact various sectors, including automotive for higher levels of automated driving (Zoghlami et al., 2021), industrial applications for predictive maintenance (Gawde et al., 2024), and urban planning for enhanced smart city functionalities (T. Johnson et al., 2023).

However, sensor fusion in AI systems is not without its weaknesses. One of the main challenges lies in dealing with the heterogeneity and complexity of sensor data, which may have different formats, resolutions, and error models. This necessitates the development of sophisticated methods for aligning, synchronizing, calibrating, and transforming sensor data before fusion. Additionally, the choice of the optimal sensor fusion algorithm and architecture is crucial and challenging, given the plethora of available methods, each with its advantages and disadvantages. Another significant challenge is evaluating the performance and quality of sensor fusion results, which depend on various factors such as accuracy, reliability, and timeliness of the sensor data and fusion method. (Gao et al., 2023; Leung et al., 2019; Sharma et al., 2022.)

Moreover, recent research by Gao et al. (2023) on AI-enabled multi-sensor fusion systems reveals vulnerabilities in current systems, indicating a lack of robustness against signal loss from specific sensors. This finding suggests that existing AI-enabled multi-sensor fusion systems may not be adequately designed to handle the loss of signal from one or more sensors, highlighting a critical area for future improvement. (Gao et al., 2023.)

While sensor fusion in AI systems offers remarkable capabilities and possibilities for enhancing environmental perception and decision-making across various domains, it also faces significant challenges. Addressing these challenges, particularly in terms of data heterogeneity, algorithm and architecture optimization, and system robustness, will be crucial for realizing the full potential of sensor fusion technologies.

3.3.4 Human-machine interfaces

Human-machine interfaces (HMIs) have undergone significant evolution with the emergence of AI, resulting in enhanced capabilities in teamwork, interaction, emotion recognition, and augmented intelligence. These interfaces now play integral roles across diverse sectors, including healthcare, defense, and consumer electronics.

Human-machine teaming (HMT) involves collaborative efforts between humans and AI systems to achieve shared objectives. Current capabilities emphasize leveraging the unique strengths of both parties: humans contribute nuanced understanding and adaptability, while machines offer speed, consistency, and data processing power. (Gonzalez et al., 2023.) For instance, in healthcare, clinicians collaborate effectively with machine learning systems to enhance patient outcomes, despite limited insight into the underlying algorithms (Esteva et al., 2021; Oniani et al., 2023a). Similarly, in defense applications, improved human-machine teamwork has demonstrated faster task completion

with reduced errors (J. Johnson, 2024; P. Sharma et al., 2020). However, challenges such as over-reliance on AI systems leading to automation bias and the necessity for effective communication and mutual understanding persist, crucial for successful collaboration (Saenz et al., 2020).

AI advancements have rendered human-machine interaction (HMI) more natural and intuitive. AI-driven systems can now comprehend and respond to human gestures, speech, and other non-verbal cues, facilitated by the integration of multimodal interfaces tailored to user preferences (Adel et al., 2023; Gao et al., 2023). Yet, limitations arise from potential misinterpretation of human intent by AI systems and the requirement for humans to adapt to machine interaction methods, which may not always align with intuition (Elyoseph et al., 2024).

AI systems have made notable progress in emotion recognition by analyzing facial expressions, voice tones, and physiological signals, enabling empathetic and personalized interactions. However, challenges include accuracy issues, especially in complex emotional states or across diverse cultural contexts, and concerns regarding privacy when AI systems collect and analyze personal emotional data. (Jiang et al., 2022.)

AI systems are increasingly designed to complement human capabilities, enabling a synergy where each party compensates for the other's shortcomings. This cooperation enhances efficiency and productivity by allowing AI to handle repetitive tasks while humans focus on creative and strategic aspects. Yet, maintaining a balance where AI supports rather than supersedes human roles remains a challenge, ensuring continued engagement and value for the human workforce. (Jiang et al., 2022; Saenz et al., 2020.)

Augmented intelligence entails AI systems enhancing human cognitive abilities without replacing them. AI assists in decision-making, predictive analytics, and complex problem-solving, evident in fields like radiology where AI aids in interpreting medical images. However, challenges include potential errors due to biased data or algorithms, leading to misplaced trust in AI-generated conclusions. (Gonzalez et al., 2023; Jiang et al., 2022; Zoghlami et al., 2021.)

The future holds vast possibilities for HMIs, potentially enabling brain-machine interactions and further streamlining interactions. Yet, ethical AI usage, privacy protection, and bias prevention present ongoing challenges. HMIs in AI systems boast impressive capabilities, but addressing associated weaknesses and striking a balance between leveraging AI's strengths and mitigating its limitations are essential for realizing their full potential.

3.3.5 Physical interaction with the environment

The fusion of robotics with AI systems has undergone significant evolution, empowering these systems to engage with the physical world in increasingly sophisticated manners.

Robotics within AI systems have transcended basic, repetitive functions, now capable of executing intricate, autonomous tasks demanding precision and adaptability. Noteworthy advancements are exemplified in autonomous surgical

robotics, where AI-equipped robots undertake surgical procedures with minimal human intervention, showcasing remarkable autonomy and precision. For instance, the development of the Smart Tissue Autonomous Robot (STAR) and its successful application in soft tissue surgeries underscore the potential for robotics to conduct complex medical procedures with heightened efficiency and safety compared to conventional methods. (Sonmez, 2022.) This progression extends beyond healthcare, with robotics integrated into AI systems across diverse sectors such as manufacturing, service industries, and exploration.

The potential applications of robotics within AI systems are extensive. In the medical realm, autonomous robots hold promise in greatly improving surgical practices, mitigating human error, expediting recovery periods, and enhancing accessibility to complex procedures (Sonmez, 2022). Beyond healthcare, robotics can bolster service industries, exemplified by the European restaurant sector's adoption of AI and robotics to automate service delivery and enhance customer interactions (Blöcher & Alt, 2021). In manufacturing, robotics can elevate productivity, refine product quality, and ensure occupational safety by assuming hazardous tasks (Huang et al., 2021; Sagodi et al., 2022).

Notwithstanding these advancements, notable weaknesses and challenges persist. Foremost among these concerns is the reliability and trustworthiness of autonomous systems. As autonomous robots undertake increasingly intricate and pivotal tasks, ensuring their reliability becomes imperative. Sonmez (2022) illustrates widespread apprehension and reluctance among individuals to undergo robotic procedures, rooted in concerns and discomfort stemming from the absence of human involvement. This underscores the necessity for further research and development to cultivate trust in and acceptance of autonomous robotics. (Sonmez, 2022.)

Technical constraints of current robotics technology present another challenge. While substantial strides have been made, limitations persist in terms of manual dexterity (Negrello et al., 2020), decision-making amid uncertainty (Zoghlami et al., 2021), and adaptability to unforeseen circumstances (Mazzolai et al., 2022). These limitations are particularly pronounced in high-stakes domains like surgeries, where autonomous systems must navigate diverse scenarios with precision and flexibility.

Furthermore, ethical and regulatory considerations pose substantial hurdles to the widespread integration of robotics into AI systems. As these systems assume roles entailing greater autonomy and impact on human lives, addressing ethical concerns surrounding accountability, privacy, and potential job displacement becomes increasingly paramount. (Chatterjee, 2019; Gervais, 2023; Robbins, 2020.)

The integration of robotics into AI systems heralds remarkable capabilities and prospects, ranging from intricate surgeries to transformative service delivery across various sectors. As research and development in this realm progress, it is imperative to strike a balance between innovation and considerations of safety, ethics, and societal implications.

3.4 Societal interactions

Abbass's (2021) also emphasizes the examination of social and ethical perspectives, highlighting AI's integration into society, participation in tasks, and communication within communities. This underscores the significance of comprehending AI's societal effects, competitiveness, and community engagement. Critical factors entail ensuring AI systems' explainability and interpretability for trust and accountability, addressing ethical concerns like algorithmic bias, job displacement, privacy issues, and evaluating AI's broader societal ramifications.

3.4.1 Ethics

Ethical considerations surrounding AI systems are intricate and multifaceted, touching upon various aspects of human life and societal functioning. Through discussions presented in articles by Ryan (2020), Kieslich et al. (2022) and Ryan and Stahl (2020), a convergence on certain ethical principles emerges, although nuanced differences exist in their interpretation and application. Some of the ethical challenges include privacy, safety and security, fairness and bias, autonomy and human agency.

Extensive data collection for AI systems raises significant privacy concerns. Surveillance and unauthorized data usage without consent may threaten individual privacy and autonomy (Kieslich et al., 2022). Some uses can also cause safety and security issues as the systems can cause unintended harm, either through malfunction or malicious use. Such cases include for example physical safety in autonomous vehicles or drones, and cybersecurity risks. (Ryan & Stahl, 2020.)

AI systems, trained on biased data, can perpetuate or exacerbate existing biases, leading to unfair outcomes for certain groups. This raises concerns about justice and equality, particularly regarding discrimination based on race, gender, or other social categories. (Ryan & Stahl, 2020.) Systems with decision-making capabilities may pose challenges to human autonomy and agency. Over-reliance on AI may undermine human decision-making processes, potentially leading to a loss of control over significant life decisions. (Kieslich et al., 2022.)

To combat these challenges, the authors suggest a number of solutions, such as ethical guidelines and principles, collaboration, regulation and education.

Emphasizing the importance of comprehensive ethical guidelines and frameworks, both articles advocate for clear principles governing the development and use of AI systems. These guidelines should address transparency, fairness, privacy, and other ethical concerns, providing a roadmap for responsible AI development. Integrating ethical principles directly into the design and development process of AI systems is also proposed. This includes enhancing transparency and explainability, detecting and mitigating bias, and ensuring that AI systems respect user privacy and autonomy. (Kieslich et al., 2022; Ryan & Stahl, 2020.)

Engaging a wide range of stakeholders, including ethicists, social scientists, policymakers, and the public, in the development and governance of AI systems is crucial. This multidisciplinary collaborative approach ensures diverse perspectives and values are considered, leading to more ethically robust AI systems. (Kieslich et al., 2022; Ryan & Stahl, 2020.)

Regulatory frameworks and oversight mechanisms are deemed necessary to ensure compliance with ethical standards and principles. This could involve independent auditing of AI systems, certification processes, and the establishment of regulatory bodies dedicated to AI ethics. In addition, raising awareness about the ethical implications of AI among developers, users, and policymakers is essential. Education and training programs can equip stakeholders with the knowledge and skills needed to address the ethical challenges posed by AI. (Kieslich et al., 2022; Ryan & Stahl, 2020.)

Nevertheless, the challenge persists in implementing these ethical guidelines in practice. The ongoing effort involves developing standards, tools, and methods to ensure that AI systems adhere to these principles. Furthermore, philosophical and conceptual analyses are required to ensure the consistency and justification of the normative statements found in AI ethics literature.

Addressing the ethical challenges in AI systems requires a multifaceted approach. While there is consensus on the key ethical issues and general solutions, implementing these solutions remains a challenge, necessitating ongoing dialogue and collaboration among all stakeholders involved in AI development and use.

3.4.2 Financial and judicial effects

AI systems have a variety of impacts on society, offering significant opportunities while also presenting notable threats. Recent discussions on AI, as evidenced by articles from Acemoglu et al. (2022) and Gervais (2023), shed light on its transformative effects on labor markets and legal systems as key examples of this diverse topic.

Acemoglu et al. (2022) conducted an empirical analysis of AI's influence on labor markets in the United States. Their research reveals a rapid growth in AI-related job vacancies, primarily driven by establishments whose tasks align with AI's capabilities. While this growth suggests a restructuring of job tasks, with AI replacing some human-performed tasks and introducing new ones with different skill demands, the aggregate effects on employment and wage growth in affected occupations and industries are currently minimal. This indicates that while AI adoption leads to notable declines in establishment hiring, any positive productivity or complementarity effects are outweighed by displacement consequences. (Acemoglu et al., 2022.)

Gervais (2023) delves into the unprecedented challenges AI poses to legal systems, highlighting the emergence of autonomous intelligent agents capable of cognitive tasks. This raises questions regarding the applicability of human laws to non-human entities. Gervais argues for regulatory frameworks integrating ethical norms into AI systems to ensure alignment with human values and legal

standards. He emphasizes the need for mechanisms, like "kill switches," to interrupt AI processes, maintaining human control to prevent potential harm. (Gervais, 2023.)

Economic insights necessitate rethinking labor market policies and education systems, while legal and ethical considerations call for proactive regulation to align AI systems with human values and legal norms. The societal impact of AI encompasses both opportunities and threats in many more areas than the two examples used here, requiring a balanced approach to leverage its benefits while mitigating risks. Current insights underscore the need for interdisciplinary efforts to address economic, legal, and ethical challenges. As AI evolves, ongoing research and policy development will be crucial in shaping a future where AI systems contribute positively to society.

3.4.3 Trust and accountability

The issue of trust, accountability, and explainability in AI systems is a multidimensional and intricate matter that has attracted considerable attention from both academia and policymakers. This brief discussion on the key points aims to provide insights into the broader landscape of these concerns.

Mark Ryan's "In AI We Trust: Ethics, Artificial Intelligence, and Reliability" (2020) critically analyzes trust in AI, arguing that AI cannot be trusted in the same manner as humans due to its lack of emotive states and responsibility capacity. Ryan differentiates between trust and reliance, suggesting that while AI can fulfill the criteria of rational trust based on prediction and reliability, it falls short in meeting the emotional and normative aspects of trust that involve emotive goodwill or moral obligations. This differentiation underscores AI's limitations in establishing trust-based relationships and underscores the necessity for clear accountability mechanisms. (Ryan, 2020.)

In "Artificial Intelligence Ethics Guidelines for Developers and Users: Clarifying Their Content and Normative Implications" by Mark Ryan and Bernd Carsten Stahl (2020), the authors delve into the normative content of AI ethics guidelines, offering detailed recommendations for developers and users. They stress the significance of transparency, justice, fairness, and non-maleficence, among other principles, asserting that AI systems should be designed and used in ways that uphold human rights, privacy, dignity, and well-being. Additionally, they emphasize the importance of AI systems being explainable, enabling users to comprehend and potentially challenge AI decisions. (Ryan & Stahl, 2020.)

It is evident that while there is agreement on the necessity for ethical AI systems that are transparent, accountable, and explainable, there is also acknowledgment of AI's inherent limitations in fostering human-like trust. While AI systems should be developed with ethical considerations in mind, the current technological landscape does not facilitate the establishment of trust relationships comparable to those between humans.

Complex algorithms can render AI decisions opaque, challenging user understanding and hindering accountability, potentially eroding trust in these

systems. The concept of explainability serves as a crucial bridge between AI systems and human trust. Explainable AI aims to render the decision-making processes of AI systems transparent and understandable to humans, thereby aiding in establishing accountability. If users can grasp how an AI system reached a specific decision, they are more likely to trust its reliability and may be better equipped to identify and rectify errors or biases. (Ryan & Stahl, 2020.)

The current state of trust, accountability, and explainability in AI systems is characterized by a growing awareness of the ethical implications of AI and the formulation of guidelines to address these concerns. However, translating these principles into practical AI applications remains a work in progress, necessitating continued research and policy development to ensure that AI systems are trustworthy, accountable, and explainable.

4 TRENDS GUIDING THE USE OF AI IN THE BATTLESPACE

The evolution of warfare has historically mirrored shifts in technology, society, and global power dynamics. Looking ahead, the future trajectory of conflict will likely be influenced by very similar factors, with the addition of environmental forces due to climate change. This section of the study synthesizes a high-level strategic overview of anticipated developments that are most likely going to have a significant effect on how the use of AI systems in warfare and conflicts develops in the forthcoming decades. The views expressed here stem from strategic forecasts published by authoritative sources such as U.S. Department of Defense (2023), NATO (2021; 2022), U.S. Office of the Director of National Intelligence (*Global Trends*, 2021; *The Future of the Battlefield*, 2021), the European Centre of Excellence for Countering Hybrid Threats (2021), and authors such as O'Hanlon (2018), Schmertzing (2018), Panwar (2017, 2022) and Johnson (2019, 2020b, 2020a, 2021, 2024).

As the horizon extends towards 2040 and beyond, several pivotal trends are projected to mold the essence of conflict and the landscape of the battlespace. Many articles stress the importance of raising awareness to guide responsible development and governance of these technologies amidst complex interactions with geopolitics and security. They emphasize the need for open discussion to navigate these challenges amid rapid technological change. (Blanchard & Taddeo, 2022; Bode et al., 2023, 2024; *Data, Analytics, and Artificial Intelligence Adoption Strategy*, 2023; *NATO 2022 Strategic Concept*, 2022; J. Johnson, 2019, 2022; Megret, 2012; Münkler, 2003; Turunen, 2022.)

4.1 Technological evolution and global dynamics

This chapter explores the strategic reshaping induced by technological advancements in the face of global urbanization. It delves into the ramifications

of metropolitan expansion on warfare dynamics, the pressing influence of climate change on international security, the impact of technology access on military capabilities, and the strategic value of energy, materials, and components in powering AI advancements.

4.1.1 Urbanization and global expansion

The trajectory of global growth and the escalating urbanization trend are poised to reshape societal frameworks, consequently impacting the conduct of conflicts. As the global population becomes more urbanized, there will be a significant impact on military operations. The increase in urbanization may pose challenges for maintaining law and order, and it will be more difficult for militaries, particularly air forces, to discriminate between military and civilian targets. Additionally, the number of megacities, with 10 million or more inhabitants, is expected to expand, leading to further complexities in urban warfare and military strategies. Urbanization, global expansion on military expenditure, city demographics, and the future of megacities may have a strong impact on future conflicts. (Cohen et al., 2020; Global Trends, 2021; Terrorism, 2004; Metz & Cuccia, 2011; Russell et al., 2019.)

4.1.2 Climate dynamics

The repercussions of climate change on essential resources like food supply and natural reserves could potentially serve as triggers for conflict. Changes in climate patterns are expected to exacerbate resource scarcity issues, particularly around water availability. This may increase the likelihood of social, economic and political instability in vulnerable regions. Rising sea levels and more frequent extreme weather events could also lead to large-scale population displacements. (*Global Trends*, 2021; *NATO 2022 Strategic Concept*, 2022; Rajagopalan, 2022.)

The combination of scarcer resources and mass migration raises the potential for more intense and prolonged conflicts. At the same time, climate change may open up previously inaccessible regions for resource extraction or new shipping lanes, intensifying geopolitical competition and tensions in these areas. Furthermore, climate change poses challenges for military operations as infrastructure and bases become more vulnerable to climate hazards. Forces may need to increase their focus on disaster relief and humanitarian assistance missions. The complex effects of climate change are likely to influence many security and conflict drivers in the coming decades. (Cohen et al., 2020; Martin, 2000; Schmertzing, 2018.)

4.1.3 Availability of technology and funding

In the realm of future conflicts, the distribution and availability of technology and funding are expected to play critical roles in determining the pace and direction of AI system development and deployment. As technology proliferates, disparities in access and capabilities may emerge between regions with

concentrated capital and those without. Nations that manage to centralize wealth and resources will likely advance more rapidly in AI technologies, potentially leading to a technology gap. (Calderaro & Blumfelde, 2022; Haefner et al., 2021; Hunter et al., 2024.)

This gap will probably influence not only military strategies but also geopolitical power dynamics. Countries with advanced AI capabilities may enjoy significant advantages in both preemptive and defensive aspects of military engagements. In contrast, nations with less developed AI infrastructures might find themselves at a strategic disadvantage, compelled to adopt different tactics or seek alliances to mitigate these disparities. (Anonymous, 2023; Bitzinger, 2022; Hunter et al., 2024.)

The shift towards open-source models in some regions could democratize access to AI technologies, enabling a broader base of innovation and potentially speeding up the development of general AI capabilities. However, the concentration of capital in certain countries, particularly evident in the declining middle class in the West and its rise in the East, is likely to influence the global distribution of AI advancements. (Anupama, 2023; *Global Trends*, 2021; O'Hanlon, 2018.)

Additionally, the concentration of wealth may lead to decreased levels of education and expertise in areas that once thrived, contributing to a brain drain as talents migrate towards more prosperous regions. This movement is expected to further consolidate the capability gap, as countries with the resources to attract and retain talent accelerate their technological growth and military preparedness. (Calderaro & Blumfelde, 2022; Nadibaidze & Miotto, 2023.)

4.1.4 Availability of energy, materials and components

As the global landscape shifts away from fossil fuels, the availability of energy, materials, and components is set to become a pivotal factor in the development of artificial intelligence systems, particularly within the scope of future conflicts. The transition to nuclear power and renewable energy sources will likely alter the geopolitical playing field. Regions rich in uranium or possessing advanced battery manufacturing capabilities may find themselves with increased leverage in global politics due to their control over essential resources for AI technologies, which are increasingly energy-dependent. (Cohen et al., 2020; *Global Trends*, 2021.)

With much of Europe potentially requiring a decade or more to achieve the capacity to build nuclear power plants, the region may face challenges in maintaining energy self-sufficiency, a factor critical to the sustainable development of AI. This delay will probably create vulnerabilities and dependencies that extend to the battlefield, where energy supply chains are as crucial as traditional logistics. (Dieguez Porras, 2024.)

In areas devoid of natural renewable resources, such as windless or arid regions, there may be an increased risk of energy scarcity. This scarcity could lead to a heightened strategic value being placed on energy-rich locations, making them key objectives or contested zones in military conflicts. Furthermore, the capability to harness "free," renewable energy may become a significant strategic

advantage, potentially influencing the deployment and operational sustainability of AI systems in the field. (Calderaro & Blumfelde, 2022; Hunter et al., 2024; Kumar et al., 2023.)

The technology supply chain is expected to be a point of vulnerability, with information technology self-sufficiency in the West, especially Europe, being at least a decade away. This gap may impact the region's competitive edge in AI development, as the manufacturing processes, raw materials, expertise, and infrastructure required to support advanced AI are currently concentrated outside these areas. Moreover, the reliance on hardware from countries like China, coupled with the software from various corporations, suggests a fragile status quo. This interconnectedness may have profound implications for the resilience of AI systems in the face of conflict, where the durability of the supply chain could be as consequential as the robustness of the AI algorithms themselves. (Hunter, Albert, Henningan, et al., 2023; Schmertzing, 2018; *The Landscape of Hybrid Threats*, 2021.)

In conclusion, the shift in energy resources, combined with the intricacies of the technology supply chain, will likely have a profound impact on the strategic development and deployment of AI systems in future conflicts. Countries that can secure a stable supply of energy and resources, and build resilient supply chains, may gain a substantial advantage in both AI development and their broader military capabilities.

4.2 Sociopolitical and regulatory factors

This chapter sheds light on the heightened capabilities and influence of nonstate entities in the wake of technological democratization, highlighting their utilization of unconventional tactics. The complexities of regional AI regulations and ethical frameworks, along with their influence on military integration, are examined. Additionally, the narrative reflects on how military operations are shaped by public perception and the media, and how societal attitudes towards conflict influence military strategy endorsement.

4.2.1 Non-state actors and grey-zone tactics

The democratization of technology is going to empower a wider spectrum of actors to partake in warfare in a significant way. Non-state actors, including terrorist organizations and insurgent groups, will have access to advanced technologies and capabilities hitherto monopolized by state militaries. Such actors, as well as authoritarian and fragile states, may play a larger role in conflicts after 2030 based on certain trends. (Global Trends, 2021; Metz & Cuccia, 2011; Ruiz Sandoval, 2013.)

States and non-state actors alike are poised to employ asymmetric stratagems and hybrid methodologies, combining conventional and unconventional techniques to exploit vulnerabilities (Rajagopalan, 2022).

Adversarial entities may increasingly resort to such grey zone tactics designed to undermine adversaries without precipitating full-fledged warfare (Panwar, 2017). These methods combine conventional and unconventional approaches, presenting unique challenges (Metz & Cuccia, 2011). Their impacts include for example the following:

1. **Ambiguity and deniability**: Grey zone tactics blur distinctions between war and peace, hindering efforts to attribute actions to specific entities. This ambiguity enables aggressors to disavow involvement, complicating responses from targeted states. (Rajagopalan, 2022; "The Landscape of Hybrid Threats," 2021.)
2. **Economic coercion**: Hybrid warfare often employs economic coercion to achieve strategic goals without direct military engagement. This can destabilize and manipulate economies, jeopardizing the stability and security of targeted nations. (*Global Trends*, 2021; O'Hanlon, 2018.)
3. **Information warfare**: Asymmetric and hybrid warfare heavily utilize information warfare, encompassing disinformation, propaganda, and cyberattacks. These tactics can sway public opinion, sow confusion, and erode trust in institutions, potentially sparking social and political turmoil. (Ayoub & Payne, 2016; Benhamou, 2023; Eilstrup-Sangiovanni, 2018; Hillson, 2009; Ioniță, 2020b; *NATO Warfighting Capstone Concept*, 2021; Williams, 2017.)
4. **Non-kinetic tactics**: Future conflicts may witness a surge in non-kinetic tactics like cyber warfare, psychological operations, and lawfare. These methods can profoundly impact a nation's infrastructure, governance, and social cohesion. (Bakir, 2017; Livieratos, 2022; Russell et al., 2019; Turunen, 2022.)
5. **Escalation risks**: The use of hybrid and asymmetric tactics heightens the risk of unintended escalation. Their ambiguity and unpredictability can lead to misjudgments and misinterpretations, escalating conflicts toward conventional warfare. (Barzashka, 2023; J. Johnson, 2020b, 2021.)
6. **Impact on deterrence**: Grey zone tactics challenge conventional deterrence strategies by operating below the threshold of conventional warfare. This undermines deterrence effectiveness and complicates decision-making for targeted states. (*Data, Analytics, and Artificial Intelligence Adoption Strategy*, 2023; *NATO 2022 Strategic Concept*, 2022; *NATO Warfighting Capstone Concept*, 2021; *The Future of the Battlefield*, 2021; *The Landscape of Hybrid Threats*, 2021)

To further add to the prevalence of different types of non-state actors, climate change impacts could exacerbate issues like water scarcity, food insecurity, economic problems and mass migration in vulnerable regions. This may increase social and political instability, empowering violent extremists to take advantage of grievances and recruit more supporters. States with weak governance, especially in the developing world, may face greater stresses on their authority

due to climate effects. Autocratic regimes may struggle more than democracies to manage instability and adapt to changes in a peaceful manner. (Benhamou, 2023; Cohen et al., 2020; Ioniță, 2020b.)

The growing urbanization of the global population is also noted as benefiting non-state actors, as cities provide opportunities for recruitment, funding criminal activities and carrying out attacks. This kind of developments could reinforce the influence of non-democratic and violent non-government entities, posing challenges for international security if not adequately addressed. (Fox, 2023; Martin, 2000; Metz & Cuccia, 2011.)

4.2.2 Regulation and ethics

The development and deployment of AI systems are likely to be significantly influenced by differing regional ethics and regulatory frameworks. Particularly in Europe, stringent regulations on AI and related technologies are expected to shape the pace and nature of technological advancements. (Panwar, 2022.) If American policymakers decide to adopt similar regulatory measures, it is probable that the United States may experience a slower rate of AI development compared to regions with less restrictive legal environments.

Countries with minimal regulatory barriers could potentially lead in the rapid development and deployment of AI systems for military use. This disparity in regulation may result in a global landscape where AI capabilities are unevenly distributed, possibly giving some nations a strategic advantage in military conflicts. (Rajagopalan, 2022.)

Ethical considerations will play a crucial role in determining the extent and manner in which AI is integrated into national defense strategies. Nations adhering to strict ethical standards for AI use in warfare will likely implement AI systems that emphasize minimizing collateral damage and enhancing decision-making transparency. Conversely, countries with less stringent ethical guidelines may prioritize the operational effectiveness of AI, possibly at the expense of broader humanitarian concerns. (Arandjelović, 2023; Filgueiras, 2022; McFarland & Assaad, 2023; O'Connell, 2023; Trusilo & Danks, 2023; Wareham, 2020.)

As AI technology continues to evolve, international cooperation and dialogue on ethical and regulatory standards will become increasingly important. This may lead to the establishment of global norms and agreements aimed at balancing the benefits of AI in military applications with the need to protect human rights and maintain international peace and security.

4.2.3 Public imagery and accountability

The future of conflicts will be significantly influenced by public imagery and accountability. The widespread dissemination of military operation imagery will enhance deterrence for liberal and democratic states and could diminish the effectiveness of partnerships with the U.S. This shift will empower the public to exert greater influence over governmental and military decisions, emphasizing

the importance of precision-guided munitions, micromunitions, intelligence, surveillance, and reconnaissance (ISR), as well as effective public communication in military endeavors. (Cohen et al., 2020; *The Future of the Battlefield*, 2021.)

Moreover, heightened public concern regarding civilian casualties will also drive change. The increased emphasis on minimizing civilian harm and avoiding collateral damage will likely prompt adjustments in military strategies and tactics to prioritize civilian protection. This concern will amplify deterrence for liberal and democratic states. Other entities, such as totalitarian or non-democratic states, or non-state actors such as terrorist organizations will be less affected, or the effect could very well be the polar opposite. (Clouse, 2023; Münkler, 2003; Petranick, 2015.)

Additionally, the rise of lawfare and the potency of false accusations will shape future conflicts. Lawfare, utilizing legal systems and principles to achieve operational goals, will empower non-state actors and autocracies, potentially deterring liberal-democratic states. Counteracting false accusations and maintaining public support for military actions will demand transparent and credible public affairs efforts. (J. Johnson, 2022; Lin, 2020; Rajagopalan, 2022; Turunen, 2022.)

In essence, the nexus of public imagery and accountability will very likely foster a more transparent and responsible approach to military operations, with a focus on reducing civilian casualties and securing public backing. These dynamics will influence the conduct of future conflicts and dictate the strategies and tactics employed by military forces of liberal and democratic states.

4.2.4 Societal resilience and desensitization

The prospect of live broadcasts of warfare may catalyze pressures to curtail conflicts while concurrently fostering societal desensitization to violence, potentially instigating more radical acts of war or terrorism. As societies grow more resilient to violence, there's a risk of becoming desensitized to the atrocities of war. This desensitization could fuel a disturbing cycle of increasingly sensational terror attacks, as terrorist organizations strive to devise more heinous methods of inflicting harm. Furthermore, this desensitization may obscure the true toll of conflicts, especially in an era where both glorified and trivialized depictions of war abound. (Blank, 2010; Megret, 2012; *Terrorism*, 2004.)

Conversely, societal resilience may also intensify pressure to halt conflicts, as the public becomes more attuned to the horrors of warfare. Yet, the desensitization to violence might also normalize the presence of women in combat roles, prompting questions for states employing military conscription or upholding limitations on women's involvement in combat. (*Global Trends*, 2021; *The Landscape of Hybrid Threats*, 2021; Johnson, 2020.)

The interplay of societal resilience and desensitization can yield intricate and diverse repercussions for future conflicts, influencing public perceptions, the conduct of warfare, and the portrayal and comprehension of conflicts.

4.3 Military strategy and conflict conduct

The focus here is on the dilemmas posed by unmanned and autonomous military technologies, including ethical considerations. The discourse extends to the strategic ramifications of next-generation weaponry and the vital role of space and aerial military assets. The concept of distributed, swarm-based warfare tactics and the strategic landscape's adaptation to contemporary nuclear proliferation are also critically analyzed.

4.3.1 Unmanned, intelligent and autonomous systems

The possible deployment of intelligent mines, guided munitions, and lethal autonomous weapon systems, operating across a spectrum of human oversight levels (human in the loop, human on the loop, human off the loop), raises concrete concerns of ethical and legal quandaries. These kinds of systems have the capacity to make engagement decisions without any human intervention. This issue can't be tackled with global legislation and agreements, because the technology to create such weapons is so simple, that even dedicated individuals can have access to it. (Caldwell & Fidock, 2018; Cohen et al., 2020; Fox, 2023; Hickman, 2020.) Similar capabilities can be integrated to existing platforms, enabling them to operate independently or collaboratively at machine speed and scale.

Recent strides in robotics have facilitated the integration of autonomous functionalities into various weapon systems. Also, the utilization of unmanned aerial, ground, surface and undersea vehicles is anticipated to continue to surge, undertaking a wide number of mundane tasks and perilous missions alike. The adoption of swarming strategies leveraging numerous, adept, and cost-effective unmanned systems could emerge as a defining feature of some future conflicts. (Amirkhanyan, 2022; Ioniță, 2020; Kovács, 2002; O'Hanlon, 2018; Rajagopalan, 2022.)

4.3.2 Directed energy and electromagnetic armaments

The maturation of directed energy weaponry, encompassing high-power microwaves, lasers and railguns, promises novel engagement methodologies capable of neutralizing traditional defenses. Lasers and high-power microwaves in particular have the potential to reform defense if they can be used to effectively counter fast-moving hypersonic weapons with the ability of long-range precision strikes. They could offer a virtually unlimited rate of fire at the speed of light with nearly zero cost per shot once the challenges of energy consumption and replenishment are overcome. However, lasers are limited by line-of-sight and can be degraded by things like atmospheric conditions, reflective surfaces, or specialized materials. High-power microwaves could also be defeated by hardening key components of potential targets. (Cohen et al., 2020; O'Hanlon, 2018; Schmertzing, 2018.)

4.3.3 Space and high-altitude platforms

The domain of space has become a contested arena with the advent of counterspace capabilities. The strategic deployment of space-based assets and high-altitude platforms will be pivotal for surveillance, communication, and weapon deployment, underscoring the strategic significance of space dominance and escalating importance of space in military stratagem. (Rajagopalan, 2022.) The integration of space technologies into conventional forces will also continue. Weapons like directed energy weapons and hypersonic missiles may be launched from reusable space planes or high-altitude platforms operating in and out of Earth's atmosphere. This allows striking targets globally with little warning. It could undermine mutual assured destruction by holding large areas of territory at risk. (Panwar, 2022; Russell et al., 2019; *The Future of the Battlefield*, 2021.)

The establishment of dual-use commercial satellite constellations in low Earth orbit presents challenges for distinguishing military from civilian assets. Attacks on these systems risk damaging critical services and escalating tensions. Persistent overhead surveillance from such platforms may also erode crisis stability by providing near-real-time intelligence. (Kovács, 2002; Rajagopalan, 2022; Schmertzing, 2018.)

Increasing the militarization and weaponization of space may also complicate security dynamics in the coming decades. Many countries are developing counter-space capabilities meant to disrupt satellite-based communications, navigation, and intelligence, surveillance, and reconnaissance. Anti-satellite missiles, cyberattacks, and other means could threaten critical space infrastructure during a crisis or conflict. The expansion of military activities in space and from high-altitude systems risks destabilizing conventional deterrence frameworks and norms of behavior. It may compel states to develop hard-to-detect countermeasures like jamming or cyber weapons in self-defense, further escalating tensions. Careful confidence-building measures will be needed to manage these emerging threats to strategic stability. (Panwar, 2017; *The Landscape of Hybrid Threats*, 2021; Turunen, 2022.)

4.3.4 Swarming and distributed warfare

Emerging technologies might facilitate novel forms of swarming and distributed warfare, characterized by coordinated yet decentralized actions across various platforms communicating with each other. This encompasses scenarios where swarms of affordable autonomous drones, missiles, and smart munitions collaborate to overwhelm targets through synchronized assaults from multiple directions simultaneously. (Ayoub & Payne, 2016; J. Johnson, 2020a.)

Such swarming tactics challenge conventional military doctrines, which typically rely on concentrated, centralized forces. They also open avenues for asymmetric warfare strategies utilizing smaller, more economical systems. However, these distributed swarm attacks could complicate escalation dynamics during crises, as identifying individual attackers and conveying intentions

clearly becomes challenging. The rapidity and synchronization of swarm offensives could provoke hurried responses from defenders, while operations spanning vast areas may obscure the true extent of threats. (Ayoub & Payne, 2016; J. Johnson, 2020a; O'Hanlon, 2018; Schmertzing, 2018.)

Establishing regulations to differentiate legitimate from illegitimate uses of swarming tactics might prove problematic for international laws and norms. Of particular concern are applications involving lethal autonomous weapons operating in swarms without direct human supervision, raising questions about maintaining control over the use of force. Swarming and distributed warfare have the potential to reshape military strategies significantly, albeit accompanied by fresh hurdles for crisis management and conflict resolution. (Ayoub & Payne, 2016; Bode et al., 2023; J. Johnson, 2020a, 2022.)

4.3.5 Nuclear proliferation and deterrence

The potential resurgence of nuclear proliferation, building ballistic missile capabilities and the erosion of norms governing tactical nuclear weapons' usage could profoundly alter strategic stability and security dynamics. It is also an existing concern that the control of nuclear weapons is given to AI systems (Torode, 2024). States, perceiving threats, may feel compelled to match the arsenals of their rivals, sparking arms races akin to those seen during the Cold War. (J. Johnson, 2021; Kanniainen, 2023; Rajagopalan, 2022.)

Various factors, such as the breakdown of major arms control treaties, technological advancements, or perceived vulnerabilities from adversaries wielding advanced non-nuclear strategic weapons, could fuel renewed proliferation. Regional crises involving nuclear-armed actors might heighten risks, introducing uncertainties regarding red lines. (Cohen et al., 2020; J. Johnson, 2019, 2021; Kanniainen, 2023; Rajagopalan, 2022.)

The integration of nuclear weapons into ongoing territorial or ideological disputes could lower the threshold for their symbolic or coercive use during crises, potentially escalating tensions and increasing the likelihood of accidental or miscalculated escalation. As nuclear technologies spread globally, containing proliferated nuclear networks becomes increasingly challenging. Unbridled nuclear proliferation threatens to unsettle existing deterrence frameworks, ushering in a more multipolar nuclear landscape with heightened risks of miscalculation between closely matched nuclear adversaries. (Blanchard & Taddeo, 2022; Bode et al., 2023; J. Johnson, 2021; Kanniainen, 2023; Rajagopalan, 2022.)

4.4 Advanced technologies and their implications

This chapter explores the transformative potential of nanotechnology and advanced materials in military applications. The revolutionary impacts of

quantum computing on information security and military operational capacity are probed, alongside the acceleration of data analysis and decision-making through AI. Lastly, the escalating significance of cyber and electronic warfare in contemporary military strategy formulation is emphasized.

4.4.1 Nanotechnology and other advanced materials

The frontiers of nanotechnology other new materials and advanced manufacturing techniques are poised to unlock innovative avenues for enhancing soldier performance and developing novel tailored systems for military exigencies. Together with advanced materials, smart manufacturing systems combine physical and simulated worlds, allowing the integration of Cyber-Physical Systems (CPS) in manufacturing. Several potential applications include smart design, smart machining, smart monitoring, smart control, smart scheduling, and industrial execution. (J. Johnson, 2020b; Singh et al., 2023.)

New materials at the nanoscale have the potential to significantly enhance military capabilities in the coming decades. Nanomaterials could improve properties like the strength of armor and explosives, as well as energy storage capacity. Metamaterials and nanocoatings may facilitate stealthier aircraft and vessels. Such advances could offer a decisive advantage to those who develop and apply these technologies first. However, these dual-use technologies could lower barriers to disruptive weapons if misapplied without oversight. (Ioniță, 2020a, 2020b; J. Johnson, 2020b) Likewise, self-assembling systems at the nanoscale applied to weapons instead of infrastructure could have uncontrolled consequences (O'Hanlon, 2018).

Graphene nanoparticles offer a wide range of potential applications across various industries, including electronics, energy storage systems, hydrogen storage systems, supercapacitors, biomedical and nanomedicine, defense and tactics, desalination, and sports equipment. Specifically in defense and tactics, graphene nanoparticles are highly durable, flame-resistant, and possess excellent electromagnetic shielding capabilities, making them ideal for military equipment and armor. Their lightweight nature and high thermal conductivity also make them useful in constructing thermal management systems for weapons and protection systems. Graphene's superior radiation shielding ability, along with its excellent electrical and thermal conductivity properties, provides enhanced radiation protection for personnel. (Yusaf et al., 2022.)

Ceramic matrix composites (CMCs) are emerging as excellent lightweight composites for aerospace applications, effectively reducing structural density to achieve lightweight development. Siemens has manufactured turbine blades using 3D printing and polycrystalline nickel superalloy powder for an SGT-400 industrial gas turbine. The 3D printing technology allows parts to be optimized for thermal, aerodynamic, strength, vibration, lightweight, and other multifaceted objectives. Researchers are exploring the use of truss-lattice structures, including a new sandwich plate structure with the addition of a multifunctional pyramid lattice, to provide high performance while considering

the heat transfer and mechanical properties of the lattice structure. (L. Xu et al., 2023.)

4.4.2 Quantum computing and advances in data processing and transfer

The advent of quantum computing and universal AI holds the potential to revolutionize warfare, potentially avoiding traditional missile systems and reshaping the contours of deterrence. At the moment, AI aids in information analysis and decision-making processes. Information and knowledge have a profound significance as formidable assets in both civilian and military realms, resonating across decision-making, intelligence and deception realms. (O'Hanlon, 2018; Rajagopalan, 2022; Schmertzing, 2018.)

Within the next decade or so, quantum computing may break current encryption standards, although efforts to develop quantum-resistant encryption are underway. Quantum sensors offer improved situational awareness in the near term, but full-scale quantum computers for direct military use are still a decade away due to technological hurdles. The sources discuss possibilities like quantum-enhanced drones, which combine quantum technologies with classical AI to potentially provide disproportionate advantages. (J. Johnson, 2021; Kovács, 2002.)

Significant uncertainties exist regarding technology development trajectories and the implications of applications like mass surveillance and perceived first-strike capabilities, which could undermine strategic stability. (Kosola & Solante, 2013; Livieratos, 2022; Martin, 2000; *What Is War Today?*, n.d..)

4.4.3 Machine speed data analysis and decision-making

AI is poised to assume a pivotal role in analysis of massive data streams from networked sensors across different military domains, underpinning decision-making processes. Such systems could give commanders near-real-time situational awareness of the battlefield. This comprehensive picture may allow for more precise targeting of critical assets and optimization of military maneuvers. (J. Johnson, 2022; Otto & Mănescu, 2023.)

However, there are also several risks. The speed of AI-guided decision-making and actions could significantly shorten response timelines during crises or escalating tensions. This may limit the options for controlled de-escalation because there would be less time for deliberation and coordination of moves between opposing sides. Another risk is the potential for unintended or uncontrolled escalation if AI systems are not properly integrated with and regulated by human judgment, especially regarding autonomous use of lethal force without appropriate human oversight or ability to override decisions. (Clouse, 2023; J. Johnson, 2020b, 2021; Megret, 2012.)

While AI-driven data analysis could provide strategic and tactical advantages through improved coordination and planning, the perception of technological advantages or vulnerabilities enabled by AI could also potentially fuel arms races as countries try to counter perceived disadvantages through new

defensive investments. There are also concerns that AI may compress timelines in a way that increases pressures for immediate action during crises, risking inadvertent further escalation. (Bode et al., 2023; J. Johnson, 2021; Otto & Mănescu, 2023; Rajagopalan, 2022.)

4.4.4 Cyber and electronic warfare

Cyberspace electromagnetic activities (CEMA) (*FM 3-12 Cyberspace Operations and Electromagnetic Warfare*, 2021) are increasingly integrated with conventional military strategies, indicating a trend towards their mainstream adoption in all the militaries around the world. Nations are investing in cyber weapons to gain strategic advantages. Heightened occurrences of cyber espionage and sabotage are also anticipated, affecting both state and non-state actors alike. (Russell et al., 2019; Turunen, 2022.)

The escalating reliance on digital infrastructures amplifies the significance of cyber capabilities and electronic warfare as indispensable tools of military strategists, especially when cyberattacks are not bound by geography. As reliance on networked systems and digital technologies grows, so do vulnerabilities that adversaries could exploit through cyber and electronic attacks, potentially targeting critical infrastructure such as power grids and financial networks. This interconnectedness complicates deterrence strategies and raises the risk of unintended escalation, as disruptions to communication networks or misinformation campaigns could exacerbate crises. (Clouse, 2023; Eilstrup-Sangiovanni, 2018; *Terrorism*, 2004; Williams, 2017.)

Future conflicts are envisioned as "multidomain battles" spanning physical and virtual realms, presenting challenges in coordinating diverse cyber, electronic, kinetic, and non-kinetic options for military planners. Regulating these domains poses challenges for international law and agreements, as norms are still evolving around issues such as defining legitimate targets and constraining disruptive or destabilizing activities in cyberspace and outer space. As offensive capabilities in different domains continue integrating with conventional forces, this could complicate nuclear deterrence calculations and escalation dynamics. (Ayoub & Payne, 2016; Clouse, 2023; J. Johnson, 2020b; Panwar, 2017.)

5 FUTURE APPLICATIONS OF AI

The critical review of the research material produced 27 separate categories, applications or use cases for AI in future conflicts and battlespace. This section of the study describes them on a strategic level, giving an overview of the effects they will likely have, and the ways they can be used in to create concrete capabilities. The categories are listed below in TABLE 6 Categorized AI applications, along with the number of times each category was mentioned in the material.

It is worth noting that many described use cases could be categorized under several different headings, for example a threat detection system for cyber security could be categorized either as cyber and electronic warfare or as threat detection and assessment. The categorization was made for the closest fit considering the context of the reference in the original document. Therefore, the exact count of mentioned in the column Number of references should be used only as a guiding order of magnitude for the relative likelihood of each usage, instead of an exact weight.

TABLE 6 Categorized AI applications

Application	**Number of references**
Cyber and electronic warfare	316
Threat detection and assessment	262
Data mining and processing	192
Decision-making support and automation	160
Autonomous vehicles and robotics	149
Analysis, predictions and situational awareness	145
Technology development	125
Autonomous weapons systems	103
Information collection	96
Biometric recognition and analysis	80
Communication systems	75
Medical diagnostics and treatment	73
Image and video analysis	72

Target identification, tracking and analysis	69
Simulation, testing and training	68
Autonomous protection systems	64
Human-machine collaboration	64
Information warfare, denial and deception	62
Logistics and supply chain management	45
Strategic deterrence	38
Predictive maintenance	29
Human performance enhancement	28
Behavioral analysis	24
Environmental monitoring	21
Societal manipulation and destabilization	21
Precision strike weapons	18
Dynamic resource allocation	17
Total	**2416**

The categories were then grouped and regrouped several times in different combinations utilizing critical analysis to obtain a logical and representative grouping for creating a higher-level overview. This phase concluded to these five groups:

1. Enriched intelligence, decision-making, and predictive capabilities
2. Operational efficiency and supply chain optimization
3. Improved autonomous systems and robotics
4. Augmented cyber and information warfare capabilities
5. Advanced human-machine interaction and performance enhancement

The groups and categories are described in the following sections. In order to provide a high-level overview of the applications that are possible, this section intentionally leaves the ethical questions regarding each potential use untouched. It is important for high-level defense and security planners to know what kind of capabilities potential adversaries might field, especially when the capabilities may be something that is deemed unethical in one's own service.

5.1 Enriched intelligence, decision-making, and predictive capabilities

AI can vastly improve intelligence gathering, automate decision-making, and enhance predictive analytics. By processing large volumes of data from various sources, AI provides real-time situational awareness and enables faster and more accurate decision-making. Its predictive capabilities allow for anticipatory measures in conflict, foreseeing enemy strategies and movements, which significantly aids in strategic planning and threat management.

5.1.1 Environmental monitoring

In future conflicts, AI will play a critical role in environmental monitoring and emergency management. Utilizing contextual data such as weather conditions, air quality, and geographic information, AI will classify human activities and predict trends using sources like social media, which can also aid in risk communication for public health emergencies (A. Jones et al., 2023; Shen et al., 2022).

AI's capabilities extend to disaster response, where it will detect, predict, and manage natural disasters, allocate resources effectively, and assess damage and population health impacts. This includes predicting earthquakes and hurricanes, assessing traffic conditions, and managing emergency responses to urban flooding and disease outbreaks. (Ortega & Araneda, 2024; Sarvajcz et al., 2024.)

Furthermore, AI will be employed for horizon scanning to anticipate unforeseen 'Black Swan' events and for environmental protection analysis. This involves evaluating how resources are utilized, predicting environmental challenges, and forecasting factors that could influence military operations or emergency responses. (Négyesi, 2024; Popa, 2022.)

5.1.2 Decision-making support and automation

AI systems will significantly enhance decision-making in military operations by automating and supporting command and control processes. These systems enable both supervised and unsupervised decision-making, streamlining battlefield management and strategic operations. They will increase operational efficiency, facilitate rapid and precise targeting, and alleviate cognitive burdens under pressure. (Davis, 2022; Shobar & Tawil, 2023.)

Additionally, AI will be crucial in cybersecurity and defense operations, autonomously identifying and neutralizing threats to improve response times and operational security (Bukkapatnam, 2023; Hagendorff & Fabi, 2023). These intelligent systems will also support critical infrastructure and manage autonomous weaponry, operating in complex scenarios without direct human oversight (Naz et al., 2023; Oh et al., 2024).

AI will further streamline administrative and logistical functions within military contexts, enhancing non-combat operations efficiency (Oniani et al., 2023b; Popa, 2022; Rao et al., 2022). It will also provide advanced situational awareness and predictive analytics, aiding military personnel in anticipating enemy strategies effectively (Boutin, 2023; Jenkins et al., 2023).

Technological advances in AI, particularly in machine learning and big data analytics, will influence military decision-making in significant ways. These technologies offer predictive modeling that improves strategic and tactical decisions and develops real-time wargaming tools for evaluating tactical options (Kassens-Noor et al., 2022; Meerveld et al., 2023).

5.1.3 Analysis, predictions and situational awareness

AI systems are likely to significantly enhance intelligence analysis, predictions, and situational awareness. These systems will be central to intelligence analysis, processing and interpreting vast datasets from diverse sources such as satellite imagery, social media, and sensor data. Utilizing deep learning and natural language processing, AI will identify complex patterns and trends, accelerating decision-making and reducing workload for analysts. This will allow the human operator to focus on higher level tasks instead of menial labor. (Mayer, 2023; Narayanan et al., 2024.)

Predictive analytics will also see substantial improvements, with AI analyzing both historical and real-time data to forecast enemy tactics and movements, aiding strategic decisions in dynamic geopolitical scenarios (Bavle et al., 2023; Singh et al., 2022).

Enhanced situational awareness through AI will integrate data from unmanned vehicles and IoT sensors, providing commanders with a comprehensive operational picture essential for quick and informed decision-making (Markatos & Mousavi, 2023; Salor & Baeza, 2023).

In addition, AI will support autonomous operations and cyber defense, managing tasks from surveillance to direct engagement with minimal human oversight. AI-driven systems will respond to threats more rapidly than traditional methods, increasing the security of critical infrastructures. (Dmytryshyn & Romanchukevych, 2022; Schraagen, 2023.)

As AI technologies advance, their integration into military systems will likely expand, enhancing defense capabilities and operational efficiency, and profoundly influencing military strategy and preparedness for future conflicts.

5.1.4 Data mining and processing

AI systems significantly enhance data mining and processing capabilities, offering substantial performance advantages over traditional methods. As powerful automation tools, they handle complex calculations and large data volumes effectively, bolstering threat detection and management (Pai et al., 2022; Xia, 2022). The integration of blockchain technology with AI is particularly promising for securely managing data through various stages of processing (Basrur & Wu, 2023; Shahzad et al., 2022).

The ability to semantically analyze both structured and unstructured data is crucial, aiding in multi-source data integration and providing essential insights for decision-making (Chedrawi & Atallah, 2022; Davy Preuveneers & Joosen, 2024). With advanced computing power and improved data links, AI facilitates real-time situational awareness and adding more and more relevant data sources (Keerthinathan et al., 2023; Žigulić et al., 2024).

The use of AI in processing vast amounts of data is transforming battlefield operations, increasing response speed and operational efficiency (Trusilo, 2023). These systems are becoming essential in applications ranging from threat

detection to target identification, underpinning broader military and security strategies.

5.1.5 Information collection

AI systems are set to transform information gathering in future conflicts through a range of technologies including autonomous vehicles and advanced sensor networks. Autonomous platforms such as UAVs, UGVs, USVs, and UUVs (unmanned aerial vehicles, unmanned ground vehicles, uncrewed surface vessels and unmanned underwater vehicles) will serve as key tools for intelligence, surveillance, and reconnaissance, engaging in combat operations and search and rescue missions in hazardous or remote areas. These vehicles will utilize multispectral and thermal sensors to collect real-time data. (Horvat et al., 2024; Shobar & Tawil, 2023.)

Beyond unmanned vehicles, AI will leverage enhanced signal detection and intelligent monitoring systems capable of long-distance surveillance, incorporating cutting-edge sensors that are lighter, more compact, and more power-efficient (Devarakonda et al., 2022; Jiao et al., 2023). AI will also facilitate the integration of data from digital and radio frequency networks for both legal and covert operations, providing comprehensive intelligence on various entities (Sangwan et al., 2023).

Additionally, AI will boost surveillance capabilities in public and sensitive areas, aid in border and customs control, and support military operations by identifying threats such as weapon caches and enemy combatants. AI-driven algorithms will analyze extensive sensor data to pinpoint critical threats effectively. (Cartwright et al., 2022; Kiener, 2022; Riesen, 2022.) This strategic deployment of AI across multiple domains underscores its pivotal role in enhancing operational security and intelligence in future military engagements.

5.1.6 Image and video analysis

AI systems will play a crucial role in image and video analysis across various military and security applications in future conflicts. These systems will be extensively used for damage assessment on large warships, surveillance with commercial satellite imagery, and facial recognition, enhancing capabilities in warfare and conflict resolution (Caverley, 2023; Duan et al., 2022; Jekateryńczuk & Piotrowski, 2024).

Further applications include automatic object classification in autonomous vehicles, detecting hostile entities, and recognizing behavioral patterns through video surveillance. AI will also be instrumental in identifying mines and Improvised Explosive Devices (IEDs) and in automatic weapon recognition, choke-point detection, and traffic analysis. (Anupama, 2023; Saifi et al., 2023.)

Additionally, AI-enhanced vision systems integrated with surveillance cameras and drones will support border surveillance and security. These systems will also analyze medical images, such as ultrasound scans, to identify critical health-related markers. (Arulprakash et al., 2022; Rehaan et al., 2024.)

AI technologies will combat disinformation by detecting deepfake videos and enhance public safety through improved video surveillance systems designed to detect and prevent crimes in public areas (Mai et al., 2023; Okolie, 2023). AI-driven intrusion detection will further secure sensitive areas by identifying unauthorized access, ensuring comprehensive security coverage across multiple domains (Li et al., 2022; Taheri & Asadizanjani, 2022).

5.1.7 Target identification, tracking and analysis

AI systems will crucially enhance target identification, tracking, and analysis across military operations, integrating with platforms like unmanned vehicles and surveillance networks to offer real-time, precise target information. These systems will autonomously analyze data from multiple sensors, distinguishing between allies and adversaries, and prioritizing threats to optimize resource deployment and minimize human exposure in combat. (Aqeel et al., 2023; Figueroa et al., 2023; Mügge, 2023.)

Furthermore, AI will refine weapon system integration, advising on weapon selection and strike tactics based on target characteristics and environmental factors, thereby increasing strike accuracy and reducing collateral damage (Bode et al., 2024; G. Wang et al., 2023). AI will also ensure that military actions comply with international laws by vetting targets against restricted lists, enhancing both the legality and ethics of operations (Figueroa et al., 2023; Trusilo & Danks, 2023).

AI's capabilities extend to post-strike analysis, where it assesses damage and informs adjustments for future missions, and to reconnaissance, improving the detection of subtle or hidden threats through advanced pattern recognition (Duan et al., 2022; Nadibaidze & Miotto, 2023).

Overall, the deployment of AI in military targeting and analysis will significantly boost operational security, efficiency, and effectiveness, positioning AI as a transformative force in future military strategies.

5.1.8 Threat detection and assessment

AI technologies will be integral to enhancing security systems, using advanced machine learning algorithms to process vast data volumes from various sources, identifying patterns that indicate potential threats (Garg & Jayanthiladevi, 2023; Hagendorff & Fabi, 2023). In cybersecurity, AI will monitor network traffic and detect early signs of cyberattacks, allowing for preemptive measures that safeguard critical infrastructures (Ganguli et al., 2023; Hagos & Rawat, 2022; Mohamed, 2023).

Additionally, AI will bolster public safety and law enforcement by utilizing predictive analytics to assess crime data and trends, optimizing resource allocation and potentially reducing crime rates (Kiener, 2022; Narayanan et al., 2024; Teo, 2022). In counterterrorism, AI will sift through communication and transaction data to identify and disrupt terrorist networks, enhancing national and global security (Katagiri, 2024; Schmid et al., 2022; S. Xu et al., 2022).

AI will also improve military situational awareness by analyzing satellite imagery and drone reconnaissance, providing real-time battlefield intelligence (Hagos & Rawat, 2022; Riesen, 2022). In emergency management, AI will predict and manage responses to natural disasters, reducing impact and aiding recovery efforts (Y. Lee & Kim, 2023; S. Xu et al., 2022).

Overall, AI's role in threat detection and assessment is evolving towards greater autonomy, learning from past incidents to better predict and mitigate future risks (Cancela & Goikoetxea, 2023; Riesen, 2022). This ongoing advancement will keep AI as a crucial component in addressing the complexities of global security.

5.2 Operational efficiency and supply chain optimization

AI enhances the speed and efficiency of military operations and logistics. It automates resource allocation, planning, and execution, enabling rapid adaptation to changing conditions. Additionally, AI-driven systems optimize supply chains by forecasting needs and managing resources efficiently, which is essential for maintaining the continuity and effectiveness of military operations.

5.2.1 Logistics and supply chain management

AI systems are set to transform logistics and supply chain management in military operations by optimizing the logistics lifecycle from resource allocation to delivery. By leveraging machine learning and predictive analytics, AI can forecast supply needs and anticipate disruptions, enabling proactive supply chain adjustments (Adib Bin Rashid et al., 2023; Ambadekar et al., 2023).

AI will significantly enhance autonomous transportation, with AI-powered vehicles autonomously navigating through conflict zones, optimizing routes in real-time, and ensuring efficient delivery of resources (Fang & Li, 2022; Otto & Mănescu, 2023).

Furthermore, the integration of AI with Internet of Things (IoT) technologies will improve logistics management. Real-time IoT data will optimize energy usage, route planning, and inventory management, particularly in managing electric vehicle fleets (Ambadekar et al., 2023; Venkatesh Kumar et al., 2024).

In cybersecurity, AI will play a vital role in protecting increasingly digital supply chains from cyber threats and fraud, using smart contracts to secure transactions and manage data integrity (Devarakonda et al., 2022; Shahzad et al., 2022). This comprehensive use of AI will significantly enhance the efficiency, security, and sustainability of military logistics operations.

5.2.2 Predictive maintenance

AI systems have strong potential to accurately forecast maintenance needs of materiel. Utilizing data from sensors in equipment such as ground vehicles and aircraft, AI algorithms may predict component failures, allowing preemptive maintenance that minimizes downtime and enhances operational readiness (Singh et al., 2023; Venketeswaran et al., 2022).

The use of deep learning and advanced modeling will improve fault detection and diagnosis, enabling the systems to adapt to changing conditions and identify faults with high precision. This advancement will likely lead to reduced maintenance costs and increased equipment uptime, boosting military efficiency (Kim & Joo, 2022; Yang et al., 2023).

In spaceborne applications, AI will be crucial for the predictive maintenance and monitoring of spacecraft, enhancing their longevity and operational effectiveness without direct human intervention (Jiao et al., 2023).

Additionally, predictive maintenance will optimize inventory management by accurately forecasting the need for specific parts and supplies, ensuring inventories are optimally stocked and critical components are readily available, thus supporting sustained military readiness (X. Jiang et al., 2023; Kim & Joo, 2022).

As military reliance on sophisticated technology grows, AI's capability to predict and prevent equipment malfunctions will be critical in optimizing response times and maintaining high operational effectiveness in various conditions (Guy et al., 2024).

5.2.3 Dynamic resource allocation

AI systems are poised to significantly enhance dynamic resource allocation, improving the efficiency and effectiveness of military and emergency response operations. Utilizing advanced computational modeling and optimization techniques, these systems will dynamically allocate resources based on real-time demands and emerging threats, integrating big data analytics for precise and timely deployment (Kaushik & Sarath, 2022; Schleiger et al., 2024).

AI-driven resource management will automate the dispatch of resources in complex scenarios such as mass casualty events or natural disasters, analyzing severity, asset status, and location-specific needs to autonomously make critical dispatch decisions. This will be crucial for rapid responses that save lives and mitigate disaster impacts (Hunter et al., 2024; Munir et al., 2022).

Additionally, AI will employ reinforcement learning to adapt and improve resource allocation strategies continuously, enhancing the response capabilities of military and emergency units under unpredictable conditions (Khan et al., 2022; Kim & Joo, 2022).

In disaster response, AI will advance predictive modeling to forecast impacts and allow proactive resource allocation and risk mitigation. These systems will monitor and analyze ongoing situations to adjust resource deployment in real-time, optimizing response efforts. (Hunter et al., 2024.)

5.2.4 Communication systems

AI systems are likely to improve communication systems, boosting both efficiency and security to meet the demands of modern warfare and crisis management. AI technologies will be essential in developing advanced communication networks with robust encryption and real-time anomaly detection to protect against cyber threats, ensuring the confidentiality and integrity of military communications (Alyousef et al., 2022; Y. Han et al., 2022).

AI will enhance network efficiency by optimizing bandwidth allocation and reducing communication delays and errors. This improvement will support better management of network loads during critical operations and ensure reliable communication in disrupted environments. (Gompert & Libicki, 2023; Hunter, Albert, Henningan, et al., 2023.)

Autonomous AI systems will maintain communication links in crisis scenarios, crucial for command and control across diverse military domains (Ruppert, 2024; Zubair et al., 2022). Additionally, AI will facilitate data privacy through federated learning, allowing devices within communication networks to learn and adapt collectively without centralizing sensitive data (Hussain et al., 2022; Rivera et al., 2022).

AI will also provide real-time translation services to overcome language barriers in multinational operations, improving collaboration and coordination among allied forces (Jekateryńczuk & Piotrowski, 2024; Stinchfield, 2023).

In cryptography, AI-driven tools may enhance encryption methods and perform advanced cryptanalysis to secure sensitive information and improve systems like navigation that rely on secure data transmission (Malallah & Wattar, 2023; X.-X. Li et al., 2022).

5.2.5 Technology development

AI technologies will be pivotal in advancing research and development across various sectors, significantly enhancing innovation and process optimization. In defense, AI will improve autonomous systems, enhancing reconnaissance, surveillance, and kinetic attacks, and will integrate advanced simulation technologies for training and operational planning (Bode et al., 2024; J. Johnson, 2022a; Schleiger et al., 2024).

In civilian sectors such as manufacturing, agriculture, and healthcare, AI will drive substantial advancements. It will enable predictive maintenance to optimize manufacturing processes, use data analytics in agriculture to boost crop yields and efficiency, and advance diagnostic and treatment options in healthcare, including biotechnological innovations like 3D bioprinting and personalized medicine (Ali et al., 2023; H. R. Han, 2023; Tyczewska et al., 2023).

AI will also improve material science by developing smarter materials like graphene, enhancing applications in electronics, energy storage, and nanomedicine (Bukkapatnam, 2023; Yusaf et al., 2022). In cybersecurity, AI will enhance threat detection and response, crucial for protecting both military and civilian data (J. Johnson, 2022a).

Additionally, AI will streamline the integration and management of emerging technologies within complex systems, coordinating operations in both military and civilian contexts to foster more sophisticated, interconnected systems that operate autonomously and efficiently (H. R. Han, 2023; Rim, 2023).

Overall, AI is set to be a cornerstone in technological evolution, enabling smarter, more efficient, and effective solutions across all domains, boosting human creativity and operational capabilities.

5.3 Improved uutonomous systems and robotics

AI enhances the capabilities of autonomous weapons, vehicles, and robotics. These systems can perform surveillance, reconnaissance, combat roles, and logistics support with minimal human intervention, potentially reducing casualties and enhancing mission effectiveness. The inclusion of autonomous vehicles ensures efficient navigation and operational capabilities in diverse environments, ranging from aerial drones to unmanned ground and maritime vehicles.

5.3.1 Autonomous weapons systems

Lethal Autonomous Weapons Systems are poised to dramatically reshape future conflicts, operating with varying levels of human oversight and leveraging artificial intelligence for tasks from surveillance to lethal engagements. LAWS are expected to improve target identification, analysis, and tracking, and will be used in both offensive and defensive military operations, marking a significant evolution in combat strategy (Horowitz et al., 2022; Jameel & Saud, 2022; Teo, 2022).

The integration of LAWS is likely to increase the use of autonomous drones and robots in combat, potentially replacing conventional weapons and vehicles, thus shifting the majority of combat functions to autonomous agents. This shift raises substantial ethical, legal, and practical challenges, particularly regarding the delegation of lethal decisions to machines, the potential for malfunctions, and the ethical implications of autonomous decision-making (Pacholska, 2023; Umbrello, 2022).

On the international stage, there will likely be challenges in forming a consensus on regulations governing the development and use of LAWS. Nations may need to implement stringent controls to ensure responsible deployment, yet achieving global agreement might be difficult. As LAWS evolve, new frameworks for accountability will be essential to address the complexities introduced by these highly capable systems (Jameel & Saud, 2022; McFarland & Assaad, 2023).

Strategically, LAWS will enable nations to conduct military operations with greater precision and reduced human risk. These systems could operate in environments where communications are limited, using predictive algorithms to

function autonomously or in sync with human operators, thereby enhancing military intelligence capabilities and impacting global security dynamics (Riesen, 2022). This technological progression will influence how states manage access to these powerful capabilities.

5.3.2 Autonomous protection systems

Autonomous protection systems equipped with AI are have a strong potential to improve security across various domains by incorporating advanced cybersecurity mechanisms using deep reinforcement learning. These systems will adaptively learn from experience, enhancing their capability to manage dynamic and complex cyber threats efficiently (Oh et al., 2024; G. Wang et al., 2023).

These autonomous systems are expected to automate incident response, reducing human operator workload and increasing the precision and speed of threat identification and responses. This automation will accelerate the Observe-Orient-Decide-Act (OODA) loop, crucial for quick decision-making in military operations (Bavle et al., 2023; A. Brown, 2023).

Furthermore, AI-driven systems will also defend against physical threats, employing AI-augmented target recognition to enhance missile defenses and intelligence analysis accuracy. This integration will improve surveillance, reconnaissance, and logistical support, boosting overall defense operation effectiveness (Subramanian et al., 2023; Yin-Chun et al., 2022).

AI will also be applied to create defensive deception frameworks against reconnaissance attacks, using deep reinforcement learning to generate real-time countermeasures, thereby disrupting adversary intelligence efforts (Kaushik & Sarath, 2022).

In the civilian sector, AI-enhanced autonomous systems will provide robust defense against various adversarial attacks, from cyber threats to unmanned assaults, and will be crucial in high-security areas like minefield neutralization and critical infrastructure protection (Bai et al., 2023; Botezatu, 2023).

Overall, the deployment of AI in autonomous protection systems promises transformative improvements in how security is managed in both military and civilian contexts, offering scalable, efficient, and adaptable solutions to emerging threats.

5.3.3 Autonomous vehicles and robotics

Autonomous vehicles and robotic systems are set to transform operations across aerial, ground, and maritime environments, enhancing efficiency and safety in both military and civilian contexts. These systems, including UAVs, UGVs and UMVs (or USVs and UUVs), will undertake roles from surveillance and reconnaissance to logistics and active combat, utilizing AI for navigation, real-time route optimization, and tactical decision-making (Ortega & Araneda, 2024; Salor & Baeza, 2023).

Robotics equipped with capabilities like natural language processing and computer vision will handle tasks too risky or complex for humans, such as bomb disposal and search and rescue missions, significantly reducing human labor while increasing precision (Boutin, 2023; Rao et al., 2022). These technologies are also expected to impact agriculture, disaster response, and manufacturing sectors profoundly.

AI-driven control systems will coordinate large swarms of autonomous units, crucial in combat for synchronized attacks and defenses, transforming battlefield dynamics with operations that are swift and less predictable to adversaries (Bae & Hong, 2023; Chedrawi & Atallah, 2022; Ganguli et al., 2023). These systems will also manage civilian and military vehicle operations, enhancing traffic management, border security, and tactical deployments (Khader, 2022; Pavlidis, 2024).

In defense, AI will enable unmanned combat systems to conduct strategic operations with greater autonomy, such as managing unmanned combat aerial vehicles (UCAVs) for precision strikes or autonomous tanks in ground operations, potentially including LAWS for enhanced mission outcomes and reduced human risk (Venketeswaran et al., 2022).

Overall, the integration of AI in autonomous vehicles and robotics indicates a significant shift towards more automated and intelligent systems, reshaping the landscape of conflict and everyday operations, and creating new tactical opportunities in various sectors.

5.3.4 Precision strike weapons

The integration of AI into precision strike weapons is set to significantly boost military capabilities by enhancing the accuracy and efficiency of targeting systems. AI will enable rapid identification and engagement of valid military targets, reducing human error and reaction time to dynamic battlefield conditions (Agarwala, 2023; Trusilo & Danks, 2023).

AI-driven precision weaponry will be used to direct GPS-based missiles and guide artillery shells, employing complex mathematical models to ensure munitions reach their targets with minimal deviation. These intelligent systems will improve the effectiveness of air-to-ground strikes by incorporating advanced perception, learning, decision-making, and collaboration capabilities (Chakravarty, 2023; Hashimov et al., 2023).

Additionally, AI will autonomously evaluate and adjust to combat environments in advanced weaponry like rockets, allowing for precise target prioritization to minimize collateral damage and civilian casualties. Some systems will include loitering capabilities, enabling them to remain in battlefields until an appropriate target is identified, thus enhancing what is termed ‘humanitarian precision’ in warfare (Aqeel et al., 2023; Patil & Rathi, 2022).

Overall, the operational application of AI in precision strike systems will transform defense strategies, ensuring strategic objectives are met with greater reliability and safety. AI's role will offer tactical and ethical advantages, making

precision strikes more discriminative and controlled, aligning military actions closely with humanitarian considerations.

5.4 Augmented cyber and information warfare capabilities

AI's role in managing and enhancing cyber defense systems extends to executing sophisticated electronic warfare strategies and cyber operations. AI can generate and analyze data for psychological operations, manage propaganda effectively, and counter misinformation. These capabilities allow for a more dynamic and responsive approach to both countering and waging cyber and information warfare, disrupting enemy communications and influencing public perception and morale.

5.4.1 Information warfare, denial and deception

AI is poised to significantly influence future conflicts through its role in information warfare, including denial and deception strategies. AI systems will enhance the generation and dissemination of deepfakes and synthetic media, which could manipulate public opinion and spread misinformation at unprecedented scales (Mai et al., 2023; Shobar & Tawil, 2023). This capability extends to creating highly realistic audio and video content that blurs the line between authentic and manipulated information (Garg & Jayanthiladevi, 2023; Petrosyan, 2024).

Adversarial machine learning will advance the abilities of cybercriminals and state actors to evade detection and spread malicious content, complicating cybersecurity efforts. In response, AI-driven defensive deception tactics will be developed to detect, deceive, and counteract these threats by misleading enemy systems about network or database statuses (Pilla et al., 2022).

AI will also play a crucial role in detecting disinformation and fake news in real-time through advanced content analysis using natural language processing and image recognition. These systems will analyze large datasets to identify misinformation patterns and automatically flag suspicious content, thus safeguarding information integrity in digital environments (Alshattnawi et al., 2024; Bai et al., 2023).

Moreover, AI will enhance strategic communication and psychological operations, tailoring messages to specific audiences to increase the effectiveness of propaganda and influence operations. AI tools will also monitor social media and communication platforms to quickly identify and counteract the spread of hostile disinformation (Dmytryshyn & Romanchukevych, 2022; Raazia et al., 2022).

In summary, as AI technologies evolve, they will dramatically reshape the landscape of information warfare, offering new methods for attack and defense. This evolution will necessitate continued advancements in AI ethics and security

measures to ensure these powerful tools do not compromise societal trust or global stability.

5.4.2 Cyber and electronic warfare

AI is set to significantly enhance cyber and electronic warfare capabilities by integrating into systems that secure communications, thwart cyberattacks, and manage complex military networks with increased efficiency and precision.

In cybersecurity, AI-driven systems will use advanced machine learning algorithms to detect cyber threats and predict attacks by analyzing network traffic patterns, allowing for preemptive measures to be taken. AI will also automate routine cybersecurity tasks, increasing the speed and effectiveness of responses to security incidents (Fazekas, 2022; Krichen, 2023).

In electronic warfare, AI will improve communication jamming and countermeasures, managing spectrum resources and conducting electronic attacks by exploiting vulnerabilities in enemy communication networks. These systems will adjust tactics dynamically in response to battlefield conditions and adversary strategies (Anupama, 2023; Fang & Li, 2022).

Adversarial AI techniques will be key in developing defenses against AI-driven threats, including training systems to recognize and counter sophisticated cyber-physical attacks. This training will incorporate both software simulations and hardware, ensuring viable responses in both cyber and physical domains (Barbeau & Garcia-Alfaro, 2022; Choi, 2022).

AI will also play a role in offensive cyber operations, coordinating attacks on critical infrastructure and military systems, potentially undermining public trust in institutions. These AI-coordinated attacks will exploit vulnerabilities with precision that is difficult for human operators to match (Leroy & Zolotaryova, 2023; Trachtman, 2022).

On the defensive front, AI will help develop adaptive cyber defense protocols to respond to new and evolving threats, autonomously patching software vulnerabilities and managing encryption standards to protect data integrity across secure military networks (Alzahrani & Aldhyani, 2022; Mohamed, 2023).

Overall, the integration of AI into cyber and electronic warfare represents a shift toward more autonomous, rapid, and data-driven conflict scenarios, enhancing both defensive and offensive capabilities and ensuring operational continuity in contested environments. This strategic use of AI will require robust ethical frameworks and stringent controls to prevent escalation and ensure compliance with international norms.

5.4.3 Societal manipulation and destabilization

AI is expected to play a dual role in both instigating and countering societal manipulation and destabilization. It will be extensively used in compromising critical infrastructure, influencing markets, and disrupting democratic processes,

leading to potential mass protests and civil unrest (P. Brown, 2024; Leroy & Zolotaryova, 2023; Mahmud, 2023).

In terms of critical infrastructure protection, AI will be crucial in identifying vulnerabilities within essential systems like energy production, power grids, and transportation. AI will enhance the security of these infrastructures against cyber threats through advanced risk management strategies, anomaly detection, and the development of adaptive security solutions. It will also enhance surveillance and monitoring to prevent unauthorized access (Demertzis et al., 2022; Haigh et al., 2023; Tam et al., 2023).

Conversely, AI could be employed in criminal activities such as hacking and market manipulation, potentially causing significant societal and economic disruptions (Mahmud, 2023; Moskalenko et al., 2023). However, similar AI systems will support management efforts against mass protests and civil unrest, aid in poverty alleviation, enforce trade restrictions, and navigate ethical challenges in automated financial trades (P. Brown, 2024; Mishra, 2023).

Maintaining trust in digital systems is crucial for the successful implementation of critical services. As AI drives more automated and predictive decision-making, it is essential to uphold human rights and ensure equity to preserve user confidence and the perception of fairness in digital society (Borda et al., 2022; Semenikhin et al., 2023). This strategic use of AI underscores its potential to significantly influence the stability and integrity of societies globally.

5.4.4 Strategic deterrence

Nations are increasingly investing in AI for defense, potentially shifting the global balance of power and sparking an AI arms race. This investment is aimed at developing new technologies for strategic advantage, which could alter the dynamics of peacetime and conflict probabilities across the globe (Sarkin & Sotoudehfar, 2024; Sultan & Jamy, 2022).

The advancement of AI could accelerate existing arms races, influence nuclear decision-making, and reshape military and political alliances. This scenario is emerging as a new revolution in military affairs, characterized by strategic maneuvers akin to a "hide and seek" game among nations (Ruppert, 2024; Sarkin & Sotoudehfar, 2024).

The global spread of military-relevant technologies is shifting power distributions in international politics, raising significant security concerns. AI's potential extends to enhancing military capabilities for both offensive and defensive strategies and monitoring nuclear activities to prevent technology misuse (Halkis et al., 2022; Liu & Guo, 2022).

AI will also play a role in countering adversaries by securing contested regions and exerting military power. New technologies will bolster digital sovereignty through extensive data collection via sensors in smart cities and other surveillance tools. This digital power will be used to identify vulnerabilities in conventional military systems, strengthen nuclear deterrence, and reduce risks of inadvertent escalation (Cancela & Goikoetxea, 2023; J. Johnson, 2022a).

Furthermore, AI will transform the nature of warfare into more remote operations, affecting global security policy and posing challenges to international law. Despite advancements, irregular warfare remains population-centric, and AI will enhance its efficiency through asymmetric tactics and misinformation strategies, enabling both state and non-state actors to engage in information warfare, denial, and deception (J. Johnson, 2022a; L. Jones, 2022).

Overall, the strategic application of AI in defense and warfare signals a major shift towards more automated, efficient, and complex conflict scenarios, necessitating robust ethical frameworks and international cooperation to manage emerging risks and ensure global stability.

5.5 Advanced human-machine interaction and performance enhancement

AI improves the interface between humans and machines, facilitating enhanced collaborative decision-making and efficiency. Beyond interaction, AI significantly augments human performance by integrating advanced diagnostics, treatment, and continuous health monitoring systems that optimize the physical and cognitive capabilities of military personnel. These technologies aid in managing stress, enhancing recovery rates, and tailoring training to individual needs, thereby ensuring that soldiers operate at their optimal performance levels in demanding environments.

5.5.1 Human performance enhancement

AI is set to transform military operations by significantly enhancing human performance, both cognitively and physically, potentially redefining traditional warfare paradigms and operational effectiveness.

Cognitive enhancements through neurotechnology, such as neuroprostheses and neuromodulation, will aim to boost intellectual capabilities including memory, attention, and decision-making speed, allowing soldiers to handle complex tasks more effectively under stress. Additionally, psychopharmaceuticals may be used to manage emotional responses and enhance mental resilience in combat situations (Jecker & Ko, 2022; Mun, 2022).

Physically, AI will aid in developing and controlling exoskeletons to provide soldiers with increased strength and endurance, while minimizing injury risks through support during strenuous activities. AI-enabled real-time biofeedback and neuromusculoskeletal training will optimize movement patterns, reducing injury rates in both training and combat (Lloyd et al., 2023).

AI will also refine military training regimes by utilizing advanced data analytics to personalize training programs, thus preventing injuries and promoting long-term wellness. AI-driven systems will support talent management, optimizing recruitment, retention, and leadership development (Chappuis, 2023; Gady, 2023; Hinton, 2023).

Operationally, AI will help mitigate moral and psychological risks on the battlefield. Autonomous systems performing surveillance and reconnaissance will reduce the need for direct human involvement in high-risk areas, preserving lives and lessening psychological impacts (Riesen, 2022).

Moreover, AI will improve recruitment strategies and human resource management by using machine learning to sift through data, identify optimal candidates, predict skill gaps, and enhance organizational performance (Hinton, 2023; Pai et al., 2022).

Overall, the integration of AI into enhancing human performance in military contexts promises to advance how soldiers are trained, equipped, and managed, ensuring operations are conducted with greater safety, efficiency, and strategic depth.

5.5.2 Medical diagnostics and treatment

AI systems have a significant promise to improve medical diagnostics and treatment, enhancing healthcare delivery in both military and civilian contexts by improving the precision and speed of medical diagnoses. AI systems will analyze a broad range of medical images, from ultrasounds to complex CT scans, detecting subtle abnormalities and diagnosing conditions more quickly and accurately than currently possible (Arulprakash et al., 2022; Guy et al., 2024).

Predictive AI models will become essential in forecasting disease progression and outbreak patterns, enabling healthcare systems to respond more effectively. In military settings, these forecasts will facilitate strategic medical logistics planning, ensuring efficient resource allocation during crises (Jenkins et al., 2023; Snider et al., 2022).

AI will also transform treatment protocols through autonomous robotic surgery, which will perform complex procedures with greater precision and efficiency, potentially reducing surgery times and improving outcomes by minimizing human error (Guy et al., 2024).

In rehabilitation, AI will support the development of personalized treatment plans and use virtual reality to provide immersive, adaptive rehabilitation environments, optimizing recovery processes (Hoppes et al., 2024).

Additionally, AI-enhanced wearable sensors will continuously monitor health, providing real-time data on physiological and behavioral changes. This technology will be invaluable in conflict zones for monitoring soldiers' health, offering early warnings of potential issues and improving battlefield casualty management (Lloyd et al., 2023).

Furthermore, as medical devices become increasingly interconnected, AI will play a crucial role in cybersecurity, protecting these systems from cyber threats and ensuring the security of medical data and device functionality (Taheri & Asadizanjani, 2022). This comprehensive integration of AI into healthcare promises significant advancements in diagnostics, treatment, and overall health management.

5.5.3 Human-machine collaboration

As digital systems proliferate, AI will play a pivotal role in enhancing usability, transforming daily life, military operations, and decision-making processes. AI is set to integrate deeply into military operations, boosting the effectiveness and efficiency of both human personnel and autonomous systems.

AI-enhanced conversational agents and chatbots will become crucial for military personnel, providing real-time decision support, disseminating information, and aiding in mission planning. These systems will leverage advanced natural language processing to improve communication speed and accuracy, facilitating intuitive interactions between soldiers and machines and improving coordination on dynamic battlefields (Ahmed, 2024; Garg & Jayanthiladevi, 2023).

Further advancements in neurotechnology, such as brain-computer interfaces, may soon allow direct communication between human cognitive processes and machines, enabling soldiers to control military hardware through thought, which could significantly reduce response times and increase operation precision (Jecker & Ko, 2022; Stinchfield, 2023).

AI will also automate and optimize tactical decision-making by processing data faster than humans, providing strategic recommendations, predicting enemy movements, and identifying threats. This will reduce cognitive load on commanders, allowing them to concentrate on critical aspects of missions (Ahn et al., 2024; Pulyala, 2024).

Moreover, as AI becomes more integral to operations, trust and transparency in AI systems will be crucial. Systems capable of explaining their decisions in understandable terms will likely be more trusted and effectively integrated into military strategies, ensuring operational effectiveness and maintaining accountability (Vorm & Combs, 2022).

In summary, AI's integration into military contexts promises not only enhanced capabilities but also groundbreaking changes in task performance and decision-making in complex, evolving conflict scenarios. This synergy between human intuition and AI’s analytical prowess will redefine military engagements, making them more strategic and safer for human personnel.

5.5.4 Simulation, testing and training

AI is set to become fundamental in simulation, testing, and training within military and security contexts, significantly enhancing the preparation of personnel for real-world conflicts. AI-driven simulations and virtual reality (VR) environments will be extensively used to train military personnel and law enforcement officers, providing realistic and dynamic scenarios that replicate the unpredictability of actual combat and emergency situations (Covaciu & Iordan, 2022; Salor & Baeza, 2023). These technologies will allow trainees to interact with virtual adversaries and make critical decisions in safe, controlled settings, thereby increasing preparedness and potentially reducing real-world casualties.

AI will personalize training by adjusting challenges based on trainee performance, tailoring the difficulty to individual needs and optimizing training outcomes by strengthening specific skills (Loh et al., 2024; Pavlidis, 2024).

In testing and validation, AI will play a critical role in developing and evaluating both autonomous systems and human-centered operations. It will use adversarial training and testing to anticipate and mitigate potential vulnerabilities, enhancing the robustness of defense technologies (Anastasiou et al., 2022; Hannon et al., 2024). AI systems will adapt continuously, improving their capability to handle unexpected or adversarial scenarios prevalent in cyber warfare and autonomous combat.

Furthermore, AI will automate the analysis of large datasets generated during simulations and tests, facilitating rapid iteration and refinement of military tactics and strategies. This capability will speed up the development cycle of military technologies and operational plans (Patil & Rathi, 2022; Yilmaz et al., 2023). As AI technologies evolve, they will also enable the seamless integration of new data into ongoing training programs, ensuring modules remain current with the latest tactics and threat intelligence. This integration of AI will not only enhance military capabilities but also lead to innovations in how complex scenarios are approached and managed in training and real-world applications.

5.5.5 Biometric recognition and analysis

AI is set to significantly enhance biometric recognition and analysis, integrating into security systems to enable advanced facial, iris, and fingerprint recognition technologies. These capabilities will improve identification accuracy in real-time and are expected to be extensively used in border security to streamline passport control, detect false documents, and monitor unauthorized entries (Boice et al., 2022; Boutin, 2023).

Additionally, AI will automate the analysis of body language and facial expressions, providing security personnel with crucial insights for identifying potential threats, particularly in crowded public spaces like airports and during large events where rapid response is essential (Kim & Joo, 2022; Xi, 2023).

In law enforcement and military operations, AI-powered facial recognition will be employed to track suspects and manage crowd control. These systems will likely be integrated with criminal databases, enhancing the ability of agencies to swiftly identify and apprehend offenders (Chattopadhyay, 2023; Yang et al., 2023).

AI will also bolster the security of biometric systems against cyber threats, crucial as these systems become integral to security infrastructure. AI's adaptive capabilities will be leveraged to protect against evolving cybersecurity threats (Moskalenko et al., 2023).

In military contexts, AI-driven biometric systems will be used for security clearance and access control, and to enhance commanders' situational awareness. By integrating biometric data with other intelligence, AI systems will provide a comprehensive operational picture, supporting decision-making during critical

operations (Ambadekar et al., 2023; Tyczewska et al., 2023). Overall, AI's integration into biometric technologies promises to reform security measures, offering more efficient, precise, and robust systems for both civil and military applications.

5.5.6 Behavioral analysis

AI systems are poised to significantly advance behavioral analysis in future conflicts, providing insights that improve security and military operational strategies. These systems will analyze and predict human behavior to anticipate threats and enhance responses across various conflict scenarios.

AI technologies will detect behavioral cues within online communities and physical environments, analyzing data from social media and surveillance to identify patterns linked to security risks like radicalization or potential terrorist activities (Fahim Sufi, 2023; Žigulić et al., 2024). In military contexts, AI-driven analysis will predict enemy behavior, aiding strategists in developing more effective tactics and potentially increasing military engagement efficacy without direct confrontation (Basrur & Wu, 2023; Salor & Baeza, 2023).

The integration of federated learning will enable AI systems to utilize decentralized data sources while maintaining data privacy, essential in coalition military operations where data sharing must balance utility and security.

AI will also adapt to changing environments and optimize performance over time through autonomous learning capabilities like reinforcement learning. This will lead to robust systems that support real-time tactical decisions in conflict scenarios (Khan et al., 2022; McFarland & Assaad, 2023).

Additionally, AI will manage crowd behavior and plan evacuation routes during emergencies, optimizing responses and potentially saving lives by predicting movement patterns and optimizing resource allocation (Taheri & Asadizanjani, 2022; Tyczewska et al., 2023).

Ethical considerations will be paramount, as the use of AI in behavioral analysis requires strict adherence to ethical standards to prevent misuse and ensure respect for individual rights and privacy (Ahn et al., 2024; Trusilo, 2023). This strategic application of AI promises to transform both military efficiency and public safety, highlighting the need for careful management and oversight.

6 DISCUSSION AND ANALYSIS

Where to take the data gathered during the review? What to do with it? The key goal for this study was to create a model that would help the reader to understand on a strategic level the development of AI-related technology regarding the future battlespace. As has been witnessed by the amount and diverse nature of publications analyzed for this study, that is indeed not an easy task.

6.1 Arguments for and against the use of AI in military context

The utilization of AI in military contexts is surrounded by a complex interplay of ethical, legal, and strategic considerations. The debate encompasses a broad spectrum of opinions and research focusing on both the potential benefits and risks associated with deploying AI systems, particularly LAWS.

On one side of the debate, proponents of LAWS argue that these technologies can enhance the ethical conduct of warfare. They contend that LAWS can adhere more strictly to the laws of war than human soldiers, potentially reducing the number of civilian casualties and minimizing collateral damage. This argument hinges on the assumption that future advancements in AI will enable these systems to accurately target combatants while sparing non-combatants, thereby conducting warfare more ethically and effectively. Furthermore, supporters suggest that LAWS can reduce the psychological and moral burden on human soldiers by decreasing their direct involvement in lethal decision-making processes. This could potentially lower the incidence of psychological trauma such as PTSD among combatants. (Arandjelović, 2023; Malmio, 2023; Riesen, 2022.)

However, the arguments supporting the use of LAWS are met with significant ethical and strategic counterarguments. Critics of LAWS highlight the unpredictability of autonomous systems, pointing out the inherent risks of allowing machines to make life-and-death decisions without human oversight.

This unpredictability could lead to unintended escalations and misinterpretations in military engagements. Moreover, the erosion of meaningful human control over military operations raises profound moral and ethical concerns. The difficulty in attributing accountability for the actions taken by LAWS complicates the legal frameworks that govern warfare and international law, potentially leading to a gap in moral responsibility. (Johnson, 2022; Malmio, 2023; Matta et al., 2022.)

The debate also addresses the impact of LAWS on global peace and security. While some argue that the precision and efficiency of LAWS could deter warfare and reduce the scale of conflict, others worry that the proliferation of these technologies could trigger a new arms race, destabilizing international relations and lowering the threshold for engaging in conflict.

From a regulatory standpoint, the international community faces challenges in establishing norms and agreements to govern the development and use of LAWS. The differing views between most of the smaller nations as opposed to key states like the U.S., China, and Russia complicate the creation of a cohesive global policy. Each country's strategic and geopolitical interests influence their stance on LAWS regulation, which may prevent the formation of a consensus in international forums such as the UN Convention on Certain Conventional Weapons (UN CCW). (Bode et al., 2023.)

Despite these challenges, there are possibilities for advancing international norms concerning LAWS. These include the leadership of smaller or non-major-power states, the establishment of new forums and processes for negotiation, the development of binding international agreements, and the enhancement of existing non-binding principles into more robust legal frameworks. Such efforts require a multi-faceted approach that combines diplomatic engagement, legal innovation, and international cooperation. (Bode et al., 2023.)

In conclusion, while AI in military contexts presents opportunities for improving the conduct of warfare and potentially enhancing global security, it also raises profound ethical, legal, and strategic challenges that must be carefully navigated. The global community must engage in a thoughtful and rigorous debate to ensure that the development and deployment of LAWS align with international law, ethical standards, and the overall goal of maintaining peace and security.

6.2 A model for applying AI to strategy and operations

Through critical analysis and combining the results of both the review of the trends and the review of the applications, it was possible to outline a straightforward visualization of the relationships of the two. To anchor the outcome into the real world of defense and security planners and decision-makers, the model was designed to include a link to both the strategic and operative levels.

Military strategy is a topic that has interested numerous authors throughout history. For the purpose of this study, a framework used for example by the U.S. Joint Chiefs of Staff (2018) was chosen. As this is not a study in strategy, comparing a number of the different available frameworks was outside the scope. Briefly, the components of military strategy are described this way:

> All strategies entail the same fundamental logic of ends, ways, and means. A comprehensive and effective strategy answers three basic questions: 1) Where do we want to go, or what are the desired **ends**? 2) How do we get there, or what are the **ways**? 3) What resources are available, or what are the **means**? 4) What are the **risks** and costs associated with the strategy? (*Joint Doctrine Note 1-18: Strategy*, 2018, p. V.)

This simple framework provides a solid strategic interface for the potential applications of AI in the future battlespace. The desired ends may be affected by the applications available. The ways and the means are most likely affected by the available capabilities, including AI-enabled capabilities, and the associated risks are definitely shaped based on the capabilities used, especially since some AI technologies have unique risks.

To complement the approach on strategy, it was important to include a framework for anchoring the operative level as well. Different types of Principles of War were considered. Freedman (2013) describes a number of them, starting from the Bible (2013, pp. 11–21), continuing to the Greeks (2013, pp. 22–41), going through Sun-Tzu and Machiavelli (2013, pp. 42–53) and ending up with Clausewitz, Bonaparte and Jomini (2013, pp. 82–95) and more recent examples.

However, Van Avery (2007) has proposed a modernized version of the national U.S. Army principles published in Field Manual 3-0, Operations (*FM 3–0, Operations*, 2001), that consists of the following parts:

1. Objective
2. Speed
3. Concentration of Effects
4. Economy of Effects
5. Pervasive Awareness
6. Continuous Planning
7. Flexibility
8. Sustainment
9. Efficiency of Command
10. Security
11. Integration of Actors
12. Surprise

Again, these principles provide enough traction to interact with the potential applications. Comparing the capabilities described in section 5, Future applications of AI, it is easy to see how each of these principles can be influenced by the way AI systems are used in future conflicts and in the battlespace.

Bringing together the trends, applications, strategy and operations, a visualization and a model is proposed below in FIGURE 4 A model for AI applications in strategy and operations. The model describes how the high-level trends have an effect on the applications, which in turn have an effect on both the strategy and the operations. While the causality is self-evident in an interconnected world, the model can help the defense and security planners and decision-makers to put together a strategic-level understanding of the key tracks or themes where AI systems are applicable, and what they can be applied to. AI systems do provide a multitude of capabilities outside the most visible (and feared) lethal autonomous weapon systems. For a senior stakeholder it is vital to understand the dependencies and possibilities. The model can be used as a basis for discussion to find potential solutions to both strategic and operational needs.

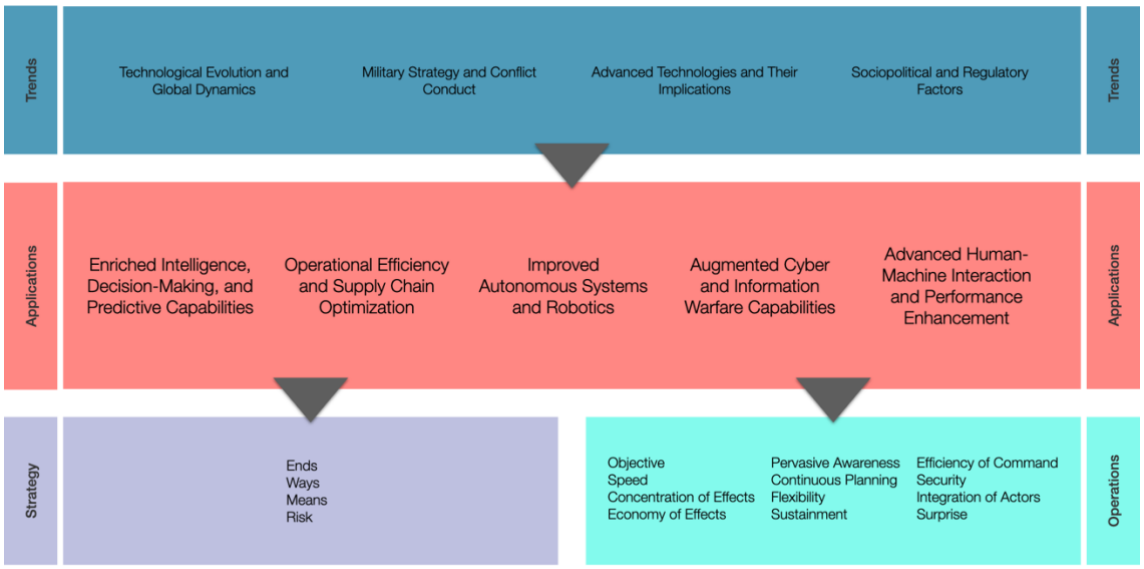

FIGURE 4 A model for AI applications in strategy and operations

6.3 Linking strategy and operations to the applications

The number of different connections and paths of influence between the different parts the model affords is immense. In order to be able to use the model for any practical analysis, it is essential to offer support for finding the most relevant dependencies. The dependencies are described in a four-step model:

- – No contribution
- * Some contribution
- ** Moderate contribution
- *** Strong contribution

The dependencies between the applications and strategy are visualized below in TABLE 7 AI influencing strategy, and the dependencies between the applications and operations in TABLE 8 AI influencing operations. The strength of the contributions was estimated critically in the somewhat limited level of depth and detail the scope of this study allowed. The estimation was done by cross-referencing the descriptions of the relevant applications (section 5, Future applications of AI) and trends (section 4, Trends guiding the use of AI in the battlespace). Again, the intensity of the contribution should be used as a foundation of further study and analysis, not as a definitive answer. Also, it is important to note, that the type of contribution might change over time as the technology develops, and should be reviewed periodically to stay relevant.

TABLE 7 AI influencing strategy

Applications of AI	Fundamental Elements of Strategy: Ends	Ways	Means	Risk
Enriched Intelligence, Decision-Making, and Predictive Capabilities				
Environmental monitoring	***	**	**	*
Decision-making support and automation	***	***	***	***
Analysis, predictions and situational awareness	***	***	***	***
Data mining and processing	**	*	**	**
Information collection	***	**	**	*
Image and video analysis	–	**	*	*
Target identification, tracking and analysis	–	***	**	*
Threat detection and assessment	***	**	**	*
Operational Efficiency and Supply Chain Optimization				
Logistics and supply chain management	*	**	***	**
Predictive maintenance	–	*	***	**
Dynamic resource allocation	–	**	***	*
Communication systems	–	**	**	*
Technology development	**	**	***	*
Improved Autonomous Systems and Robotics				
Autonomous weapons systems	–	***	***	***
Autonomous protection systems	–	**	**	**
Autonomous vehicles and robotics	–	**	***	*
Precision strike weapons	–	***	*	**
Augmented Cyber and Information Warfare Capabilities				
Information warfare, denial and deception	**	***	**	**
Cyber and electronic warfare	**	***	**	**
Societal manipulation and destabilisation	**	***	**	**
Strategic deterrence	***	***	**	**
Advanced Human-Machine Interaction and Performance Enhancement				
Human performance enhancement	–	*	**	*
Medical diagnostics and treatment	–	–	**	*
Human-machine collaboration	–	**	**	*
Simulation, testing and training	*	***	**	*
Biometric recognition and analysis	–	*	*	*
Behavioral analysis	–	**	*	*

TABLE 8 AI influencing operations

Applications of AI	Principles of War											
	Objective	Speed	Concentration of Effects	Economy of Effects	Pervasive Awareness	Continuous Planning	Flexibility	Sustainment	Efficiency of Command	Security	Integration of Actors	Surprise
Enriched Intelligence, Decision-Making, and Predictive Capabilities												
Environmental monitoring	**	**	–	*	**	**	*	*	**	*	–	*
Decision-making support and automation	***	***	***	***	***	***	*	***	*	**	*	***
Analysis, predictions and situational awareness	***	***	***	**	***	***	*	**	*	*	*	***
Data mining and processing	**	*	**	**	***	**	*	*	*	*	*	***
Information collection	*	**	***	**	***	**	*	**	*	**	–	***
Image and video analysis	*	**	*	*	***	**	*	–	*	**	–	***
Target identification, tracking and analysis	**	**	***	**	**	**	*	**	*	**	–	***
Threat detection and assessment	**	*	**	**	***	**	*	*	*	***	–	**
Operational Efficiency and Supply Chain Optimization												
Logistics and supply chain management	*	*	**	**	–	**	***	***	–	–	**	**
Predictive maintenance	*	*	*	*	–	**	***	**	–	–	–	**
Dynamic resource allocation	*	*	**	***	–	**	***	**	–	–	**	**
Communication systems	*	**	*	–	*	*	**	*	***	–	***	***
Technology development	***	*	**	**	**	**	*	–	*	–	*	**
Improved Autonomous Systems and Robotics												
Autonomous weapons systems	**	***	***	**	*	–	**	–	–	*	–	***
Autonomous protection systems	*	*	**	**	*	–	*	–	–	*	–	*
Autonomous vehicles and robotics	**	***	**	**	**	–	**	–	–	*	–	**
Precision strike weapons	***	***	***	**	–	–	*	–	–	*	–	***
Augmented Cyber and Information Warfare Capabilities												
Information warfare, denial and deception	**	–	**	*	**	–	**	*	–	*	***	***
Cyber and electronic warfare	**	–	*	**	**	–	**	*	*	*	**	***
Societal manipulation and destabilisation	**	–	*	*	–	–	**	*	–	**	–	**
Strategic deterrence	***	–	*	*	–	*	**	**	–	*	–	*
Advanced Human-Machine Interaction and Performance Enhancement												
Human performance enhancement	–	*	*	*	–	–	**	*	*	*	–	**
Medical diagnostics and treatment	–	–	–	*	–	–	–	*	–	*	–	–
Human-machine collaboration	–	**	*	**	**	–	*	**	*	**	**	*
Simulation, testing and training	*	*	**	**	–	*	*	*	–	–	*	**
Biometric recognition and analysis	–	–	–	*	**	*	*	*	–	*	–	*
Behavioral analysis	*	–	–	*	**	*	*	*	–	*	–	***

6.4 Linking trends to the applications

In section 4, Trends guiding the use of AI in the battlespace, the 17 significant future trends were explored and presented in detail. These trends were recognized based on literature, and it is very likely that most if not all of them will have an effect on how the process of adapting AI systems into conflicts will play out. With the trends being described, the potential applications of AI presented in section 5, Future applications of AI, were cross-referenced with the trends through critical thematic evaluation.

Due to the limitations imposed on this study and the significant number of pairings (17 trends times 27 applications), the analysis was conducted in a simplified manner, resulting in binary relationships: either a trend has an effect on an application or not. However, the real-world relationships are complex and nuanced, and it is recognized that this analysis is not definitive. The results should be used as a basis for thought and discussion. The analysis process resulted in a matrix describing the relationships between the trends and the applications, presented below in TABLE 9 The relations of trends and AI use cases. The arrows in the diagram display the existence and direction of the influence.

TABLE 9 The relations of trends and AI use cases

Applications of AI	Technological Evolution and Global Dynamics				Sociopolitical and Regulatory Factors				Military Strategy and Conflict Conduct					Advanced Technologies and Their Implications			
	Urbanization and global expansion	Climate dynamics	Availability of technology and funding	Availability of energy, materials and components	Non-state actors and grey zone tactics	Regulation and ethics	Public imagery and accountability	Societal resilience and desensitization	Unmanned, intelligent and autonomous systems	Directed energy and electromagnetic armaments	Space and high-altitude platforms	Swarming and distributed warfare	Nuclear proliferation adn deterrence	Nanotechnology and other advanced materials	Quantum computing and advances in data processing and transfer	Machine speed data analysis and decision-making	Cyber and electronic warfare
Enriched Intelligence, Decision-Making, and Predictive Capabilities																	
Environmental monitoring	↵	↵	↵	↵	↵		↵	↵	↵		↵			↵	↵	↵	
Decision-making support and automation	↵		↵	↵	↵	↵	↵	↵			↵	↵		↵	↵	↵	↵
Analysis, predictions and situational awareness	↵		↵	↵	↵	↵	↵	↵	↵		↵	↵	↵	↵	↵	↵	↵
Data mining and processing			↵	↵	↵	↵	↵	↵						↵	↵	↵	↵
Information collection	↵		↵	↵		↵			↵		↵	↵		↵	↵	↵	
Image and video analysis			↵	↵		↵								↵	↵	↵	
Target identification, tracking and analysis	↵		↵	↵	↵		↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵
Threat detection and assessment	↵	↵	↵	↵	↵		↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵
Operational Efficiency and Supply Chain Optimization																	
Logistics and supply chain management	↵	↵	↵	↵					↵		↵	↵		↵	↵	↵	
Predictive maintenance			↵	↵								↵		↵	↵	↵	
Dynamic resource allocation			↵	↵			↵		↵		↵	↵			↵	↵	↵
Communication systems			↵	↵					↵		↵			↵	↵	↵	↵
Technology development	↵	↵	↵	↵			↵		↵	↵	↵	↵	↵	↵	↵	↵	↵
Improved Autonomous Systems and Robotics																	
Autonomous weapons systems			↵	↵	↵	↵	↵	↵	↵	↵	↵	↵		↵	↵	↵	↵
Autonomous protection systems	↵	↵	↵	↵	↵		↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵
Autonomous vehicles and robotics	↵		↵	↵	↵		↵		↵		↵	↵		↵	↵	↵	↵
Precision strike weapons	↵		↵	↵	↵	↵	↵	↵	↵	↵	↵	↵		↵	↵	↵	↵
Augmented Cyber and Information Warfare Capabilities																	
Information warfare, denial and deception	↵		↵	↵	↵	↵	↵	↵	↵				↵		↵	↵	↵
Cyber and electronic warfare	↵		↵	↵	↵		↵	↵		↵	↵	↵	↵		↵	↵	↵
Societal manipulation and destabilisation	↵	↵	↵	↵	↵		↵	↵	↵				↵		↵	↵	↵
Strategic deterrence	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵	↵
Advanced Human-Machine Interaction and Performance Enhancement																	
Human performance enhancement			↵	↵		↵	↵	↵						↵	↵	↵	
Medical diagnostics and treatment			↵	↵		↵			↵					↵	↵	↵	
Human-machine collaboration			↵	↵			↵	↵	↵			↵		↵	↵	↵	
Simulation, testing and training			↵	↵			↵	↵	↵			↵			↵	↵	↵
Biometric recognition and analysis			↵	↵		↵	↵	↵							↵	↵	
Behavioral analysis			↵	↵			↵					↵			↵	↵	↵

Trends

It is notable, that several of the trends seem to be more influential than others. The trends Availability of technology and funding; Availability of energy, materials and components; Quantum computing and advances in data processing and transfer; and Machine speed data analysis and decision-making were seen to influence every type of application. In a world with finite time resources, they at least seem to be the ones to keep an eye on, for everyone interested in the development of AI-enabled capabilities in future battlespace. Likewise, out of all applications, Strategic deterrence is affected by all of the trends. To be able to forecast the developments in the balance of global deterrence, one really must be able to assimilate a wealth of information from different fields.

6.5 Applying the model

How to apply the model in practice? It can be used to reverse-engineer the potential tools to leverage to solve a concrete need or a problem. As an example, let's consider a defense and security planner is concerned about the efficiency of command in operations. Backtracking from that, consulting TABLE 8 AI influencing operations and cross-referencing the descriptions of the different applications when needed, it seems plausible that the following applications could have an effect on it:

- Enhanced intelligence, decision-making, and predictive capabilities
- Operational efficiency and supply chain optimization
- Advanced human-machine interaction and performance enhancement

Again, backtracking, consulting TABLE 9 The relations of trends and AI use cases and cross-referencing the trend descriptions, the following trends can be seen as the most relevant:

- Technological evolution and global dynamics
- Advanced technologies and their implications

The process is visualized below in FIGURE 5 An example of using the model for finding key themes. This way, by using the model and the supporting material provided in this study, it is possible to find key themes both on the application and trend level, that should be the focus of analysis, ideation, research and development in order to improve any given pain point in both strategy and operations. With the key themes selected, it is easy to open up the avenues of inquiry based on the theme descriptions in this study.

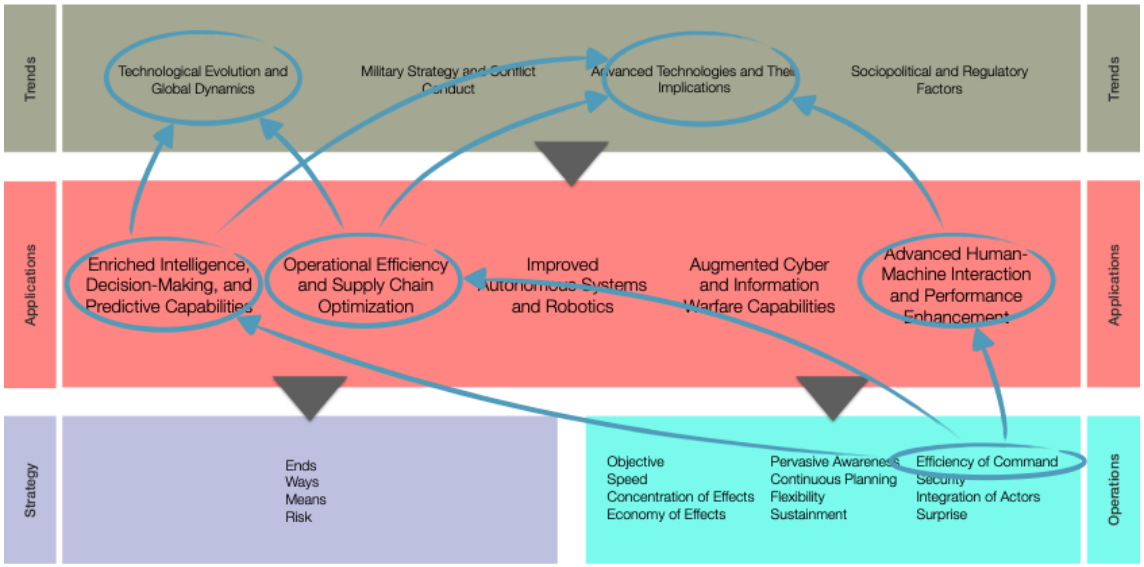

FIGURE 5 An example of using the model for finding key themes

7 CONCLUSIONS

This study set out to find what kind of applications of AI are likely to have the most impact on future warfare and the battlespace in the near future (between 2024 and 2030). To close on the subject, it was essential to research what kind of developments in global trends and technology are likely to have significant impact on the development of AI systems in the defense and security domain, and what kind of AI system use scenarios are likely in the future battlespace. Since the topic is vast, the depth of the study was limited in order to be able to provide a strategic-level overview for a senior defense or security decision-maker.

The study proposes that the trends likely having the strongest impact on the development of AI systems for the defense and security domain are 1) technological evolution and global dynamics, 2) sociopolitical and regulatory factors, 3) military strategy and conflict conduct, and 4) advanced technologies and their implications. From a strategic and national security perspective these should be key interest from both the point of keeping up to date on the developments, but also from the point of policy-making in order to be able to influence the developments in a benevolent manner. These are some of the key factors that outline the strategic landscape the future warfare is conducted in.

In that landscape, the applications of AI we can currently forecast are going to fall in the following categories: 1) enhanced intelligence, decision-making, and predictive capabilities; 2) operational efficiency and supply chain optimization; 3) advanced human-machine interaction and performance enhancement; 4) cyber and information warfare enhancement; and 5) autonomous systems and robotics. All of these applications have significant potential to alter both the battlespace itself, and the warfare conducted in it, and thus will most likely have a serious effect on all conflicts to come.

The future battlespace will include both the traditional battlefield with the warfighters, and the wider society with all the civilians and the infrastructure. There are numerous traditional capabilities for creating effect in the whole battlespace, and AI systems will add even more new defensive and offensive elements to the complex environment.

However, the utilization of AI in military settings, particularly with LAWS, is also marked by a complex mix of ethical, legal, and strategic issues. Proponents argue that LAWS can conduct warfare more ethically than humans by adhering more closely to the laws of war, thereby reducing civilian casualties and the psychological burden on soldiers, which could lessen incidents of PTSD. However, critics point out the risks associated with the unpredictability of autonomous systems and the lack of human oversight, which could lead to unintended escalations and a dilution of accountability. This complicates the legal and ethical frameworks of international warfare.

The debate extends to the effects of LAWS on global peace and security, with concerns that their proliferation might spur an arms race and destabilize international relations. Regulatory challenges arise from the divergent views of different nations, complicating the creation of a unified global policy on the use and development of LAWS. Despite these challenges, there are opportunities to advance international norms through the leadership of smaller nations, new negotiation forums, and the development of binding agreements.

Ultimately, while LAWS present potential improvements in the conduct of warfare and global security, they also introduce significant challenges that require careful consideration and international dialogue to ensure they align with international law and ethical standards.

In order to be able to plan for and to build the capabilities needed to keep the society and the population safe, defense and security planners and decision-makers need to understand the potential of AI technology. Unlike nuclear weapon technology, AI systems are easily approachable and affordable. Even non-state actors will have both the knowhow and financial means to leverage the possibilities the technology offers. As responsible decision-makers we cannot ignore this. Therefore, we must stay up to date on the capability development, even on the types of systems we might not utilize ourselves. Since the technology is so easily accessible and cannot be controlled with international treaties in the same way as for example nuclear weapons, it is entirely possible that such systems might be used against us some day.

There needs to be clear and widely shared ethical guidelines and legal frameworks on how AI systems are developed and utilized. The guidelines must be in alignment with international law and human values. To achieve this, it is necessary to engage in active public discourse, including an interdisciplinary board of participants from different fields.

Staying current on the developments in AI field is a daunting task. New systems and studies are published continuously. To alleviate this, the study proposes a model for structuring knowledge, and conducting both research and discussion. The proposed model does integrate the potential applications of AI into strategic and operational frameworks. Still, the work of generating new understanding should be conducted in interdisciplinary teams.

Even though the study is comprehensive, it is not complete. Further studies should be conducted on the trends influencing the adoption of AI systems in defense and security use, in the technologies themselves and their potential

applications, and especially the relationships between these two and military operations and strategy. Nevertheless, this study offers a solid foundation for generating the future understanding.

BIBLIOGRAPHY

Abbass, H. (2021). Editorial: What is Artificial Intelligence? *IEEE Transactions on Artificial Intelligence*, *2*(2), 94–95. https://doi.org/10.1109/TAI.2021.3096243

Acemoglu, D., Autor, D., Hazell, J., & Restrepo, P. (2022). Artificial Intelligence and Jobs: Evidence from Online Vacancies: Journal of Labor Economics. *Journal of Labor Economics*, *40*, S293–S340. https://doi.org/10.1086/718327

Adel, O., Fathalla, K. M., & Abo ElFarag, A. (2023). MM-EMOR: Multi-Modal Emotion Recognition of Social Media Using Concatenated Deep Learning Networks. *Big Data and Cognitive Computing*, *7*(4), Article 4. https://doi.org/10.3390/bdcc7040164

Adib Bin Rashid, Ashfakul Karim Kausik, Ahamed Al Hassan Sunny, & Mehedy Hassan Bappy. (2023). Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges. *International Journal of Intelligent Systems*, *2023*. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1155/2023/8676366

Agarwala, N. (2023). Robots and Artificial Intelligence in the Military. *Univerzita Obrany. Ustav Strategickych Studii. Obrana a Strategie*, *2023*(2), 83–100. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection; Social Science Premium Collection. https://doi.org/10.3849/1802-7199.23.2023.02.083-100

Ahmed, A. M. M. (2024). A New "Mammy" in the Age of Digitalization; Human Insecurity Versus Utopian Affective Algorithms in Kazuo Ishiguro's Klara and The Sun. *3L, Language, Linguistics, Literature*, *30*(1), 24–35. ProQuest Central; Publicly Available Content Database; Social Science Premium Collection. https://doi.org/10.17576/3L-2024-3001-03

Ahn, J., Kim, J., & Sung, Y. (2024). The role of perceived freewill in crises of human-AI interaction: The mediating role of ethical responsibility of AI. *International Journal of Advertising*, *0*(0), 1–27. https://doi.org/10.1080/02650487.2023.2299563

AI and autonomous weapons arms transfers. (2022, August). OpenGlobalRights. https://www.openglobalrights.org/ai-and-autonomous-weapons-arms-transfers/

AI weaponry should be banned from the battlefield. (2023, August 14). UNSW Sites. https://www.unsw.edu.au/newsroom/news/2023/08/ai-weaponry-should-be-banned-from-the-battlefield

Ali, M. A., Irfan, M. S., Khan, T., Khalid, M. Y., & Umer, R. (2023). Graphene nanoparticles as data generating digital materials in industry 4.0. *Scientific Reports (Nature Publisher Group)*, *13*(1), 4945. ProQuest Central; Publicly

Available Content Database; SciTech Premium Collection. https://doi.org/10.1038/s41598-023-31672-y

Alshattnawi, S., Shatnawi, A., AlSobeh, A. M., & Magableh, A. A. (2024). Beyond Word-Based Model Embeddings: Contextualized Representations for Enhanced Social Media Spam Detection. *Applied Sciences*, *14*(6), 2254. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/app14062254

Alyousef, A. S., Srinivasan, K., Mohamad Shady Alrahhal, Alshammari, M., & Al-Akhras, M. (2022). Preserving Location Privacy in the IoT against Advanced Attacks using Deep Learning. *International Journal of Advanced Computer Science and Applications*, *13*(1). Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.14569/IJACSA.2022.0130152

Alzahrani, A., & Aldhyani, T. H. H. (2022). Artificial Intelligence Algorithms for Detecting and Classifying MQTT Protocol Internet of Things Attacks. *Electronics*, *11*(22), 3837. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics11223837

Ambadekar, P. K., Ambadekar, S., Choudhari, C. M., Patil, S. A., & Gawande, S. H. (2023). Artificial intelligence and its relevance in mechanical engineering from Industry 4.0 perspective. *Australian Journal of Mechanical Engineering*, *0*(0), 1–21. https://doi.org/10.1080/14484846.2023.2249144

Amirkhanyan, Z. (2022). A Failure to Innovate: The Second Nagorno-Karabakh War. *Parameters*, *52*(1), 119–134.

Anastasiou, T., Karagiorgou, S., Petrou, P., Papamartzivanos, D., Giannetsos, T., Tsirigotaki, G., & Keizer, J. (2022). Towards Robustifying Image Classifiers against the Perils of Adversarial Attacks on Artificial Intelligence Systems. *Sensors*, *22*(18), 6905. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s22186905

Anonymous. (2023). *Current Research Resources in DEFENSE ACQUISITION* (2839081576). Defense Acquisition Research Journal; ProQuest Central; SciTech Premium Collection. https://www.proquest.com/scholarly-journals/current-research-resources-defense-acquisition/docview/2839081576/se-2?accountid=11774

Anupama, V. (2023). Potential impact of artificial intelligence on the emerging world order. *F1000Research*, *11*. https://doi.org/10.12688/f1000research.124906.2

Aqeel, I., Khormi, I. M., Khan, S. B., Shuaib, M., Almusharraf, A., Alam, S., & Alkhaldi, N. A. (2023). Load Balancing Using Artificial Intelligence for Cloud-Enabled Internet of Everything in Healthcare Domain. *Sensors*, *23*(11), 5349. https://doi.org/10.3390/s23115349

Arachchi Dimuthu Maduranga, H. A., & Dinesh Samarasinghe, G. (2023). Impact of embedded AI mobile smart speech recognition on consumer attitudes towards AI and purchase intention across Generations X and Y. *European Journal of Management Studies (Online)*. https://doi.org/10.1108/EJMS-03-2023-0019

Arandjelović, O. (2023). A case for "killer robots": Why in the long run martial AI may be good for peace. *Journal of Ethics in Entrepreneurship and Technology*, *3*(1), 20–32. https://doi.org/10.1108/JEET-01-2023-0003

Arulprakash, E., Martin, A., & Lakshmi, T. M. (2022). A Study on Indirect Performance Parameters of Object Detection. *SN Computer Science*, *3*(5), 386. ProQuest Central; SciTech Premium Collection. https://doi.org/10.1007/s42979-022-01277-9

Ayoub, K., & Payne, K. (2016). Strategy in the Age of Artificial Intelligence. *Journal of Strategic Studies*, *39*(5–6), 793–819. https://doi.org/10.1080/01402390.2015.1088838

Bae, I., & Hong, J. (2023). Survey on the Developments of Unmanned Marine Vehicles: Intelligence and Cooperation. *Sensors*, *23*(10), 4643. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s23104643

Bai, J., Zhang, X., Longyun Qi, Liu, W., Zhou, X., Liu, Y., Lv, X., Sun, B., Duan, B., Zhang, S., & Che, X. (2023). Survey on Application of Trusted Computing in Industrial Control Systems. *Electronics*, *12*(19), 4182. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics12194182

Bakir, V. (2017). Political-intelligence elites, Strategic Political Communication and the press: The need for, and utility of, a benchmark of public accountability demands. *Intelligence and National Security*, *32*(1), 85–106. https://doi.org/10.1080/02684527.2016.1231866

Barbeau, M., & Garcia-Alfaro, J. (2022). Cyber-physical defense in the quantum Era. *Scientific Reports (Nature Publisher Group)*, *12*(1). ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1038/s41598-022-05690-1

Barzashka, I. (2023). Seeking Strategic Advantage: The Potential of Combining Artificial Intelligence and Human-centred Wargaming. *The RUSI Journal*, *0*(0), 1–7. https://doi.org/10.1080/03071847.2023.2282862

Basrur, R., & Wu, S.-S. (2023). India's conventional strategy in a nuclear environment: A neglected link. *Defence Studies*, *23*(3), 457–476. https://doi.org/10.1080/14702436.2023.2211013

Bavle, H., Sanchez-Lopez, J. L., Cimarelli, C., Tourani, A., & Voos, H. (2023). From SLAM to Situational Awareness: Challenges and Survey. *Sensors*,

23(10), 4849. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s23104849

Beaver, I. (2022). Is AI at human parity yet? A case study on speech recognition. *The AI Magazine*, *43*(4), 386. https://doi.org/10.1002/aaai.12071

Benhamou, M. (2023). Next for Europe: Defining its own battlefield tactics. *European View*, *22*(2), 166–175. https://doi.org/10.1177/17816858231205729

Bermejo-Berros, J., & Gil Martínez, M. A. (2021). The relationships between the exploration of virtual space, its presence and entertainment in virtual reality, 360º and 2D. *Virtual Reality*, *25*(4), 1043–1059. https://doi.org/10.1007/s10055-021-00510-9

Bhatt, D., Patel, C., Talsania, H., Patel, J., Vaghela, R., Pandya, S., Modi, K., & Ghayvat, H. (2021). CNN Variants for Computer Vision: History, Architecture, Application, Challenges and Future Scope. *Electronics*, *10*(20), Article 20. https://doi.org/10.3390/electronics10202470

Bitzinger, R. A. (2022). The 4th Industrial Revolution, Military-Civil Fusion, and the Next RMA. *Insight Turkey*, *24*(3), 11–22. ProQuest Central; Social Science Premium Collection. https://doi.org/10.25253/99.2022243.2

Blanchard, A., & Taddeo, M. (2022). Jus in bello Necessity, The Requirement of Minimal Force, and Autonomous Weapons Systems. *Journal of Military Ethics*, *21*(3–4), 286–303. https://doi.org/10.1080/15027570.2022.2157952

Blank, L. R. (2010). *Defining the Battlefield in Contemporary Conflict and Counterterrorism: Understanding the Parameters of the Zone of Combat* (SSRN Scholarly Paper 1677965). https://papers.ssrn.com/abstract=1677965

Blöcher, K., & Alt, R. (2021). AI and robotics in the European restaurant sector: Assessing potentials for process innovation in a high-contact service industry. *Electronic Markets*, *31*(3), 529–551. https://doi.org/10.1007/s12525-020-00443-2

Bode, I., Huelss, H., Nadibaidze, A., Qiao-Franco, G., & Watts, T. F. A. (2023). Prospects for the global governance of autonomous weapons: Comparing Chinese, Russian, and US practices. *Ethics and Information Technology*, *25*(1), 5. https://doi.org/10.1007/s10676-023-09678-x

Bode, I., Huelss, H., Nadibaidze, A., Qiao-Franco, G., & Watts, T. F. A. (2024). Algorithmic Warfare: Taking Stock of a Research Programme. *Global Society*, *38*(1), 1–23. https://doi.org/10.1080/13600826.2023.2263473

Boice, E. N., Hernandez Torres, S. I., Knowlton, Z. J., Berard, D., Gonzalez, J. M., Guy, A., & Snider, E. J. (2022). Training Ultrasound Image Classification Deep-Learning Algorithms for Pneumothorax Detection Using a Synthetic Tissue Phantom Apparatus. *Journal of Imaging*, *8*(9), 249. Coronavirus Research Database; ProQuest Central; Publicly Available Content

Database; SciTech Premium Collection. https://doi.org/10.3390/jimaging8090249

Boodhoo, N. (2024, April 4). *Regulating autonomous weapons: A treaty to regulate AI in war*. Axios. https://www.axios.com/2024/04/04/ai-weapons-war-autonomous-regulation-ban

Borda, A., Molnar, A., Neesham, C., & Kostkova, P. (2022). Ethical Issues in AI-Enabled Disease Surveillance: Perspectives from Global Health. *Applied Sciences*, *12*(8), 3890. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/app12083890

Botezatu, U.-E., PhD. (2023). AI-Centric secure outer space operations. *Bulletin of "Carol I" National Defense University*, *12*(3), 205–221. ProQuest Central; Publicly Available Content Database; Social Science Premium Collection.

Boutin, B. (2023). State responsibility in relation to military applications of artificial intelligence. *Leiden Journal of International Law*, *36*(1), 133–150. ProQuest Central; Social Science Premium Collection. https://doi.org/10.1017/S0922156522000607

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford university press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brown, A. (2023). Ethics, autonomy, and killer drones: Can machines do right? *Comparative Strategy*, *42*(6), 731–746. https://doi.org/10.1080/01495933.2023.2263333

Brown, P. (2024). Education, opportunity and the future of work in the fourth industrial revolution. *British Journal of Sociology of Education*, *0*(0), 1–19. https://doi.org/10.1080/01425692.2023.2299970

Bukkapatnam, S. T. S. (2023). Autonomous materials discovery and manufacturing (AMDM): A review and perspectives. *IISE Transactions*, *55*(1), 75–93. https://doi.org/10.1080/24725854.2022.2089785

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, *31*(3), 415–434. https://doi.org/10.1080/09662839.2022.2101885

Caldwell, A., & Fidock, J. (2018, April 26). *Mastering the battlefields of the 21st century*. https://www.dst.defence.gov.au/podcast/mastering-battlefields-21st-century

Calimeri, F., Cauteruccio, F., Cinelli, L., Marzullo, A., Stamile, C., Terracina, G., Durand-Dubief, F., & Sappey-Marinier, D. (2021). A Logic-Based Framework Leveraging Neural Networks for Studying the Evolution of

Neurological Disorders. *Theory and Practice of Logic Programming*, *21*(1), 80–124. https://doi.org/10.1017/S1471068419000449

Cancela, E., & Goikoetxea, J. (2023). Spanish Fake Sovereignty: From Privatising the Nation-State to Becoming a Digital Colony. *Ethnopolitics*, *0*(0), 1–21. https://doi.org/10.1080/17449057.2023.2275882

Cartwright, B., Frank, R., Weir, G., & Padda, K. (2022). Detecting and responding to hostile disinformation activities on social media using machine learning and deep neural networks. *Neural Computing & Applications*, *34*(18), 15141–15163. ProQuest Central; SciTech Premium Collection. https://doi.org/10.1007/s00521-022-07296-0

Caverley, J. D. (2023). Horses, nails, and messages: Three defense industries of the Ukraine war. *Contemporary Security Policy*, *44*(4), 606–623. https://doi.org/10.1080/13523260.2023.2257965

Cebrowski, A. K. (2000). Military responses to the information age. *RUSI Journal: Royal United Services Institute for Defense Studies*, *145*(5), 25–29.

Chakravarty, M. (2023). Hidden Circuitry of the Present and Future. *Globsyn Management Journal*, *17*(1/2), 125–126. ProQuest Central.

Chappuis, I. (2023). Towards 2030: Future-proofing human capital management. *Strategic HR Review*, *22*(2), 42–46. ProQuest Central. https://doi.org/10.1108/SHR-01-2023-0004

Chatterjee, S. (2019). Impact of AI regulation on intention to use robots: From citizens and government perspective. *International Journal of Intelligent Unmanned Systems*, *8*(2), 97–114. https://doi.org/10.1108/IJIUS-09-2019-0051

Chattopadhyay, S. (2023). DRDO showcases over 330 technologies and systems. *Vayu Aerospace and Defence Review*, *2*, 72–73. ProQuest Central; SciTech Premium Collection.

Chedrawi, C., & Atallah, Y. (2022). Artificial intelligence in the defense sector: An RBV and isomorphism perspectives to the case of the Lebanese Armed Forces. *Journal of Asia Business Studies*, *16*(2), 279–293. ProQuest Central. https://doi.org/10.1108/JABS-09-2020-0377

Chen, H., Zhao, H., Qi, B., Wang, S., Shen, N., & Li, Y. (2020). Human motion recognition based on limit learning machine. *International Journal of Advanced Robotic Systems*, *17*(5), 1729881420933077. https://doi.org/10.1177/1729881420933077

Chintamani, K., Overgaard, T., Tan, C. A., Ellis, R. D., & Pandya, A. (2008). Physically-based Augmented Reality for Remote Robot Tele-operation: Applications in Training and Simulation. *IIE Annual Conference. Proceedings*, 977–982.

Choi, Y.-J. (2022). SECURITY THREAT SCENARIOS OF DRONES AND ANTI-DRONE TECHNOLOGY. *Academy of Strategic Management Journal*, *21*(1), 1–7. ProQuest Central.

Chuprov, S., Belyaev, P., Gataullin, R., Reznik, L., Neverov, E., & Viksnin, I. (2023). Robust Autonomous Vehicle Computer-Vision-Based Localization in Challenging Environmental Conditions. *Applied Sciences*, *13*(9), Article 9. https://doi.org/10.3390/app13095735

Clouse, D. C. (2023, December 5). *War Has Changed, and the Army's Conceptualization of Operational Art Must Follow Suit*. Modern War Institute. https://mwi.westpoint.edu/war-has-changed-and-the-armys-conceptualization-of-operational-art-must-follow-suit/

Cohen, R., Chandler, N., Efron, S., Frederick, B., Han, E., Klein, K., Morgan, F., Rhoades, A., Shatz, H., & Shokh, Y. (2020). *The Future of Warfare in 2030: Project Overview and Conclusions*. RAND Corporation. https://doi.org/10.7249/RR2849.1

Covaciu, F., & Iordan, A.-E. (2022). Control of a Drone in Virtual Reality Using MEMS Sensor Technology and Machine Learning. *Micromachines*, *13*(4), 521. https://doi.org/10.3390/mi13040521

Cuhadar, C., & Tsao, H. N. (2022). A Computer Vision Sensor for AI-Accelerated Detection and Tracking of Occluded Objects. *Advanced Intelligent Systems*, *4*(11), 2100285-n/a. https://doi.org/10.1002/aisy.202100285

Dang, W., Guo, J., Liu, M., Liu, S., Yang, B., Yin, L., & Zheng, W. (2022). A Semi-Supervised Extreme Learning Machine Algorithm Based on the New Weighted Kernel for Machine Smell. *Applied Sciences*, *12*(18), 9213-. https://doi.org/10.3390/app12189213

Data, Analytics, and Artificial Intelligence Adoption Strategy. (2023). U.S. Department of Defence.

Davis, S. I. (2022). Artificial intelligence at the operational level of war. *Defense & Security Analysis*, *38*(1), 74–90. https://doi.org/10.1080/14751798.2022.2031692

Davy Preuveneers, & Joosen, W. (2024). An Ontology-Based Cybersecurity Framework for AI-Enabled Systems and Applications. *Future Internet*, *16*(3), 69. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/fi16030069

de Klerk, W., & Pretorius, J. (2019). Guideline for conducting critical reviews in psychology research. *Journal of Psychology in Africa*, *29*(6), 645–649. https://doi.org/10.1080/14330237.2019.1691793

Demertzis, K., Taketzis, D., Demertzi, V., & Skianis, C. (2022). An Ensemble Transfer Learning Spiking Immune System for Adaptive Smart Grid

Protection. *Energies*, *15*(12), 4398. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/en15124398

Devarakonda, A., Sharma, N., Saha, P., & Ramya, S. (2022). Network intrusion detection: A comparative study of four classifiers using the NSL-KDD and KDD'99 datasets. *Journal of Physics: Conference Series*, *2161*(1), 012043. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1088/1742-6596/2161/1/012043

Dieguez Porras, P. (2024). Sustaining regional Nuclear Human Capacity Building in Europe. *Nuclear Engineering and Design*, *419*, 112916-. https://doi.org/10.1016/j.nucengdes.2024.112916

Dmytryshyn, L. I., & Romanchukevych, M. Y. (2022). LABOR MARKET IN UKRAINE: CURRENT SITUATION AND DEVELOPMENT PROSPECT. *Problemy Ekonomiky*, *2*, 39–46. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database. https://doi.org/10.32983/2222-0712-2022-2-39-46

Docalysis – Frequently Asked Questions. (n.d.). Retrieved April 23, 2024, from https://docalysis.com/faq

Duan, C., Yin, J., & Wang, Z. (2022). Design and Implementation of a Damage Assessment System for Large-Scale Surface Warships Based on Deep Learning. *Mathematical Problems in Engineering*, *2022*. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1155/2022/1462508

Duggan, W. (2024, April 24). *Artificial Intelligence Stocks: The 10 Best AI Companies*. US News & World Report. https://money.usnews.com/investing/articles/artificial-intelligence-stocks-the-10-best-ai-companies

Eikmeier, D. C. (2019). Simplicity: A Tool for Working with Complexity and Chaos. *Joint Force Quarterly : JFQ*, *92*, 30–35.

Eilstrup-Sangiovanni, M. (2018). Why the World Needs an International Cyberwar Convention. *Philosophy & Technology*, *31*(3), 379–407. https://doi.org/10.1007/s13347-017-0271-5

Elyoseph, Z., Refoua, E., Asraf, K., Lvovsky, M., Shimoni, Y., & Hadar-Shoval, D. (2024). Capacity of Generative AI to Interpret Human Emotions From Visual and Textual Data: Pilot Evaluation Study. *JMIR Mental Health*, *11*(1), e54369. https://doi.org/10.2196/54369

Esteva, A., Chou, K., Yeung, S., Naik, N., Madani, A., Mottaghi, A., Liu, Y., Topol, E., Dean, J., & Socher, R. (2021). Deep learning-enabled medical computer vision. *NPJ Digital Medicine*, *4*(1), 5–5. https://doi.org/10.1038/s41746-020-00376-2

Fact Sheet No. 32: Terrorism and Counter-Terrorism. (2008, July 1). OHCHR. https://www.ohchr.org/en/publications/fact-sheets/fact-sheet-no-32-terrorism-and-counter-terrorism

Fahim Sufi. (2023). A New Social Media-Driven Cyber Threat Intelligence. *Electronics*, *12*(5), 1242. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics12051242

Fang, A., & Li, R. (2022). Penetration Multilayer Overload Signal Generation Based on TransGAN. *Journal of Physics: Conference Series*, *2224*(1), 012022. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1088/1742-6596/2224/1/012022

Fazekas, F. (2022). Application of Artificial Intelligence in Military Operations Planning 1. *Academic and Applied Research in Military and Public Management Science*, *21*(2), 41–54. ProQuest Central. https://doi.org/10.32565/aarms.2022.2.3

Figueroa, M. D., Orozco, A. H., Martínez, J., & Jaime, W. M. (2023). The risks of autonomous weapons: An analysis centred on the rights of persons with disabilities. *International Review of the Red Cross*, *105*(922), 278–305. https://doi.org/10.1017/S1816383122000881

Filgueiras, F. (2022). The politics of AI: Democracy and authoritarianism in developing countries. *Journal of Information Technology & Politics*, *19*(4), 449–464. https://doi.org/10.1080/19331681.2021.2016543

FM 3–0, Operations. (2001). U.S. Department of the Army.

FM 3-12 Cyberspace Operations and Electromagnetic Warfare. (2021). U.S. Department of the Army.

Fox, A. C. (2023, December 4). *Myths and Principles in the Challenges of Future War*. AUSA. https://www.ausa.org/publications/myths-and-principles-challenges-future-war

Freedman, L. (2013). *Strategy: A History*. Oxford University Press.

Gady, F.-S. (2023). War, Conflict and the Military. *Survival*, *65*(4), 179–187. https://doi.org/10.1080/00396338.2023.2239070

Ganguli, C., Shandilya, S. K., Nehrey, M., & Havryliuk, M. (2023). Adaptive Artificial Bee Colony Algorithm for Nature-Inspired Cyber Defense. *Systems*, *11*(1), 27. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/systems11010027

Gao, X., Wang, Z., Feng, Y., Ma, L., Chen, Z., & Xu, B. (2023). Benchmarking Robustness of AI-Enabled Multi-sensor Fusion Systems: Challenges and Opportunities. *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, 871–882. https://doi.org/10.1145/3611643.3616278

Garbuio, M., & Lin, N. (2021). Innovative idea generation in problem finding: Abductive reasoning, cognitive impediments, and the promise of artificial intelligence. *Journal of Product Innovation Management*, *38*(6), 701–725. https://doi.org/10.1111/jpim.12602

Garg, R. & Jayanthiladevi. (2023). Preventing Cyber Attacks using Artificial Intelligence. *I-Manager's Journal on Software Engineering*, *18*(2), 1–9. ProQuest Central; SciTech Premium Collection. https://doi.org/10.26634/jse.18.2.20367

Gawde, S., Patil, S., Kumar, S., Kamat, P., & Kotecha, K. (2024). An explainable predictive maintenance strategy for multi-fault diagnosis of rotating machines using multi-sensor data fusion. *Decision Analytics Journal*, *10*, 100425. https://doi.org/10.1016/j.dajour.2024.100425

Gervais, D. J. (2023). Towards an effective transnational regulation of AI. *AI & SOCIETY*, *38*(1), 391–410. https://doi.org/10.1007/s00146-021-01310-0

Gibbs, S. (2015, July 27). Musk, Wozniak and Hawking urge ban on warfare AI and autonomous weapons. *The Guardian*. https://www.theguardian.com/technology/2015/jul/27/musk-wozniak-hawking-ban-ai-autonomous-weapons

Giordano, P. (2023, October 16). Empowering NATO's Multi-Domain Operations Through Digital Transformation. *NATO's ACT*. https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/

glass.ai. (2023, October 12). Mapping the AI sector in China. *Medium*. https://glassai.medium.com/mapping-the-ai-sector-in-china-it-is-much-smaller-than-the-us-and-similar-in-size-to-the-uk-3559f785cbee

Global Trends. (2021). Office of the Director of National Intelligence. https://www.dni.gov/index.php/gt2040-home

Gompert, D. C., & Libicki, M. (2023). Detect and Engage: A New American Way of War. *Survival*, *65*(5), 65–74. https://doi.org/10.1080/00396338.2023.2261246

Gonzalez, C., Admoni, H., Brown, S., & Willams Woolley, A. (2023). COHUMAIN: Building the Socio-Cognitive Architecture of Collective Human-Machine Intelligence. *Topics in Cognitive Science*. https://doi.org/10.1111/tops.12673

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, *26*(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Guy, A., Hernandez Torres, S. I., Knowlton, Z. J., Bedolla, C., Salinas, J., & Snider, E. J. (2024). Toward Smart, Automated Junctional Tourniquets—AI Models to Interpret Vessel Occlusion at Physiological Pressure Points. *Bioengineering*, *11*(2), 109. Coronavirus Research Database; ProQuest

Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/bioengineering11020109

Haefner, N., Wincent, J., Parida, V., & Gassmann, O. (2021). Artificial intelligence and innovation management: A review, framework, and research agenda☆. *Technological Forecasting and Social Change*, *162*, 120392. https://doi.org/10.1016/j.techfore.2020.120392

Hagendorff, T., & Fabi, S. (2023). Why we need biased AI: How including cognitive biases can enhance AI systems. *Journal of Experimental & Theoretical Artificial Intelligence*, *0*(0), 1–14. https://doi.org/10.1080/0952813X.2023.2178517

Hagos, D. H., & Rawat, D. B. (2022). Recent Advances in Artificial Intelligence and Tactical Autonomy: Current Status, Challenges, and Perspectives. *Sensors*, *22*(24), 9916. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s22249916

Haigh, K. Z., Wong, A., & Chen, Y. (2023). Introduction to the special issue on Innovative Applications of Artificial Intelligence (IAAI 2023). *AI Magazine*, *44*(4), 352–353. https://doi.org/10.1002/aaai.12132

Halkis, M., Dohamid, A. G., & Sutanto, R. (2022). Deontology of Lethal Autonomous Weapon Systems in The Total People's Defense and Security System. *NeuroQuantology*, *20*(15), 4854–4866. ProQuest Central; SciTech Premium Collection. https://doi.org/10.14704/NQ.2022.20.15.NQ88491

Han, H. R. (2023). Hybrid Fiber Materials according to the Manufacturing Technology Methods and IOT Materials: A Systematic Review. *Materials*, *16*(4), 1351. https://doi.org/10.3390/ma16041351

Han, Y., Li, G., & Chen, T. (2022). Design of intelligent surveillance system based on wireless ad-hoc network under special conditions. *Journal of Ambient Intelligence and Humanized Computing*, *13*(7), 3655–3667. ProQuest Central; SciTech Premium Collection. https://doi.org/10.1007/s12652-020-02140-6

Hannon, B., Kumar, Y., Dejaun Gayle, Li, J. J., & Morreale, P. (2024). Robust Testing of AI Language Model Resiliency with Novel Adversarial Prompts. *Electronics*, *13*(5), 842. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics13050842

Hasanujjaman, M., Chowdhury, M. Z., & Jang, Y. M. (2023). Sensor Fusion in Autonomous Vehicle with Traffic Surveillance Camera System: Detection, Localization, and AI Networking. *Sensors*, *23*(6), Article 6. https://doi.org/10.3390/s23063335

Hashimov, E., Sabziyev, E., & Huseynov, B. (2023). TARGETING A ROCKET AT A MOVING OBJECT USING UNMANNED AERIAL VEHICALS (UAVs). *Journal of Defense Resources Management*, *14*(2), 117–124. ProQuest

Central; Publicly Available Content Database; SciTech Premium Collection.

Hickman, P. L. (2020, May 12). *The Future of Warfare Will Continue to Be Human*. War on the Rocks. https://warontherocks.com/2020/05/the-future-of-warfare-will-continue-to-be-human/

Hillson, R. (2009). *The DIME/PMESII Model Suite Requirements Project*. https://www.semanticscholar.org/paper/The-DIME-PMESII-Model-Suite-Requirements-Project-Hillson/4cb817c6bcd3c7229fbd1a2411b25437576570df

Hinton, P. (2023). Put Latent Data to Work: Using Technology to Improve Personnel Management in Military Forces. *The RUSI Journal*, *168*(1–2), 20–29. https://doi.org/10.1080/03071847.2023.2213063

Hoey, J., Schröder, T., & Alhothali, A. (2016). Affect control processes: Intelligent affective interaction using a partially observable Markov decision process. *Artificial Intelligence*, *230*, 134–172. https://doi.org/10.1016/j.artint.2015.09.004

Hoppes, C. W., Lambert, K. H., Whitney, S. L., Erbele, I. D., Esquivel, C. R., & Yuan, T. T. (2024). Leveraging Technology for Vestibular Assessment and Rehabilitation in the Operational Environment: A Scoping Review. *Bioengineering*, *11*(2), 117. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/bioengineering11020117

Horowitz, M. C., Contributed equally to this work with: Michael C. Horowitz, Kahn, L., Macdonald, J., Schneider, J., Jacquelyn Schneider Julia Macdonald, & Jacquelyn Schneider Jacquelyn Schneider Contributed equally to this work with: Michael C. Horowitz. (2022). COVID-19 and public support for autonomous technologies—Did the pandemic catalyze a world of robots? *PLoS One*, *17*(9). Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1371/journal.pone.0273941

Horvat, M., Krtalić, A., Akagić, A., & Mekterović, I. (2024). Ontology-Based Data Observatory for Formal Knowledge Representation of UXO Using Advanced Semantic Web Technologies. *Electronics*, *13*(5), 814. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics13050814

Huang, Z., Shen, Y., Li, J., Fey, M., & Brecher, C. (2021). A Survey on AI-Driven Digital Twins in Industry 4.0: Smart Manufacturing and Advanced Robotics. *Sensors*, *21*(19), Article 19. https://doi.org/10.3390/s21196340

Hunter, L. Y., Albert, C. D., Henningan, C., & Rutland, J. (2023). The military application of artificial intelligence technology in the United States, China, and Russia and the implications for global security. *Defense & Security Analysis*, *39*(2), 207–232. https://doi.org/10.1080/14751798.2023.2210367

Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial intelligence and information warfare in major power states: How the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. *Defense & Security Analysis*, *0*(0), 1–35. https://doi.org/10.1080/14751798.2024.2321736

Hunter, L. Y., Albert, C., Rutland, J., & Hennigan, C. (2023). The Fourth Industrial Revolution, Artificial Intelligence, and Domestic Conflict. *Global Society*, *37*(3), 375–396. https://doi.org/10.1080/13600826.2022.2147812

Hussain, S., Ahmed, S., Thasin, A., & Saad, R. M. A. (2022). AI-Enabled Ant-Routing Protocol to Secure Communication in Flying Networks. *Applied Computational Intelligence and Soft Computing*, *2022*. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1155/2022/3330168

Ioniță, C.-C. (2020a). Adapting Mosaic Warfare Specific Capabilities to the New Technological Developments. *Strategic Impact*, *76*, 22–34.

Ioniță, C.-C. (2020b). The "Mosaic" Warfare: A New American Strategy for the Future. *Strategic Impact*, *75*, 25–42.

Jameel, T., & Saud, A. (2022). Policies of Artificial Intelligence in the EU: Learning Curve from the UK and China? *Journal of European Studies*, *38*(2), 1.

Jecker, N. S., & Ko, A. (2022). The Unique and Practical Advantages of Applying A Capability Approach to Brain Computer Interface. *Philosophy & Technology*, *35*(4), 101. ProQuest Central; SciTech Premium Collection; Social Science Premium Collection. https://doi.org/10.1007/s13347-022-00597-1

Jekateryńczuk, G., & Piotrowski, Z. (2024). A Survey of Sound Source Localization and Detection Methods and Their Applications. *Sensors*, *24*(1), 68. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s24010068

Jenkins, P. R., Robbins, M. J., & Lunday, B. J. (2023). Optimising aerial military medical evacuation dispatching decisions via operations research techniques. *BMJ Military Health*, *169*(e1), e90–e92. ProQuest Central. https://doi.org/10.1136/bmjmilitary-2020-001631

Jesson, J., & Lacey, F. (2006). How to do (or not to do) a critical literature review. *Pharmacy Education*, *6*(2), Article 2. https://pharmacyeducation.fip.org/pharmacyeducation/article/view/103

Jiang, N., Liu, X., Liu, H., Lim, E. T. K., Tan, C.-W., & Gu, J. (2022). Beyond AI-powered context-aware services: The role of human–AI collaboration. *Industrial Management & Data Systems*, *123*(11), 2771–2802. https://doi.org/10.1108/IMDS-03-2022-0152

Jiang, X., Fan, J., Zhu, Z., Wang, Z., Guo, Y., Liu, X., Jia, F., & Dai, C. (2023). Cybersecurity in neural interfaces: Survey and future trends. *Computers in Biology and Medicine*, *167*. ProQuest Central; SciTech Premium Collection. https://doi.org/10.1016/j.compbiomed.2023.107604

Jiao, J., Zhao, L., Pan, W., & Li, X. (2023). Development and Core Technologies for Intelligent SWaP3 Infrared Cameras: A Comprehensive Review and Analysis. *Sensors*, *23*(9), 4189. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s23094189

Johnson, J. (2019). Artificial intelligence & future warfare: Implications for international security. *Defense & Security Analysis*, *35*(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800

Johnson, J. (2020a). Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare. *The RUSI Journal*, *165*(2), 26–36. https://doi.org/10.1080/03071847.2020.1752026

Johnson, J. (2020b). Deterrence in the age of artificial intelligence & autonomy: A paradigm shift in nuclear deterrence theory and practice? *Defense & Security Analysis*, *36*(4), 422–448. https://doi.org/10.1080/14751798.2020.1857911

Johnson, J. (2021). "Catalytic nuclear war" in the age of artificial intelligence & autonomy: Emerging military technology and escalation risk between nuclear-armed states. *Journal of Strategic Studies*, *ahead-of-print*(ahead-of-print), 1–41. https://doi.org/10.1080/01402390.2020.1867541

Johnson, J. (2022a). Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age. *European Journal of International Security*, *7*(3), 337–359. ProQuest Central; Social Science Premium Collection. https://doi.org/10.1017/eis.2021.23

Johnson, J. (2022b). The AI Commander Problem: Ethical, Political, and Psychological Dilemmas of Human-Machine Interactions in AI-enabled Warfare. *Journal of Military Ethics*, *21*(3–4), 246–271. https://doi.org/10.1080/15027570.2023.2175887

Johnson, J. (2024). Finding AI Faces in the Moon and Armies in the Clouds: Anthropomorphising Artificial Intelligence in Military Human-Machine Interactions. *Global Society*, *38*(1), 67–82. https://doi.org/10.1080/13600826.2023.2205444

Johnson, T., Kanjo, E., & Woodward, K. (2023). DigitalExposome: Quantifying impact of urban environment on wellbeing using sensor fusion and deep learning. *Computational Urban Science*, *3*(1), 14. https://doi.org/10.1007/s43762-023-00088-9

Joint Doctrine Note 1-18: Strategy. (2018). U.S. Joint Chiefs of Staff.

Jones, A., Koehler, S., Jerge, M., Graves, M., Bayley King, Dalrymple, R., Freese, C., & James Von Albade. (2023). BATMAN: A Brain-like Approach for

Tracking Maritime Activity and Nuance. *Sensors*, *23*(5), 2424. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s23052424

Jones, L. (2022). The Future of Warfare is Irregular. *The Fletcher Forum of World Affairs*, *46*(2), 1–11. ProQuest Central; Social Science Premium Collection.

Kaku, M. (2023). *Quantum supremacy: How the quantum computer revolution will change everything* (First edition). Doubleday.

Kanade, V. (2022, February 25). Narrow AI vs. General AI vs. Super AI. *Spiceworks*. https://www.spiceworks.com/tech/artificial-intelligence/articles/narrow-general-super-ai-difference/

Kangasniemi, M., Utriainen, K., Ahonen, S.-M., Pietilä, A.-M., Jääskeläinen, P., & Liikanen, E. (2013). Kuvaileva kirjallisuuskatsaus: Eteneminen tutkimuskysymyksestä jäsennettyyn tietoon. *Hoitotiede*, *25*(4), Article 4.

Kanniainen, V. (2023). *Strategic and tactical nuclear weapons in politics and warfare*. https://www.doria.fi/handle/10024/187821

Kassens-Noor, E., Darcy, K., Cojocaru, A. I., Rzepecki, R., Jang, S., Jiang, W., Monzert, T., Cai, M., & Crittenden, M. (2022). Proposing the foundations of scAInce by exploring the future of artificially intelligent, sustainable, and resilient megaprojects. *Journal of Mega Infrastructure & Sustainable Development*, *2*(sup1), 5–20. https://doi.org/10.1080/24724718.2022.2131098

Katagiri, N. (2024). Artificial Intelligence and Cross-Domain Warfare: Balance of Power and Unintended Escalation. *Global Society*, *38*(1), 34–48. https://doi.org/10.1080/13600826.2023.2248179

Kaushik, S., & Sarath, G. (2022). A Privacy Preserving Approach for Mitigating Data Poisoning Attack in Federated Learning. *NeuroQuantology*, *20*(10), 8272–8281. ProQuest Central; SciTech Premium Collection. https://doi.org/10.14704/nq.2022.20.10.NQ55812

Keerthinathan, P., Amarasingam, N., Hamilton, G., & Gonzalez, F. (2023). Exploring unmanned aerial systems operations in wildfire management: Data types, processing algorithms and navigation. *International Journal of Remote Sensing*, *44*(18), 5628–5685. https://doi.org/10.1080/01431161.2023.2249604

Khader, J. (2022). Welcome to the Metaverse: Social Media, the Phantasmatic Big Other, and the Anxiety of the Prosthetic Gods. *Rethinking Marxism*, *34*(3), 397–405. https://doi.org/10.1080/08935696.2022.2111957

Khan, F., R Lakshmana Kumar, Mustufa Haider Abidi, Kadry, S., Alkhalefah, H., & Aboudaif, M. K. (2022). Federated Split Learning Model for Industry 5.0: A Data Poisoning Defense for Edge Computing. *Electronics*, *11*(15), 2393. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics11152393

Kibbee, M. (2023, December 19). *LibGuides: A Guide to Evidence Synthesis*. https://guides.library.cornell.edu/evidence-synthesis

Kiener, M. (2022). Can we Bridge AI's responsibility gap at Will? *Ethical Theory and Moral Practice*, *25*(4), 575–593. ProQuest Central; Social Science Premium Collection. https://doi.org/10.1007/s10677-022-10313-9

Kieslich, K., Keller, B., & Starke, C. (2022). Artificial intelligence ethics by design. Evaluating public perception on the importance of ethical design principles of artificial intelligence. *Big Data & Society*, *9*(1), 20539517221092956. https://doi.org/10.1177/20539517221092956

Kim, M., & Joo, S. (2022). Time-Constrained Adversarial Defense in IoT Edge Devices through Kernel Tensor Decomposition and Multi-DNN Scheduling. *Sensors*, *22*(15), 5896. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s22155896

Kissinger, H., Schmidt, E., & Huttenlocher, D. P. (2021). *The age of AI: And our human future* (First edition). Little, Brown and Company.

Kosola, J., & Solante, T. (2013). *Digitaalinen taistelukenttä: Informaatioajan sotakoneen tekniikka* [D5 Oppikirja, ammatillinen käsi- tai opaskirja taikka sanakirja]. Maanpuolustuskorkeakoulu. https://www.doria.fi/handle/10024/94298

Kovács, L. (2002). *Battlefield of the future*. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/13051/Kovcs%20Laszlo_Battlefield%20of%20the%20future.pdf?sequence=1

Krichen, M. (2023). Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence. *Computers*, *12*(5), 107. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/computers12050107

Kumar, A., Verma, R., Choudhary, N. K., & Singh, N. (2023). "Optimal placement and sizing of distributed generation in power distribution system: A comprehensive review." *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, *45*(3), 7160–7185. https://doi.org/10.1080/15567036.2023.2216167

Latiff, R. H. (2017). *Future war: Preparing for the new global battlefield*. Alfred A. Knopf.

Lee, K. (2021). *AI superpowers: China, Silicon Valley, and the new world order*. Houghton Mifflin Harcourt.

Lee, K.-F., & Chen, Q. (2021). *AI 2041* (First edition). Currency.

Lee, Y., & Kim, J. (2023). Robustness of Deep Learning Models for Vision Tasks. *Applied Sciences*, *13*(7), 4422. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/app13074422

Leroy, I., & Zolotaryova, I. (2023). CRITICAL INFRASTRUCTURE DEFENSE: PERSPECTIVES FROM THE EU AND USA CYBER EXPERTS. *Natsional'nyi Hirnychyi Universytet. Naukovyi Visnyk*, *5*, 165–170. ProQuest Central; SciTech Premium Collection. https://doi.org/10.33271/nvngu/2023-5/165

Leung, C. K., Braun, P., & Cuzzocrea, A. (2019). AI-Based Sensor Information Fusion for Supporting Deep Supervised Learning. *Sensors (Basel, Switzerland)*, *19*(6), 1345-. https://doi.org/10.3390/s19061345

Li, H., Guo, Y., Huo, S., Hu, H., & Sun, P. (2022). Defensive deception framework against reconnaissance attacks in the cloud with deep reinforcement learning. *Science China. Information Sciences*, *65*(7), 170305. https://doi.org/10.1007/s11432-021-3462-4

Lin, H. (2020, March 27). *Doctrinal Confusion and Cultural Dysfunction in the Pentagon Over Information and Cyber Operations*. Default. https://www.lawfaremedia.org/article/doctrinal-confusion-and-cultural-dysfunction-pentagon-over-information-and-cyber-operations

Liu, Y., & Guo, Y. (2022). Towards Real-Time Warning and Defense Strategy AI Planning for Cyber Security Systems Aided by Security Ontology. *Electronics*, *11*(24), 4128. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics11244128

Livieratos, C. (2022, June 14). *From Complicated to Complex: The Changing Context of War*. Modern War Institute. https://mwi.westpoint.edu/from-complicated-to-complex-the-changing-context-of-war/

Lloyd, D. G., Saxby, D. J., Pizzolato, C., Worsey, M., Diamond, L. E., Palipana, D., Bourne, M., Cardoso de Sousa, A., Malik Muhammad Naeem Mannan, Nasseri, A., Perevoshchikova, N., Maharaj, J., Crossley, C., Quinn, A., Mulholland, K., Collings, T., Xia, Z., Cornish, B., Devaprakash, D., … Barrett, R. S. (2023). Maintaining soldier musculoskeletal health using personalised digital humans, wearables and/or computer vision. *Journal of Science and Medicine in Sport, Suppl. Supplement 1*, *26*, S30–S39. ProQuest Central. https://doi.org/10.1016/j.jsams.2023.04.001

Lochner, M., & Smilek, D. (2023). The uncertain advisor: Trust, accuracy, and self-correction in an automated decision support system. *Cognitive Processing*, *24*(1), 95–106. https://doi.org/10.1007/s10339-022-01113-1

Loh, P. K. K., Lee, A. Z. Y., & Balachandran, V. (2024). Towards a Hybrid Security Framework for Phishing Awareness Education and Defense. *Future Internet*, *16*(3), 86. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/fi16030086

Lonsdale, D. J. (2004). *The nature of war in the information age: Clausewitzian future*. Cass.

Lovelock, J. E. (2019). *Novacene: The coming age of hyperintelligence*. Allen Lane.

Mahmud, A. (2023). Application and Criminalization of the Artificial Intelligence in Business: Recommendation to Counter the Regulatory Challenges. *Journal of Applied Security Research*, *18*(4), 689–699. https://doi.org/10.1080/19361610.2022.2079939

Mai, K. T., Bray, S., Davies, T., & Griffin, L. D. (2023). Warning: Humans cannot reliably detect speech deepfakes. *PLoS One*, *18*(8). ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1371/journal.pone.0285333

Malmio, I. (2023). Ethics as an enabler and a constraint – Narratives on technology development and artificial intelligence in military affairs through the case of Project Maven. *Technology in Society*, *72*, 102193-. https://doi.org/10.1016/j.techsoc.2022.102193

Markatos, N. G., & Mousavi, A. (2023). Manufacturing quality assessment in the industry 4.0 era: A review. *Total Quality Management & Business Excellence*, *34*(13–14), 1655–1681. https://doi.org/10.1080/14783363.2023.2194524

Martin, E. D. (2000). Characteristics of the Future Battlefield and Deployment. In *Strategies to Protect the Health of Deployed U.S. Forces: Assessing Health Risks to Deployed U.S. Forces: Workshop Proceedings*. National Academies Press (US). https://www.ncbi.nlm.nih.gov/books/NBK225065/

Matsuzaka, Y., & Yashiro, R. (2023). AI-Based Computer Vision Techniques and Expert Systems. *AI*, *4*(1), Article 1. https://doi.org/10.3390/ai4010013

Matta, V., Bansal, G., Akakpo, F., Christian, S., Jain, S., Poggemann, D., Rousseau, J., & Ward, E. (2022). Diverse perspectives on bias in AI. *Journal of Information Technology Case and Application Research*, *24*(2), 135–143. https://doi.org/10.1080/15228053.2022.2095776

Mayer, M. (2023). Trusting machine intelligence: Artificial intelligence and human-autonomy teaming in military operations. *Defense & Security Analysis*, *39*(4), 521–538. https://doi.org/10.1080/14751798.2023.2264070

Mazzolai, B., Mondini, A., Dottore, E. D., Margheri, L., Carpi, F., Suzumori, K., Cianchetti, M., Speck, T., Smoukov, S. K., Burgert, I., Keplinger, T., Siqueira, G. D. F., Vanneste, F., Goury, O., Duriez, C., Nanayakkara, T., Vanderborght, B., Brancart, J., Terryn, S., … Lendlein, A. (2022). Roadmap on soft robotics: Multifunctionality, adaptability and growth without borders. *Multifunctional Materials*, *5*(3), 032001. https://doi.org/10.1088/2399-7532/ac4c95

Mbuthia, R. (2017, July 16). *Cyber Warfare versus Information Warfare: Two Very Different Concepts*. https://www.linkedin.com/pulse/cyber-warfare-versus-information-two-very-different-concepts-mbuthia

McCombes, S. (2023, January 2). *How to Write a Literature Review | Guide, Examples, & Templates*. Scribbr. https://www.scribbr.com/dissertation/literature-review/

McFarland, T., & Assaad, Z. (2023). Legal reviews of in situ learning in autonomous weapons. *Ethics and Information Technology*, *25*(1), 9. Art, Design & Architecture Collection; ProQuest Central; SciTech Premium Collection; Social Science Premium Collection. https://doi.org/10.1007/s10676-023-09688-9

Meerveld, H. W., Lindelauf, R. H. A., Postma, E. O., & Postma, M. (2023). The irresponsibility of not using AI in the military. *Ethics and Information Technology*, *25*(1), 14. Art, Design & Architecture Collection; ProQuest Central; SciTech Premium Collection; Social Science Premium Collection. https://doi.org/10.1007/s10676-023-09683-0

Megret, F. (2012). *War and the Vanishing Battlefield* (SSRN Scholarly Paper 1986548). https://papers.ssrn.com/abstract=1986548

Metz, S., & Cuccia, P. (2011, February). *Defining War for the 21st Century*. https://apps.dtic.mil/sti/citations/ADA536539

Militani, D. R., de Moraes, H. P., Rosa, R. L., Wuttisittikulkij, L., Ramírez, M. A., & Rodríguez, D. Z. (2021). Enhanced Routing Algorithm Based on Reinforcement Machine Learning-A Case of VoIP Service. *Sensors (Basel, Switzerland)*, *21*(2), 504-. https://doi.org/10.3390/s21020504

Mishra, S. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. *Applied Sciences*, *13*(10), 5875. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/app13105875

Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, *10*(2), 2272358. https://doi.org/10.1080/23311916.2023.2272358

Moskalenko, V., Kharchenko, V., Moskalenko, A., & Kuzikov, B. (2023). Resilience and Resilient Systems of Artificial Intelligence: Taxonomy, Models and Methods. *Algorithms*, *16*(3), 165. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/a16030165

Mügge, D. (2023). The securitization of the EU's digital tech regulation. *Journal of European Public Policy*, *30*(7), 1431–1446. https://doi.org/10.1080/13501763.2023.2171090

Mun, J. (2022). Optimizing WARFIGHTERS ' INTELLECTUAL CAPABILITY: RETURN ON INVESTMENT OF Military Education AND RESEARCH. *Defense AR Journal*, *29*(3), 192–245. ProQuest Central; SciTech Premium Collection.

Munir, A., Aved, A., & Blasch, E. (2022). Situational Awareness: Techniques, Challenges, and Prospects. *AI*, *3*(1), 55. https://doi.org/10.3390/ai3010005

Münkler, H. (2003, March). *The wars of the 21st century – ICRC*. International Review of the Red Cross; 1. https://www.icrc.org/en/doc/resources/documents/article/other/5lpgqc.htm

Nadibaidze, A., & Miotto, N. (2023). The Impact of AI on Strategic Stability is What States Make of It: Comparing US and Russian Discourses. *Journal for Peace and Nuclear Disarmament*, *6*(1), 47–67. https://doi.org/10.1080/25751654.2023.2205552

Narayanan, D., Nagpal, M., McGuire, J., Schweitzer, S., & De Cremer, D. (2024). Fairness Perceptions of Artificial Intelligence: A Review and Path Forward. *International Journal of Human–Computer Interaction*, *40*(1), 4–23. https://doi.org/10.1080/10447318.2023.2210890

NATO 2022 Strategic Concept. (2022). NATO.

NATO Warfighting Capstone Concept. (2021). NATO's Strategic Warfare Development Command.

Naz, F., Kumar, A., Agrawal, R., Garza-Reyes, J. A., Majumdar, A., & Chokshi, H. (2023). Artificial intelligence as an enabler of quick and effective production repurposing: An exploratory review and future research propositions. *Production Planning & Control*, *0*(0), 1–24. https://doi.org/10.1080/09537287.2023.2248947

Negrello, F., Stuart, H. S., & Catalano, M. G. (2020). Hands in the Real World. *Frontiers in Robotics and AI*, *6*. https://doi.org/10.3389/frobt.2019.00147

Négyesi, I. (2024). POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE IN EU AND UN PEACEKEEPING ACTIVITIES. *Land Forces Academy Review*, *29*(1), 11–19. ProQuest Central; SciTech Premium Collection.

O'Connell, M. E. (2023). Banning Autonomous Weapons: A Legal and Ethical Mandate. *Ethics & International Affairs*, *37*(3), 287–298. https://doi.org/10.1017/S0892679423000357

Oh, S. H., Kim, J., Nah, J. H., & Park, J. (2024). Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity. *Electronics*, *13*(3), 555. https://doi.org/10.3390/electronics13030555

O'Hanlon, M. (2018). *Forecasting change in military technology, 2020-2040*.

Okolie, C. (2023). Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns. *Journal of International Women's Studies*, *25*(2), 1–16. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; Social Science Premium Collection.

Oniani, D., Hilsman, J., Peng, Y., Poropatich, R. K., Pamplin, J. C., Legault, G. L., & Wang, Y. (2023a). Adopting and expanding ethical principles for generative artificial intelligence from military to healthcare. *NPJ Digital Medicine*, *6*(1), 225–225. https://doi.org/10.1038/s41746-023-00965-x

Oniani, D., Hilsman, J., Peng, Y., Poropatich, R. K., Pamplin, J. C., Legault, G. L., & Wang, Y. (2023b). Adopting and expanding ethical principles for generative artificial intelligence from military to healthcare. *NPJ Digital Medicine*, *6*(1), 225. ProQuest Central; Publicly Available Content Database. https://doi.org/10.1038/s41746-023-00965-x

Ortega, P., & Araneda, C. (2024). Prologue for a "Weak": Decolonization and Otherness as Projectual Strategies to Approach the Understanding of a Foggy Imaginary in the Biobío Delta. *Journal of Architectural Education*, *78*(1), 47–65. https://doi.org/10.1080/10464883.2024.2303922

Otto, S., & Mănescu, G. (2023). WILL ARTIFICIAL INTELLIGENCE (AI) REPLACE A HUMAN COMMANDER IN THE ARMY? *Scientific Bulletin - Nicolae Balcescu Land Forces Academy*, *28*(1), 79–87. ProQuest Central; SciTech Premium Collection. https://doi.org/10.2478/bsaft-2023-0009

Ouhami, M., Hafiane, A., Es-Saady, Y., El Hajji, M., & Canals, R. (2021). Computer Vision, IoT and Data Fusion for Crop Disease Detection Using Machine Learning: A Survey and Ongoing Research. *Remote Sensing*, *13*(13), Article 13. https://doi.org/10.3390/rs13132486

Pacholska, M. (2023). Military Artificial Intelligence and the Principle of Distinction: A State Responsibility Perspective. *Israel Law Review*, *56*(1), 3–23. ProQuest Central; Social Science Premium Collection. https://doi.org/10.1017/S0021223722000188

Pai, R. Y., Shetty, A., Shetty, A. D., Bhandary, R., Shetty, J., Nayak, S., Dinesh, T. K., & D'souza, K. J. (2022). Integrating artificial intelligence for knowledge management systems – synergy among people and technology: A systematic review of the evidence. *Economic Research-Ekonomska Istraživanja*, *35*(1), 7043–7065. https://doi.org/10.1080/1331677X.2022.2058976

Panwar, L. G. S. (2017, October 6). Future Wars21st Century Warfare: From "Battlefield" to "Battlespace." *Future Wars*. https://futurewars.rspanwar.net/21st-century-warfare-from-battlefield-to-battlespace/

Panwar, L. G. S. (2022, October 27). Future WarsRegulation of AI-Enabled Military Systems: A Risk Based Approach – Part I. *Future Wars*. https://futurewars.rspanwar.net/regulation-of-ai-enabled-military-systems-a-risk-based-approach-part-i/

Paré, G., & Kitsiou, S. (2017). Chapter 9 Methods for Literature Reviews. In *Handbook of eHealth Evaluation: An Evidence-based Approach [Internet]*.

University of Victoria.
https://www.ncbi.nlm.nih.gov/books/NBK481583/

Patil, H. V., & Rathi, K. G. (2022). Artificial Intelligence in Defence-A Perusal. *NeuroQuantology*, *20*(11), 5397–5414. ProQuest Central; SciTech Premium Collection. https://doi.org/10.14704/nq.2022.20.11.NQ66541

Pavlidis, G. (2024). Unlocking the black box: Analysing the EU artificial intelligence act's framework for explainability in AI. *Law, Innovation and Technology*, *16*(1), 293–308. https://doi.org/10.1080/17579961.2024.2313795

Payne, K. (2018). Artificial Intelligence: A Revolution in Strategic Affairs? *Survival*, *60*(5), 7–32. https://doi.org/10.1080/00396338.2018.1518374

Petranick, M. (2015). *On Isis. The Reality of the 21st Century Battlefield*. https://www.grin.com/document/311551

Petrosyan, M. (2024). The Role of Non-State Actors in Modern Warfare: The Case of Syria and Nagorno-Karabakh. *Journal of Balkan and Near Eastern Studies*, *26*(2), 149–163. https://doi.org/10.1080/19448953.2023.2233364

Pilla, V. M., Dixit, S., Gyaneshwar, A., Chadha, U., Srinivasan, K., & Jung Taek Seo. (2022). Leveraging Computational Intelligence Techniques for Defensive Deception: A Review, Recent Advances, Open Problems and Future Directions. *Sensors*, *22*(6), 2194. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s22062194

Popa, C. (2022). SPECIFIC PROCEDURES TO INCREASE EFFICIENCY OF THE DECISION-MAKING PROCESS IN THE CONTEXT OF THE VARIABLE GEOMETRY CONFLICT. *Bulletin of "Carol I" National Defense University*, *11*(1), 32–44. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; Social Science Premium Collection. https://doi.org/10.53477/2284-9378-22-57

Pouyanfar, S., Sadiq, S., Yan, Y., Tian, H., Tao, Y., Reyes, M. P., Shyu, M.-L., Chen, S.-C., & Iyengar, S. S. (2018). A Survey on Deep Learning: Algorithms, Techniques, and Applications. *ACM Computing Surveys*, *51*(5), 92:1-92:36. https://doi.org/10.1145/3234150

ProQuest. (2024, April 4). https://www-proquest-com.ezproxy.jyu.fi/publicationbrowse/380588702DA54EC6PQ/1?accountid=11774

Pulyala, S. R. (2024). From Detection to Prediction: AI-powered SIEM for Proactive Threat Hunting and Risk Mitigation. *Turkish Journal of Computer and Mathematics Education*, *15*(1), 34–43. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection; Social Science Premium Collection.

Raazia, I., Muhammad Ahtasham Jan Butt, & Rafaqat, I. (2022). Conceptualizing Hybrid Warfare: India's Tactics Confronting Pakistan's Security. *Journal of*

the Research Society of Pakistan, *59*(3), 104. ProQuest Central; Social Science Premium Collection.

Raj, R., & Kos, A. (2022). A Comprehensive Study of Mobile Robot: History, Developments, Applications, and Future Research Perspectives. *Applied Sciences*, *12*(14), 6951. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/app12146951

Rajagopalan, R. P. (2022). *Future Warfare and Technology: Issues and Strategies*. Global Policy.

Ranganeni, V., Ponto, N., & Cakmak, M. (2023). *Evaluating Customization of Remote Tele-operation Interfaces for Assistive Robots* (arXiv:2304.02771). arXiv. https://doi.org/10.48550/arXiv.2304.02771

Rao, T., Chen, M., Ge Mu, & Tang, X. (2022). Infrared-to-Visible Upconversion Devices. *Coatings*, *12*(4), 456. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/coatings12040456

Rehaan, M., Kaur, N., & Kingra, S. (2024). Face manipulated deepfake generation and recognition approaches: A survey. *Smart Science*, *12*(1), 53–73. https://doi.org/10.1080/23080477.2023.2268380

Riesen, E. (2022). The Moral Case for the Development and Use of Autonomous Weapon Systems. *Journal of Military Ethics*, *21*(2), 132–150. https://doi.org/10.1080/15027570.2022.2124022

Rim, H. J. (2023). The US-China Strategic Competition and Emerging Technologies in the Indo-Pacific Region: Strategies for Building, Dominating, and Managing Networks. *Asian Perspective*, *47*(1), 1–25. https://doi.org/10.1353/apr.2023.0000

Rivera, C., Staley, E., & Llorens, A. (2022). Learning multi-agent cooperation. *Frontiers in Neurorobotics*. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3389/fnbot.2022.932671

Robbins, S. (2020). AI and the path to envelopment: Knowledge as a first step towards the responsible regulation and use of AI-powered machines. *AI & SOCIETY*, *35*(2), 391–400. https://doi.org/10.1007/s00146-019-00891-1

Robles Herrera, S., Ceberio, M., & Kreinovich, V. (2022). When is deep learning better and when is shallow learning better: Qualitative analysis. *International Journal of Parallel, Emergent and Distributed Systems*, *37*(5), 589–595. https://doi.org/10.1080/17445760.2022.2070748

Ruiz Sandoval, D. (2013, June 26). From the Battlefield to the Battle-space. *Democrito2000's Weblog*. https://democrito2000.ca/53-2/

Ruppert, L. (2024). Geopolitics of Technological Futures: Warfare Technologies and Future Battlefields in German Security Debates. *Geopolitics*, *29*(2), 581–606. https://doi.org/10.1080/14650045.2023.2174431

Russell, S. (2023). AI weapons: Russia's war in Ukraine shows why the world must enact a ban. *Nature*, *614*(7949), 620–623. https://doi.org/10.1038/d41586-023-00511-5

Russell, S., Abdelzaher, T., & Suri, N. (2019). Multi-Domain Effects and the Internet of Battlefield Things. *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, 724–730. https://doi.org/10.1109/MILCOM47813.2019.9020925

Ryan, M. (2020). In AI We Trust: Ethics, Artificial Intelligence, and Reliability. *Science and Engineering Ethics*, *26*(5), 2749–2767. https://doi.org/10.1007/s11948-020-00228-y

Ryan, M., & Stahl, B. C. (2020). Artificial intelligence ethics guidelines for developers and users: Clarifying their content and normative implications. *Journal of Information, Communication and Ethics in Society*, *19*(1), 61–86. https://doi.org/10.1108/JICES-12-2019-0138

Saenz, M. J., Revilla, E., & Simón, C. (2020). Designing AI Systems With Human-Machine Teams. *MIT Sloan Management Review*, *61*(3), 1–5.

Sagodi, A., Schniertshauer, J., & van Giffen, B. (2022). Engineering AI-Enabled Computer Vision Systems: Lessons From Manufacturing. *IEEE Software*, *39*(6), 51–57. https://doi.org/10.1109/MS.2022.3189904

Saifi, I., Bhat, B. A., Hamdani, S. S., Bhat, U. Y., Lobato-Tapia, C. A., Mir, M. A., Dar, T. U. H., & Ganie, S. A. (2023). Artificial intelligence and cheminformatics tools: A contribution to the drug development and chemical science. *Journal of Biomolecular Structure and Dynamics*, *0*(0), 1–19. https://doi.org/10.1080/07391102.2023.2234039

Salor, L. C., & Baeza, V. M. (2023). Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications. *Telecom*, *4*(4), 709. https://doi.org/10.3390/telecom4040032

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Scribe.

Sangwan, R. S., Youakim Badr, & Srinivasan, S. M. (2023). Cybersecurity for AI Systems: A Survey. *Journal of Cybersecurity and Privacy*, *3*(2), 166. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/jcp3020010

Sarkin, J. J., & Sotoudehfar, S. (2024). Artificial intelligence and arms races in the Middle East: The evolution of technology and its implications for regional and international security. *Defense & Security Analysis*, *0*(0), 1–23. https://doi.org/10.1080/14751798.2024.2302699

Sarvajcz, K., Ari, L., & Menyhart, J. (2024). AI on the Road: NVIDIA Jetson Nano-Powered Computer Vision-Based System for Real-Time Pedestrian and Priority Sign Detection. *Applied Sciences*, *14*(4), Article 4. https://doi.org/10.3390/app14041440

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war* (First edition). W.W. Norton & Company.

Scharre, P. (2023). *Four battlegrounds: Power in the age of artificial intelligence* (First edition). W.W. Norton & Company.

Schleiger, E., Mason, C., Naughtin, C., Reeson, A., & Paris, C. (2024). Collaborative Intelligence: A Scoping Review Of Current Applications. *Applied Artificial Intelligence*, *38*(1), 2327890. https://doi.org/10.1080/08839514.2024.2327890

Schmertzing, L. (2018). *The Future of Warfare*.

Schmid, S., Riebe Thea, & Reuter, C. (2022). Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion Between Civilian and Defense R&D. *Science and Engineering Ethics*, *28*(2). Humanities Index; ProQuest Central; SciTech Premium Collection. https://doi.org/10.1007/s11948-022-00364-7

Schraagen, J. M. (2023). Responsible use of AI in military systems: Prospects and challenges. *Ergonomics*, *66*(11), 1719–1729. https://doi.org/10.1080/00140139.2023.2278394

Semenikhin, M., Fomina, O., Aksyonova, O., & Khmeliuk, A. (2023). Management Accounting of Payment Risks of Online Trade during Military Operations. *Theoretical and Practical Research in Economic Fields*, *14*(2), 473–483. ProQuest Central. https://doi.org/10.14505/tpref.v14.2(28).23

Shahzad, K., Aseeri, A. O., & Munam Ali Shah. (2022). A Blockchain-Based Authentication Solution for 6G Communication Security in Tactile Networks. *Electronics*, *11*(9), 1374. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics11091374

Sharma, A., Sharma, V., Jaiswal, M., Wang, H.-C., Jayakody, D. N. K., Basnayaka, C. M. W., & Muthanna, A. (2022). Recent Trends in AI-Based Intelligent Sensing. *Electronics*, *11*(10), Article 10. https://doi.org/10.3390/electronics11101661

Sharma, P., Sarma, K. K., & Mastorakis, N. E. (2020). Artificial Intelligence Aided Electronic Warfare Systems- Recent Trends and Evolving Applications. *IEEE Access*, *8*, 224761–224780. https://doi.org/10.1109/ACCESS.2020.3044453

Shen, D., Bao, S., Pietrafesa, L. J., & Gayes, P. (2022). Improving Numerical Model Predicted Float Trajectories by Deep Learning. *Earth and Space Science*, *9*(9). ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1029/2022EA002362

Shereshevsky, Y. (2022). International humanitarian law-making and new military technologies. *International Review of the Red Cross*, *104*(920–921),

2131–2152. ProQuest Central; Social Science Premium Collection. https://doi.org/10.1017/S1816383122000443

Shiekh, H. (2022). AI as a Tool of Hybrid Warfare: Challenges and Responses. *Journal of Information Warfare*, *21*(2), 36–49. ProQuest Central; SciTech Premium Collection; Social Science Premium Collection.

Shobar, M. A., & Tawil, R. (2023). Law enforcement and position locating in LTE network (status and challenges). *TELKOMNIKA*, *21*(6), 1221–1233. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.12928/TELKOMNIKA.v21i6.25353

Singh, A., Kalaichelvi, V., & Karthikeyan, R. (2022). A survey on vision guided robotic systems with intelligent control strategies for autonomous tasks. *Cogent Engineering*, *9*(1), 2050020. https://doi.org/10.1080/23311916.2022.2050020

Singh, A., Madaan, G., Hr, S., & Kumar, A. (2023). Smart manufacturing systems: A futuristics roadmap towards application of industry 4.0 technologies. *International Journal of Computer Integrated Manufacturing*, *36*(3), 411–428. https://doi.org/10.1080/0951192X.2022.2090607

Skarding, J., Gabrys, B., & Musial, K. (2021). Foundations and Modeling of Dynamic Networks Using Dynamic Graph Neural Networks: A Survey. *IEEE Access*, *9*, 79143–79168. https://doi.org/10.1109/ACCESS.2021.3082932

Snider, E. J., Hernandez-Torres, S. I., Guy, A., & Boice, E. N. (2022). Evaluation of an Object Detection Algorithm for Shrapnel and Development of a Triage Tool to Determine Injury Severity. *Journal of Imaging*, *8*(9), 252. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/jimaging8090252

Sonmez, F. (2022). Going under Dr. Robot's knife: The effects of robot anthropomorphism and mortality salience on attitudes toward autonomous robot surgeons. *Psychology & Health*, *0*(0), 1–18. https://doi.org/10.1080/08870446.2022.2130311

Spelda, P. (2020). Machine learning, inductive reasoning, and reliability of generalisations. *AI & SOCIETY*, *35*(1), 29–37. https://doi.org/10.1007/s00146-018-0860-6

Stinchfield, B. T. (2023). The military and commercial development of brain–computer interfaces: International (in)security with brain-machine teaming. *Defense & Security Analysis*, *39*(2), 233–252. https://doi.org/10.1080/14751798.2023.2191807

Stop the "Stop the Killer Robot" Debate: Why We Need Artificial Intelligence in Future Battlefields. (2022, June 21). Council on Foreign Relations. https://www.cfr.org/blog/stop-stop-killer-robot-debate-why-we-need-artificial-intelligence-future-battlefields

Strategic guidelines for developing AI-solutions. (2020). The Finnish Ministry of Defence. https://julkaisut.valtioneuvosto.fi/handle/10024/162372

Subramanian, H. V., Canfield, C., Shank, D. B., & Kinnison, M. (2023). Combining uncertainty information with AI recommendations supports calibration with domain knowledge. *Journal of Risk Research*, *26*(10), 1137–1152. https://doi.org/10.1080/13669877.2023.2259406

Sultan, A., & Jamy, S. H. (2022). Artificial Intelligence Revolution: Contemporary Trends and Implications for the Future of Warfare. *Journal of Security and Strategic Analyses*, *8*(1), 7–24. ProQuest Central; Publicly Available Content Database; Social Science Premium Collection.

Taheri, S., & Asadizanjani, N. (2022). An Overview of Medical Electronic Hardware Security and Emerging Solutions. *Electronics*, *11*(4), 610. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics11040610

Tam, C., Balau, M., & Oliveira, T. (2023). What Influences People's Adoption of Cognitive Cybersecurity? *International Journal of Human–Computer Interaction*, *0*(0), 1–18. https://doi.org/10.1080/10447318.2023.2279411

Taylor & Francis. (2024, April 4). https://taylorandfrancis.com/about/our-brands/

Teo, S. A. (2022). How Artificial Intelligence Systems Challenge the Conceptual Foundations of the Human Rights Legal Framework. *Nordic Journal of Human Rights*, *40*(1), 216–234. https://doi.org/10.1080/18918131.2022.2073078

Terrorism: Reducing Vulnerabilities and Improving Responses: U.S - Russian Workshop Proceedings (p. 10968). (2004). National Academies Press. https://doi.org/10.17226/10968

Texts adopted – Autonomous weapon systems – Wednesday, 12 September 2018. (2018). European Parliament. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html

The Future of the Battlefield. (2021). Office of the Director of National Intelligence.

The Landscape of Hybrid Threats: A Conceptual Model. (2021). Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

Torode, G. (2024, May 2). *US Official Urges China, Russia to Declare Only Humans, Not AI, Control Nuclear Weapons*. US News & World Report. //www.usnews.com/news/world/articles/2024-05-02/us-official-urges-china-russia-to-declare-only-humans-not-ai-control-nuclear-weapons

Tóth, Z., Caruana, R., Gruber, T., & Loebbecke, C. (2022). The Dawn of the AI Robots: Towards a New Framework of AI Robot Accountability. *Journal of Business Ethics*, *178*(4), 895–916. https://doi.org/10.1007/s10551-022-05050-z

Trachtman, J. P. (2022). Managing Cybersecurity and Technology Appropriation Threats to International Investment: Trust or Verify. *The International Lawyer*, *55*(2), 193–220. ProQuest Central.

Trusilo, D. (2023). Autonomous AI Systems in Conflict: Emergent Behavior and Its Impact on Predictability and Reliability. *Journal of Military Ethics*, *22*(1), 2–17. https://doi.org/10.1080/15027570.2023.2213985

Trusilo, D., & Danks, D. (2023). Artificial intelligence and humanitarian obligations. *Ethics and Information Technology*, *25*(1), 12. Art, Design & Architecture Collection; ProQuest Central; SciTech Premium Collection; Social Science Premium Collection. https://doi.org/10.1007/s10676-023-09681-2

Turunen, M. (2022). The Cyber Era`s Character of War. *European Conference on Cyber Warfare and Security*, 378–384. https://www.proquest.com/docview/2805589107/abstract/9D162E20B9BE45ABPQ/1

Tyczewska, A., Twardowski, T., & Woźniak-Gientka, E. (2023). Agricultural biotechnology for sustainable food security. *Trends in Biotechnology*, *41*(3), 331–341. ProQuest Central; SciTech Premium Collection. https://doi.org/10.1016/j.tibtech.2022.12.013

Umbrello, S. (2022). Editorial for the Special Issue on Meaningful Human Control and Autonomous Weapons Systems. *Information*, *13*(5), 215. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/info13050215

van Assen, M., Banerjee, I., & De Cecco, C. N. (2020). Beyond the Artificial Intelligence Hype: What Lies Behind the Algorithms and What We Can Achieve. *Journal of Thoracic Imaging*, *35*, S3. https://doi.org/10.1097/RTI.0000000000000485

Van Avery, C. E. (2007, July 1). *12 new principles of warfare*. Armed Forces Journal. http://armedforcesjournal.com/12-new-principles-of-warfare/

Venkatesh Kumar, C., Chaturvedi, A., A, A. T., Srinivas, P. V. V. S., Ranjit, P. S., Rastogi, R., Arun, M. R., & Rajaram, A. (2024). AI-IOT-Based Adaptive Control Techniques for Electric Vehicles. *Electric Power Components and Systems*, *0*(0), 1–19. https://doi.org/10.1080/15325008.2024.2304685

Venketeswaran, A., Lalam, N., Wuenschell, J., Ohodnicki, P. R., Jr, Mudabbir Badar, Chen, K. P., Lu, P., Duan, Y., Chorpening, B., & Buric, M. (2022). Recent Advances in Machine Learning for Fiber Optic Sensor Applications. *Advanced Intelligent Systems*, *4*(1). ProQuest Central; Publicly

Available Content Database; SciTech Premium Collection. https://doi.org/10.1002/aisy.202100067

Vorm, E. S., & Combs, D. J. Y. (2022). Integrating Transparency, Trust, and Acceptance: The Intelligent Systems Technology Acceptance Model (ISTAM). *International Journal of Human–Computer Interaction*, *38*(18–20), 1828–1845. https://doi.org/10.1080/10447318.2022.2070107

Wang, G. (2020). A neural network structure specified for representing and storing logical relations. *Neural Computing and Applications*, *32*(18), 14975–14993. https://doi.org/10.1007/s00521-020-04852-4

Wang, G., Shu, H., Gu, Y., Huang, Y., Zhao, H., & Yang, L. (2023). A Novel Virus Capable of Intelligent Program Infection through Software Framework Function Recognition. *Electronics*, *12*(2), 460. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/electronics12020460

Wang, X., Tang, F., Chen, H., Cheung, C. Y., & Heng, P.-A. (2023). Deep semi-supervised multiple instance learning with self-correction for DME classification from OCT images. *Medical Image Analysis*, *83*, 102673. https://doi.org/10.1016/j.media.2022.102673

War & Law. (2014, April 28). [Topic]. International Committee of the Red Cross. https://www.icrc.org/en/war-and-law%E2%80%83

Wareham, M. (2020). Stopping Killer Robots. *Human Rights Watch*. https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and

Wei, Y., Tran, S., Xu, S., Kang, B., & Springer, M. (2020). Deep Learning for Retail Product Recognition: Challenges and Techniques. *Computational Intelligence and Neuroscience*, *2020*, e8875910. https://doi.org/10.1155/2020/8875910

What is war today? (n.d.). The Changing Character of War Centre. Retrieved March 1, 2024, from https://www.ccw.ox.ac.uk/what-is-war-today

Williams, B. T. (2017, April 25). *Cyberwarfare and information warfare must be distinguished [Commentary]*. C4ISRNet. https://www.c4isrnet.com/2017/04/25/cyberwarfare-and-information-warfare-must-be-distinguished-commentary/

Xi, X. (2023). Advancing Language Assessment with AI and ML–Leaning into AI is Inevitable, but Can Theory Keep Up? *Language Assessment Quarterly*, *20*(4–5), 357–376. https://doi.org/10.1080/15434303.2023.2291488

Xia, L. (2022). The Indoor Space Layout of University Laboratories Based on Wireless Communication and Artificial Intelligence Decision-Making. *Wireless Communications & Mobile Computing (Online)*, *2022*. ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.1155/2022/5121762

Xu, H. (2022). Intelligent automobile auxiliary propagation system based on speech recognition and AI driven feature extraction techniques. *International Journal of Speech Technology*, *25*(4), 893–905. https://doi.org/10.1007/s10772-022-09958-9

Xu, L., Sun, Z., Ruan, Q., Xi, L., Gao, J., & Li, Y. (2023). Development Trend of Cooling Technology for Turbine Blades at Super-High Temperature of above 2000 K. *Energies*, *16*(2), 668. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/en16020668

Xu, S., Li, L., Zhou, Z., Mao, Y., & Huang, J. (2022). A Task Allocation Strategy of the UAV Swarm Based on Multi-Discrete Wolf Pack Algorithm. *Applied Sciences*, *12*(3), 1331. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/app12031331

Yang, Q., Huang, A., Fan, L., Chan, C. S., Lim, J. H., Ng, K. W., Ong, D. S., & Li, B. (2023). Federated Learning with Privacy-preserving and Model IP-right-protection. *Machine Intelligence Research*, *20*(1), 19–37. ProQuest Central; SciTech Premium Collection. https://doi.org/10.1007/s11633-022-1343-2

Yessenbayev, Z., Kozhirbayev, Z., & Shintemirov, A. (2022). Development of a computer vision module for autonomous vehicles. *Journal of Mathematics, Mechanics and Computer Science*, *116*(4), Article 4. https://doi.org/10.26577/JMMCS.2022.v116.i4.06

Yilmaz, F. G. K., Yilmaz, R., & Ceylan, M. (2023). Generative Artificial Intelligence Acceptance Scale: A Validity and Reliability Study. *International Journal of Human–Computer Interaction*, *0*(0), 1–13. https://doi.org/10.1080/10447318.2023.2288730

Yin-Chun, H., Yu-Xiang, Z., & Wei-Chen, H. (2022). Development of an Underground Tunnels Detection Algorithm for Electrical Resistivity Tomography Based on Deep Learning. *Applied Sciences*, *12*(2), 639. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/app12020639

Yu, S. N., Lee, J. K., Kim, S. H., Park, B. S., Kim, K. H., & Cho, I. J. (2013). *EXPERIMENTAL STUDY OF TELE-OPERATION DEVICES FOR THE REMOTE HANDLING SYSTEM IN A PYROPROCESSING FACILITY*. https://www-proquest-com.ezproxy.jyu.fi/docview/1447149214/3C1DCA34FB20462APQ/9?accountid=11774&sourcetype=Conference%20Papers%20&%20Proceedings

Yusaf, T., Abu Shadate Faisal Mahamude, Kaniz Farhana, Wan Sharuzi Wan Harun, Kumaran Kadirgama, Devarajan Ramasamy, Mohd Kamal Kamarulzaman, Subramonian, S., Hall, S., & Hayder Abed Dhahad. (2022). A Comprehensive Review on Graphene Nanoparticles: Preparation, Properties, and Applications. *Sustainability*, *14*(19), 12336. ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/su141912336

Žigulić, N., Glučina, M., Lorencin, I., & Matika, D. (2024). Military Decision-Making Process Enhanced by Image Detection. *Information*, *15*(1), 11. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database; SciTech Premium Collection. https://doi.org/10.3390/info15010011

Zoghlami, F., Kaden, M., Villmann, T., Schneider, G., & Heinrich, H. (2021). AI-Based Multi Sensor Fusion for Smart Decision Making: A Bi-Functional System for Single Sensor Evaluation in a Classification Task. *Sensors*, *21*(13), Article 13. https://doi.org/10.3390/s21134405

Zubair, M., Ghubaish, A., Unal, D., Al-Ali, A., Reimann, T., Alinier, G., Hammoudeh, M., & Qadir, J. (2022). Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System. *Sensors*, *22*(21), 8280. Coronavirus Research Database; ProQuest Central; Publicly Available Content Database. https://doi.org/10.3390/s22218280

APPENDICES

APPENDIX 1: DOCALYSIS EXPORT SAMPLE

Document	Use case	Page
2023_Technology trade controls and US–China competition.pdf	AI could be used to power sophisticated weapons and surveillance systems,	Page 2
2023_Technology trade controls and US–China competition.pdf	AI could be used to develop and govern technological and industrial parts of critical and emerging technologies,	Page 3
2023_Technology trade controls and US–China competition.pdf	AI could be used by countries to build technology ecosystems that exclude the Chinese market thereby excluding China from having access to superior US technologies and uncontested supply chains,	Page 3
2023_Technology trade controls and US–China competition.pdf	AI could be used to enforce trade restrictions within the area of semiconductors, and semiconductor-manufacturing equipment, related components, and chip-design software,	Page 2
2023_Technology trade controls and US–China competition.pdf	AI could potentially be used to assist in espionage activities, cyber-enabled capabilities, and surveillance.	Page 2
AL-Dosari et al_2024_Artificial Intelligence and Cyber Defense System for Banking Industry.pdf	Using artificial neural networks, artificial immune systems, fuzzy logic, and genetic algorithms to prevent and detect cybercrime (Pages 3-4)	Pages 3-4
AL-Dosari et al_2024_Artificial Intelligence and Cyber Defense System for Banking Industry.pdf	Using ANNs to process distributed information to detect irregularities and propose countermeasures	Page 5
AL-Dosari et al_2024_Artificial Intelligence and Cyber Defense System for Banking Industry.pdf	Using AI algorithms to discover vulnerabilities in security systems	Page 6
AL-Dosari et al_2024_Artificial Intelligence and Cyber Defense System for Banking Industry.pdf	Employing deep learning and ANNs to identify and prevent web-based attacks	Page 11
AL-Dosari et al_2024_Artificial Intelligence and Cyber Defense System for Banking Industry.pdf	Assisting in the automation of operations, such as discovering unidentified workstations, computers, code repositories and other hardware components and applications on a network	Page 11
AL-Dosari et al_2024_Artificial Intelligence and Cyber Defense System for Banking Industry.pdf	Finding patterns in data and making decisions appropriately	Page 4
AL-Dosari et al_2024_Artificial Intelligence and Cyber Defense System for Banking Industry.pdf	Automatically detecting and preventing malicious conduct, lowering the chance	Page 11

	of a security breach and reducing data compromised	
AL-Dosari et al_2024_Artificial Intelligence and Cyber Defense System for Banking Industry.pdf	Identifying fake/biased inputs, AI-powered password attacks, fictitious data, chat bot privacy/leaks, accumulation of data, and redundancy	Page 29
AL-Hawamleh_2023_Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related.pdf	AI can be used to improve malware defense mechanisms	Page 1
AL-Hawamleh_2023_Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related.pdf	AI can be used to disable hacking attempts	Page 6
AL-Hawamleh_2023_Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related.pdf	AI can help increase the accuracy of operations in cybersecurity	Page 7
AL-Hawamleh_2023_Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related.pdf	AI can be used to detect and respond to security threats	Page 7
AL-Hawamleh_2023_Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related.pdf	AI can be used for scenario recognition in multistep cyber-attacks	Page 8
AL-Hawamleh_2023_Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related.pdf	AI can facilitate machine learning for detecting irregularities in network activity	Page 7
AL-Hawamleh_2023_Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related.pdf	AI can be utilized in improving security of cyberspace	Page 6
Abbas et al_2023_When Human Meets Technology.pdf	Prediction of future threats by means of machine learning and data analysis	Page 4
Abbas et al_2023_When Human Meets Technology.pdf	AI-powered drones for surveillance and attack	Page 5
Abbas et al_2023_When Human Meets Technology.pdf	Cybersecurity applications, including detection and protection from cyber attacks	Page 5
Abbas et al_2023_When Human Meets Technology.pdf	Military robots with cognitive capabilities	Page 6
Abbas et al_2023_When Human Meets Technology.pdf	Automated decision making processes for targeting and selecting enemy targets	Page 7
Abbas et al_2023_When Human Meets Technology.pdf	AI-powered communication systems for military use	Page 8
Abbas et al_2023_When Human Meets Technology.pdf	AI-assisted intelligence gathering and processing	Page 9
Abbas et al_2023_When Human Meets Technology.pdf	Use of facial recognition for law enforcement and border control	Page 11