UNIDIR

FULL REPORT

Artificial Intelligence Beyond Weapons

Application and Impact of AI in the Military Domain

SARAH GRAND-CLÉMENT

Acknowledgments

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. The preparation of this report has been supported by generous funding for UNIDIR's Security and Technology Programme by the Czech Republic, Germany, Italy, the Netherlands, and Switzerland, and by Microsoft.

The author wishes to thank the experts who participated in the research and provided valuable inputs during the course of the study. The author is particularly grateful to all those who took the time to review the report and help improve it: Jason Lin, Stefan Nievelstein, Ioana Puscas, Dongyoun Cho, Giacomo Persi Paoli, Yasmin Afina and a reviewer who chose to remain anonymous.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

Citation

Sarah Grand-Clément, "Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain", UNIDIR, Geneva, 2023.

Author

Sarah Grand-Clément

Researcher, Conventional Arms and Ammunition, Security and Technology

Sarah Grand-Clément is a Researcher in the Conventional Arms and Ammunition Programme and the Security and Technology Programme of UNIDIR. Her work examines the intersection of technology and conventional arms, exploring both the benefits, as well as the challenges and threats technology can pose to international security. Sarah also has expertise in the use of futures methodologies as a way to help explore policy issues, in particular the use of horizon scanning, serious gaming and future scenarios. She holds an MSc in Arab World Studies from Durham University.

Acronyms & Abbreviations

AI	Artificial intelligence
C2	Command and control
CDE	Collateral damage estimation
GGE	Group of Governmental Experts
ISR	Intelligence, surveillance and reconnaissance
JRC	Joint Research Centre
LAWS	Lethal autonomous weapons system
LLM	Large language model

Contents

Executive Summary

Within the United Nations, the application of artificial intelligence (AI) in the military domain has, to-date, primarily been discussed in the context of the United Nations Group of Governmental Experts (GGE) on emerging technologies in the area of lethal autonomous weapons systems (LAWS). However, the application of AI within the military domain extends beyond the issue of LAWS. In the midst of discussions and debates around the opportunities and risks of AI for military purposes, as well as the governance and responsible use of these technologies, this report aims to increase understanding of the role of AI in the execution of military tasks beyond applications relating to the use of force and the narrow tasks of target selection and target engagement within the targeting process.

Through a review of the literature and engagement with experts, the report identifies 18 military tasks—denoted in this report as 'upstream' tasks—that occur prior to the narrow tasks of target selection and target engagement—in other words, 'downstream' tasks. These 18 upstream tasks are divided across four functional areas: command and control (C2), information management, logistics, and training.

For each of these tasks, a non-exhaustive overview of current AI capabilities is provided, as well as of feasible near-future capabilities, which encompass AI capabilities deemed by experts to be 'fairly certain' or 'likely' to emerge in the near future. This near future is set nominally to 2035, which is considered, for the purpose of the study, a suitable timeframe to examine realistic future impact. This mapping pertains to the state-of-play and technical feasibility of AI currently and in the near future, and not the level of adoption of AI by different actors.

Analysis of this mapping of AI capabilities demonstrates several points:

- A wide range of capabilities are currently technically feasible. However, the (future) existence of these capabilities does not necessarily imply or mean that they will be integrated in specific military tasks and military operations more widely.
- Many of the near-future AI capabilities focus on data fusion, analysis (including predictions and extrapolations), and simulations, placing an emphasis on AI capabilities that centre around the transformation of data into knowledge as well as systems which can learn, adapt, and react to changing information.
- Near-future capabilities primarily feature AI capabilities that demonstrate an enhancement of existing capabilities, notably by being able to work with more data and have better reasoning capabilities. To a lesser extent 'new' near-future abilities featured, demonstrating that ground-breaking revolutions in AI are not expected in the near future, at least as regards these specific military tasks.
- The relationship between AI and data, whereby AI is used to assist with data but is also dependent on it, demonstrates that issues of data integrity, quality, and veracity are going to remain key going forward. It also raises the question as to whether enough attention is being paid to these issues versus the AI capabilities themselves.

The following opportunities and challenges emerge when considering the impact of AI in the execution of upstream military tasks:

STRENGTHS AND OPPORTUNITIES	LIMITATIONS AND CHALLENGES
• Analysis of large amounts of varied data • Speed of communication, analysis, and decision-making • Planning and development of alternatives for action • Safety and security of virtual and physical assets • Optimisation of personnel time and effort	• Lack of (good quality) data impacting efficiency and accuracy of AI algorithms • 'Black box' nature of AI decision-making • Questions around applicability of meaningful human control to certain military tasks deemed 'low risk' • (Lack of) trust in AI's reasoning capabilities • Incorporation of AI increasing cybersecurity vulnerabilities • Overreliance on AI leading to rigid thinking around respective strengths and capabilities of humans versus machines • Skills degradation in military personnel • Generation of a faster operational tempo • Lack of harmonisation among different actors on use and application of AI • Unknown impact of AI application

The report concludes with the following considerations:

- Examination of the impact of AI on the upstream military tasks shows many similarities in the discussion compared to downstream tasks. Moreover, upstream tasks would have an impact on the downstream tasks as well as the broader conduct of a military operation.
- However, the operationalisation of AI in upstream tasks may be, in some cases, less controversial for decision makers than their inclusion in downstream tasks. This may be due to the inclusion of AI being less visible in upstream compared to downstream tasks—which may be a factor making the integration of AI in upstream tasks more likely.
- To that end, AI capabilities relating to both upstream and downstream military tasks should be included in discussions on AI for military purposes, particularly in light of issues relating to governance and responsible AI.

1. Introduction

1.1 Addressing the use of artificial Intelligence in the military domain

Within the United Nations, the application of artificial intelligence (AI) in the military domain has, to-date, primarily been discussed in the context of the United Nations Group of Governmental Experts (GGE) on emerging technologies in the area of lethal autonomous weapons systems (LAWS).[1] Within this context, most of the focus has been in terms of "maintaining human control over weapons, the critical functions of weapons, attacks, the targeting process, and (final) decisions to use force"[2]—in other words, focusing on the application of AI to the use of force specifically.

However, the focus on AI for military purposes within the United Nations has started to broaden beyond these strict confines. Greater attention has turned to the governance of AI more broadly, with the United Nations Secretary-General noting how AI could be used to "launch cyberattacks, generate deepfakes, or for spreading disinformation and hate speech"[3]—thereby moving away from solely looking at AI through the lens of LAWS within the peace and security domain. Moreover, AI is noted in one of the Secretary-General's latest policy briefs on peace and security issues as a technology requiring national strategies, norms, and rules within a global framework, due to its "increasing ubiquity [...] combined with its rapid scalability, lack of transparency and pace of innovation, [which] poses potential risks to international peace and security and presents governance challenges".[4]

Furthermore, the United Nations is forming a new multi-stakeholder High-level Advisory Body on Artificial Intelligence, to "undertake analysis and advance recommendations for the international governance of artificial

1 The aim of the GGE, according to the 2022 Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or Have Indiscriminate Effects, is to "intensify the consideration of proposals and elaborate, by consensus, possible measures, including taking into account the example of existing protocols within the Convention, and other options related to the normative and operational framework on emerging technologies in the area of lethal autonomous weapon systems, building upon the recommendations and conclusions of the Group of Governmental Experts related to emerging technologies in the area of lethal autonomous weapon systems, and bringing in expertise on legal, military, and technological aspects"; Report of the 2023 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, CCW/GGE.1/2023/2, May 23, 2023, https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_2_Advance_version.pdf.

2 Merel Ekelhof and Giacomo Persi Paoli, The Human Element in Decisions about the Use of Force, 2020, UNIDIR: Geneva, https://unidir.org/publication/human-element-decisions-about-use-force.

3 "Guterres Calls for AI 'that Bridges Divides', Rather than Pushing Us Apart", United Nations, 18 July 2023, https://news.un.org/en/story/2023/07/1138827.

4 United Nations, "A New Agenda for Peace: Our Common Agenda Policy Brief 9", 2023, https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf, 28.

intelligence".[5] AI was also—for the first time—the topic of a Security Council meeting on 18 July 2023, with the debate focusing on the opportunities and risks posed by AI to international peace and security.[6] Discussions notably touched upon the positive and transformational value of AI, but also of how it could change the threat landscape and warfare more broadly.

Beyond initiatives taken within the United Nations, States themselves have also started paying greater attention to the growing role of AI for military purposes beyond LAWS. This notably culminated in the Responsible AI in the Military domain (REAIM) summit, held in early 2023, from which a call to action on the responsible development, deployment, and use of AI in the military domain emerged.[7] The call to action notably highlights that "militaries are increasing their use of AI across a range of applications and contexts"[8] and that responsible use of AI is of paramount importance. As such, the governance and responsible use of AI for military purposes entails understanding how AI is currently being applied, and will be, especially beyond applications relating to the use of force and the narrow tasks of target selection and target engagement within the targeting process, which have to-date been the areas of greatest focus.

1.2 Purpose, scope, and methodology

Past studies have documented the broader current and potential uses of AI within the military, which includes helping, or even enabling, cyberspace operations; logistics planning; intelligence, surveillance and reconnaissance (ISR); and data analysis.[9] However, these insights into AI applications can be quite broad, without much specificity as to how AI applies in a military operation, particularly outside of the targeting process.

Thus, this report aims to increase understanding of the role and implications of AI[10] in the execution of military tasks that comprise a

5 "Multistakeholder Advisory Body on Artificial Intelligence", United Nations, https://www.un.org/techenvoy/content/artificial-intelligence.

6 "Artificial Intelligence: Opportunities and Risks for International Peace and Security - Security Council, 9381st Meeting", UN Web TV, July 18, 2023, https://media.un.org/en/asset/k1j/k1ji81po8p.

7 "Call to Action on Responsible Use of AI in the Military Domain", Government of the Netherlands, February 16, 2023, https://www.government.nl/ministries/ministry-of-foreign-affairs/news/2023/02/16/reaim-2023-call-to-action.

8 "REAIM Call to Action", Government of the Netherlands, February 16, 2023, https://www.government.nl/ministries/ministry-of-foreign-affairs/news/2023/02/16/reaim-2023-call-to-action, 1.

9 See for example Wyatt Hoffman and Heeu Millie Kim, Reducing the Risks of Artificial Intelligence for Military Decision Advantage, Center for Security and Emerging Technology, 2023; Niklas Masuhr, AI in Military Enabling Applications, CSS Analyses in Security Policy No. 251, October 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse251-EN.pdf; Kelley M. Sayler, Artificial Intelligence and National Security, Congressional Research Service Report, November 10, 2020, https://sgp.fas.org/crs/natsec/R45178.pdf; Forrest E. Morgan et al., Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World, Santa Monica: RAND Corporation, 2020.

10 Given that this study looks at a range of AI capabilities, both present and future, in addition to the fact that there is no agreed definition of AI, it was decided that providing a definition may be too prescriptive and could in fact limit discussions. For ease, this report therefore refers to AI in general terms, noting that this term encompasses a number of subfields whereby the capabilities and needs of different types of AI (e.g., machine learning, deep learning, computer vision, natural language processing, etc.) differ.

military operation, beyond the narrow tasks of target selection and target engagement and use of weapons themselves.[11] Beyond the much-discussed debate around the use of AI in engaging a target and applying lethal force, this report examines what it means to implement AI in the many steps and processes that come beforehand. It aims to do so by providing a realistic overview of AI capabilities, without overemphasising the role AI does or may play within the military domain.[12] As a result, this report focuses solely on exploring AI capabilities relating to upstream tasks during a military operation, including those which have an indirect effect of lethality, but are not tasks specifically related to target selection and target engagement, which are considered downstream tasks.

This report also presents a discussion on the impact of AI application to these upstream military tasks, complementing existing debates regarding the integration of AI into the targeting process and weapon systems specifically. To this end, this report is primarily aimed at members of the diplomatic community focused on disarmament and technology issues, as well as other relevant stakeholders operating in this field, such as research and advocacy organisations.

Specifically, this report focuses on AI capabilities and applications currently and in the near future, set nominally to 2035. This time frame was chosen for two main reasons:

- First, to ensure that realistic AI applications are presented, a limited time frame within the foreseeable future was selected.
- Second, the adoption of technology within the military is not a rapid process, due to a range of reasons, including lengthy procurement and approvals processes. Therefore, the 2035 timeframe is far enough from the time of writing that changes in the application of AI in the military can be considered realistic.

This report is based on a review of the relevant literature, as well as on data collected through interviews and an expert workshop. Initial interviews, held in September 2022, were with former members of the military, Member State representatives, and members of the technical community, which served to review and validate both the military tasks themselves as well as areas of AI applications. The workshop, held in October 2022, brought together representatives from the technical, military, and research communities to further discuss and debate applications of AI and associated impacts. Subsequent interviews were also held in August to September 2023, to refine and validate the mapping of AI capabilities.

---

11 The targeting process includes a range of phases: find, fix, track, target, engage and assess (see Merel Ekelhof and Giacomo Persi Paoli, The Human Element in Decisions about the Use of Force for further detail). Within the context of this report, the phases 'engage' and 'assess' are out of scope. Additionally, weapons are specifically defined as the means of delivery of lethal force, with the study looking at tasks which may enable or feed into the decision to use lethal force but are not used as the means of delivery of lethal force themselves.

12 Overemphasising AI capabilities can lead to erroneous assessments and policy decisions. For a more detailed discussion on this topic, see for example Cameron Hunter and Bleddyn E. Bowen, "We'll never have a model of an AI major-general: Artificial Intelligence, command decisions, and kitsch visions of war", Journal of Strategic Studies (2023), https://doi.org/10.1080/01402390.2023.2241648 and Yasmin Afina, "Intelligence is dead: long live Artificial Intelligence", Chatham House, July 14, 2022, https://www.chathamhouse.org/2022/07/intelligence-dead-long-live-artificial-intelligence.

1.3 Report structure

The report first maps the military functional areas and their related tasks and provides insight on AI capabilities regarding the execution of specific military tasks now and in the near future (**Chapter 2**). The report subsequently explains the impact and implications of AI integration in these tasks (**Chapter 3**), before providing concluding remarks (**Chapter 4**).

2. Role of AI in the execution of military tasks

This chapter first introduces the military tasks used as the framework of reference for this study, before mapping current and feasible near-future AI capabilities to these tasks.

2.1 Mapping military tasks

The use of weapons in instances of conflict is only one of many activities during a military operation. There are many other activities during a military operation that occur and precede the narrow tasks of target selection and target engagement. Therefore, to fully understand the application of AI prior to the use of weapons, it is necessary to define military tasks which would typically comprise a military operation, aside from use of lethal force. The military tasks are shown in figure 1 and are divided into four functional areas:[13]

1. **Command and control (C2)**: C2 refers to the decision-making aspect of a military operation. For this study, tasks under the C2 functional area primarily focus on the analysis elements in support of military decision-making and planning, as opposed to the conduct of military action, which falls outside of the present study's scope.
2. **Information management:** Information management refers to the collecting, processing, exploiting, and disseminating of information relating to a military operation. Within the context of this study, this functional area also contains elements relating to defensive cyberspace operations.
3. **Logistics:** Logistics refers to the movement, supply, and monitoring of personnel and equipment to sustain a military operation.
4. **Training:** Training refers to the instruction and preparation of military personnel.

The military tasks within these functional areas are agnostic of command level, focusing instead on activities undertaken. While the tasks are numbered for clarity, this does not imply a hierarchical relationship between either the tasks or the functional areas, nor a chronology in terms of the tasks outlined.

Overall, these military tasks are used as a framework for the subsequent mapping of AI capabilities. As such, while they aim to reflect the various activities comprised within a mission, the purpose is not for these tasks to form a comprehensive list nor reflect any particular military doctrine. Indeed, missions and therefore tasks comprised within will differ in terms of their scope, situation, actors involved, and more. Rather, the military tasks outlined below should be seen as a tool to

13 The tasks and functional areas were elaborated based on a review of existing literature, namely Ekelhof and Persi Paoli, The Human Element in Decisions about the Use of Force; Masuhr, AI in Military Enabling Applications; Sayler, Artificial Intelligence and National Security, and inputs from interviews with Stefan Nievelstein (28/09/2022) and two anonymous experts (14/07/2022 and 13/10/2022).

help frame the present discussion. Additionally, for scope purposes, the tasks below do not take into account the daily running of the military infrastructure more broadly, which would include administrative tasks such as human resource management, payroll management, or fraud detection and prevention. Similarly, (emergency) medical care during and post-mission is also considered out of scope.

Figure 1. Upstream military tasks

FUNCTIONAL AREA	MILITARY TASK
C2	1. Undertake target analysis (i.e., identifying the most relevant targets) 2. Determine choice of weapons and weaponeering[14] 3. Assess weapon capabilities and effects (e.g., munition fragmentation patterns, secondary explosions, etc.) 4. Estimate protection, collateral damage, and risk mitigation, including non-strike entities (e.g., civilian patterns of life, time of attack) 5. Develop mission implementation plan (e.g., identification of courses of action and pathways, etc.) 6. Plan for contingencies (e.g., loss of equipment, loss of communication, etc.) 7. Plan and adapt manoeuvres in the battlefield based on available information, intelligence and data collected real time in the land, air, naval, space and cyber domains 8. Continuous impact assessment of the campaign (including assessing public opinion, etc.)
Information management	9. Clean, filter, and fuse data collected via intelligence, surveillance and reconnaissance (ISR) 10. Analyse data collected through ISR across the land, air, naval, space and cyber domains 11. Analyse own, friendly and adversary capabilities (e.g., manpower, equipment, training, facilities, status of equipment, etc.) 12. Analyse the environment (which includes terrain, infrastructure, non-strike entities, impact on civilians, etc.) 13. Synthesise the key points emerging from the analysis of the data collected 14. Disseminate information across the chain of C2 15. Manage information and communication security
Logistics	16. Logistical support of deployment (i.e., acquisition of necessary material/equipment, plan deployment of personnel, plan transport of equipment and personnel, manage force protection) 17. Assess operational effectiveness of people and equipment (i.e., real-time monitoring of performance and status)
Training	18. Undertake training and simulation (i.e., educate military personnel and undertake individual and collection training)

14 "Weaponeering is the process of determining the quantity of a specific type of lethal or non-lethal means required to generate the desired effect on a given target"; Ekelhof and Persi Paoli, The Human Element in Decisions about the Use of Force, 4.

2.2 Application of AI capabilities across military tasks

The tables below present the mapping of AI capabilities against each of the military tasks.[15] Often, the application of AI in the military domain tends to either focus specifically on the use of force and the narrow tasks of target selection and target engagement, or mention the use of AI in general terms, such as to aid with analysis, but without specifying the specifics of such analysis. This mapping of AI capabilities to specific military tasks (beyond the narrow tasks of target selection and target engagement within the targeting process) therefore aims to address these gaps. It should be noted that there can be differing opinions as to the existence of various capabilities; the tables therefore aim to show the consensus views, while acknowledging and also in places clearly identifying that alternative opinions exist, particularly in light of the rapidly advancing pace of technology.

This mapping does not aim to be comprehensive of the entire spectrum of AI capabilities, focusing instead on the ones deemed most relevant and pertinent for each task based on the literature and expert insights. It should, however, be noted that this mapping pertains to the state-of-play and technical feasibility of AI currently and in the near future, and not the level of adoption of AI by different actors.[16] Indeed, there is a wide range of factors that impact adoption of AI (or indeed, any other technology), such as in terms of available resources and infrastructure to support AI development and deployment, human resources and expertise in AI, relevance of a capability, or willingness of adoption of AI by different actors. A discussion of these factors is beyond the scope of this present report, which focuses on understanding AI capabilities agnostic of such variables.

---

15 AI capabilities based on insights from literature (notably: Masuhr, AI in Military Enabling Applications; Sayler, Artificial Intelligence and National Security; Peter Svenmarck et al., Possibilities and Challenges for Artificial Intelligence in Military Applications, NATO, 2018; "Artificial Intelligence is the Future of Warfare (Just Not in the Way You Think)", Paul Maxwell, April 20, 2020, https://mwi.usma.edu/artificial-intelligence-future-warfare-just-not-way-think/; Morgan et al., Military Applications of Artificial Intelligence; Zhang et al., "Application of Artificial Intelligence in Military"; José Javier Galán, Ramón Alberto Carrasco, and Antonio LaTorre, "Military Applications of Machine Learning: A Bibliometric Perspective", Mathematics, 10, no. 9 (2022), https://doi.org/10.3390/math10091397; Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," Texas National Security Review 1, no. 3 (2018): 36–57, https://doi.org/10.15781/T2639KP49; Erik Lin-Greenberg, "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making", Texas National Security Review, 3, no. 2 (2020): 56–76, http://dx.doi.org/10.26153/tsw/8866); discussions by workshop participants (Dr. Michael Gerz, Lt. Col. Martijn Hädicke, Anna Knack, Dr. Jason Lin, Dr. Andrew Lohn, Dr. Mark Manantan, Dr. Peter Svenmarck, Ret. Col. Jean-Christophe Noel, Dr. Diane Vavrichek); and validated through interviews with Dr. Joel Brynielsson (12/09/2023), Thomas Grohs (01/09/2023), and Dr. Martin Hagström (04/09/2023).

16 Specific Technology Readiness Levels (TRLs) have not been assigned to the current and feasible near-future capabilities. However, it is assumed that all technologies mentioned are or would be at TRL 7 ("system prototype demonstration in operational environment") or above. For further information on TRLs for AI, see Fernando Martínez-Plumed, Emilia Gómez and José Hernández-Orallo, "Futures of Artificial Intelligence through Technology Readiness Levels," Telematics and Informatics, 58 (2021), https://doi.org/10.1016/j.tele.2020.101525.

Command and Control

	CURRENT AI CAPABILITIES	FEASIBLE NEAR-FUTURE AI CAPABILITIES
1. UNDERTAKE TARGET ANALYSIS	• **Network mapping** to identify highly valuably targets within a network, based on, for example, pattern recognition and analysis of communication means • **Calculation and assessment of inter-dependencies** between different targets • Identification of individuals and objects via **image recognition or other data types** (e.g., individuals of interest, buildings, military vehicles) to include both targets to engage and those to avoid • Automation of agents and their actions in **wargaming simulations** and synthetic environments for training and planning • **Identification of targets** (human or other), via motion of points, bodies, and systems of bodies and patterns of life • Application of AI to the **analysis of synthetic aperture radar data from space-based assets**, particularly in instances of adverse weather conditions	• **Assessment aid** as to whether the selected targets abide by the stated objectives, desired effect and rules of engagement • **Prediction** of contextualized opponent behaviour • **Provision of several courses of action** or recommended courses of action based on the mission's strategy and intended targets[17] • **Simulations and extrapolations of future outcomes** based on data and assessments stemming from the target analysis[18] • **Prioritisation, filtering, and triage of information** in a faster manner regarding operational conditions and data • Enhanced provision of support to **red teaming** (i.e., undertaking a challenging function to existing plans) • Provision of **initial and rapid legal advice** as 'first opinions' ahead of human military legal advisers, such as to assess whether there are contradictions between on-the-ground action and legal and regulatory frameworks[19]
2. DETERMINE CHOICE OF WEAPONS AND WEAPONEERING	• Provision of a **menu of options or recommendation** regarding choice of weapons, based on target and environment data within a singular domain of operation • **Decision aid** for weaponeering, taking into account the technology applied to targeting and collateral damage estimation (CDE)	• Provision of a **menu of options or recommendation** regarding choice of weapons, based on target and environment data across domains (i.e., joint capability, ability to take into account all elements and pieces of equipment across multiple domains) • **Simulations and extrapolations of future outcomes**, including on CDE, enabling identification of future outcomes based on weaponeering choices

17 Based on the pace of development of capabilities such as large language models, this was noted as being closer to a current capability.

18 Experts noted however some uncertainty with regard to this capability, with some indicating that they felt this capability was unlikely to be feasible in the near future.

19 It was noted that this may be extremely difficult to computerise, as the analysis and argumentation feeding into legal advice is complex; therefore this capability should not be seen as a replacement for legal advisers, but a lower-level type of capability.

3. ASSESS WEAPON CAPABILITIES AND EFFECTS	• **Simulations and extrapolations of future outcomes, including on CDE**, enabling identification of future outcomes based on weapon capabilities and choices • **Provision of several courses of action** or recommended courses of action based on the analysis of weapon capabilities and effects based on target and environment data within a singular domain of operation • **Modelling of disruption** of weapon effects to critical infrastructure	• Improved **simulation of weapon effects**, including on more accurately represented environments • **Calculation and assessment of interdependencies** between different targets • **Provision of more advanced courses of action** or recommended courses of action based on the analysis of weapon capabilities and effects (e.g., taking more variables into account, cross-domain data, etc.) • **Increased accuracy of modelling of disruption** of weapon effects to critical infrastructure, including modelling of a multitude of effects and wider area, and across time
4. ESTIMATE PROTECTION, COLLATERAL DAMAGE, AND RISK MITIGATION	• **Calculation of basic civilian patterns of life** (e.g., broad behavioural patterns, traffic trends, etc.) • **Provision of several courses of action** or recommended courses of action based on the CDE and risk mitigation analysis • **Prediction and assessment of collateral damage**, including the destructiveness of various types of weapons on specific targets	• **Calculation of more advanced civilian patterns of life** (e.g., by demographic groups, increased specificity, detail, interrelation, etc.) • **Simulations and extrapolations of future outcomes**, including on CDE, enabling identification of future outcomes based on weaponeering choices
5.DEVELOP MISSION IMPLEMENTATION PLAN	• **Provision of several courses of action** or recommended courses of action with regard to mission implementation based on target and environment data within a single domain of operation • **Simulations** of optimal force position in theatre • **Simulations and extrapolations** of mission implementation	• Development of **large-scale mission implementation scenarios** • **Provision of several courses of action** or recommended courses of action with regard to mission implementation across domains (i.e., joint capability, ability to take into account all elements and pieces of equipment across multiple domains) • Assessment of patterns of decision-making and, based on these, **proposal of novel tactics** and pathways towards mission implementation
6. PLAN FOR CONTINGENCIES	• **Optimisation of data routing** within tactical networks • **Simulations and extrapolations** regarding possible pathways and their respective contingency plans • **Provision of several courses of action** or recommended courses of action with regard to possible contingencies	• Conduct of AI-generated **wargames and red teaming** to assist with the planning of contingencies • Identification in real time of **contingency plans**, such as secondary communications systems or new communication and transport routes

7. PLAN AND ADAPT MANOEUVRES IN THE BATTLEFIELD	• **Analysis in real-time of sensor data** in order to direct systems towards a specific location or in response to a movement, sound, visual, or other in a specific domain (i.e., sensor allocation)	• Support to the creation of a common operational picture via the use of **data fusion** (i.e., the integration of multiple sources and types of data) • Use of ISR data, image recognition, and target tracking in order to **process data and locate targets over time, in changing circumstances, and across domains of operation** (e.g., land domain and cyber domain)
8. CONTINUOUS IMPACT ASSESSMENT OF THE CAMPAIGN	• Conduct of **sentiment analysis**, based on natural language processing for example, on news and social media data captured from the public domain • **Detect misinformation** with generative AI	• **Simulations and extrapolations** of future outcomes of the campaign's impact • **Estimation of battle damage assessment** for greater range of weapons (e.g., simultaneous use of weapons such as missiles, armed uncrewed systems, tanks, etc.) • Faster and improved **estimation of casualty numbers** throughout the campaign

Information Management

	CURRENT AI CAPABILITIES	FEASIBLE NEAR-FUTURE AI CAPABILITIES
9. CLEAN, FILTER, AND FUSE DATA COLLECTED	• Fusion of 2D data, such as images, to **create 3D models** • **Geolocation of images** • **Identification and classification of data**, such as targets • **Pattern recognition** within raw visual, written, audio, and other data to help identify specific incidents or hostile activity (e.g., via detection of anomalies in patterns, deepfakes, etc.)	• **Synthesis of large quantities of data**, such as imagery or video • **Fusion of data across the full electromagnetic spectrum** (i.e., visible, ultraviolet, infrared, microwaves, radio waves etc.) to create a 'common operating picture', including a (partial) fusion of cross-domain and all-source intelligence • **Detection of deviations** in the 'common operating picture' from the intended plan • **Enhancement of early-warning capabilities** with regard to developments or operations in the field
10. ANALYSE DATA COLLECTED THROUGH ISR ACROSS LAND, AIR, NAVAL, SPACE AND CYBER DOMAINS	• **Analysis of data** across the full electromagnetic spectrum (i.e., visible, ultraviolet, infrared, microwaves, radio waves etc.) in specific domains of operation and specific individual spectrums to identify elements of interest • **Analysis of large quantities of data**, such as imagery or video • **Analysis in real time of sensor data** in order to direct systems towards a specific location or in response to a movement, sound, visual, etc. in a specific domain (i.e., sensor allocation)	• **Analysis of fused data**, across domains of operation and across the different spectrums • **Analysis of a wide range of fused information** (e.g., social media/open source information, military intelligence, data from across the electromagnetic spectrum)

11. ANALYSE OWN, FRIENDLY AND ADVERSARY CAPABILITIES	• **Identification of individuals and objects** (e.g., military equipment, amount, location, etc.) via the full electromagnetic spectrum (i.e., visible, ultraviolet, infrared, microwaves, radio waves, etc.) • **Identification of communication means**, utilising these for pattern recognition and pattern extrapolation • **Monitoring of combat capabilities** in real time	• **Simulations and extrapolations** of future outcomes • **Prediction** of how adversary capabilities may develop • **Simulation and/or prediction of outcomes** in engagement between friendly and adversary forces • **Enhanced prediction of behaviour** based on an analysis of behavioural patterns
12. ANALYSE THE ENVIRONMENT	• **Analysis of civilian traffic flows** (land, air, maritime) • **Planning of the most appropriate route** forces can take • **Identification of individuals and objects** (e.g., improvised explosive devices, snipers, etc.) via image recognition and/or analysis of the full electromagnetic spectrum • **Analysis of cyber space** with regards to information, disinformation tactics, etc. • **Real-time map building** of conflict or disaster-stricken areas	• **Analysis of no-go (restricted) zones** including the incorporation of live data • **Analysis of terrain traversability**, to identify any obstacles (e.g., environmental) or threats • **Analysis of the interconnections** between objects in a system (e.g., interconnections between infrastructure) • Improved **real-time map building** of disaster and conflict zones • **Modelling of the interior of specific buildings** (e.g., rooms, hallways, etc.)
13. SYNTHESISE THE KEY POINTS EMERGING FROM THE ANALYSIS OF THE DATA COLLECTED	• **Retrieval systems** that can reference search engines or databases • Generation of **automatic summaries** of key information • Automated **analysis of data** to extract key information[20]	• Generation of more advanced and precise **automatic summaries** of key information (e.g., summaries and key point generation can be tailored based on the audience or reader) • (Partial) **fusion of multi-domain and all-source intelligence**

20 There was uncertainty noted with this capability, due to the recent advances in large language models (LLMs), with some experts leaning towards the fact that this is a current capability, and others who believe it is a near-future capability.

14. DISSEMINATION OF INFORMATION ACROSS THE CHAIN OF C2	• **Filtering** of (non-relevant) information • **Aggregation of information**	• **Generation of automatic reports**[21] • **Automated distribution of messages** to relevant individuals[22]
15. MANAGE INFORMATION AND COMMUNICATION SECURITY	• Integration of AI into cyber operations to improve cybersecurity and better **counter cyberthreats** (e.g., via AI-powered anomaly detection)[23] • **Detection of intruders** based on anomalous behaviour	• **Advanced biometrics** • Building of fault trees to find weak points in systems • Support for **information classification** (e.g., by text and content analysis) • **Verification of information veracity** and data provenance

Logistics

	CURRENT AI CAPABILITIES	FEASIBLE NEAR-FUTURE AI CAPABILITIES
16. LOGISTICAL SUPPORT OF DEPLOYMENT	• **Analysis of the best paths and transport modes** for a given mission and environmental and traffic conditions • **Provision of recommendations** on the best paths and transport modes for a given mission and environmental and traffic conditions • **Organisation of staff rotation** (i.e., scheduling) • **Moderation and overview of optimal or desired energy utilisation** • Assistance with **automated planning and scheduling** of personnel and logistics • **Identification of equipment maintenance needs** via image recognition (e.g., cracks in propellors or blades)	• **Assessment of equipment needs** and provision of acquisition recommendations • (Improved) **prediction of equipment resupply needs** based on patterns of use and stockpile management data • **Optimisation of logistical supply chains** (e.g., faster or more efficient routes, early warning when supplies low, etc.)

21 There was uncertainty noted with this capability, due to the recent advances in LLMs, with some experts leaning towards the fact that this is a current capability, and others who believe it is a near-future capability.

22 There was an uncertainty noted with this capability, due to the recent advances in LLMs, with some experts leaning towards the fact that this is a current capability, and others who believe it is a near-future capability.

23 There was an uncertainty noted with this capability, with most experts leaning towards the fact that this is a current capability, and others who believe it is a near-future capability.

17. ASSESS OPERATIONAL EFFECTIVENESS OF PEOPLE AND EQUIPMENT	• **Evaluation and early warning** regarding the physical and medical readiness of military personnel • Basic **triage** of injured or unwell personnel • **Provision of recommendations** on how to improve personnel health, resilience, and readiness • **Predictive maintenance needs** on equipment	• **Predictive maintenance needs** on deployed equipment based on mission progress and conditions • (Improved) **prediction of resupply needs** (e.g., ammunition, spare parts) through a connected and digital logistics chain

Training

	CURRENT AI CAPABILITIES	FEASIBLE NEAR-FUTURE AI CAPABILITIES
18. UNDERTAKE TRAINING AND SIMULATION	• Design of **virtual simulations or real-life exercises**, with AI opponents of different difficulty to match and challenge the trainees' level of competence • **Estimation of losses and outcomes** from operation simulations • **Tracking of individuals' learning progress** and offering of tailored learning activities based on progress • **Generation of synthetic data** for simulation planning and development of simulated actions plans • Automatic **detection and mapping of significant learning situations** during operations, in support of after-action reviews • Assistance in simulation as a **tactical co-pilot or as synthetic intelligent agents** to be coordinated with	• (Improved) **modelling and simulation** predictions of outcomes and adversary decision-making • **Modelling** of best patrolling routes and behaviour • Design and conduct of **AI-generated wargames and red teaming**[24] • Support to the **generation of mission tactics**

24 There was an uncertainty noted with this capability, with some participants leaning towards the fact that this is a current capability, and others who believe it is a near-future capability.

2.2.1 Mapping

As demonstrated in Section 2.2, AI application areas are numerous. So as to best understand this wealth of data and ensure comparability between military tasks, each AI capability was mapped against a set of AI categories, derived from a taxonomy devised by the European Commission's Joint Research Centre (JRC).[25]

This taxonomy, where AI categories are shown agnostic of users and area of application, focuses specifically on the capabilities AI offers. The AI categories from the JRC taxonomy are reasoning, planning, learning, communication, perception, integration and interaction, services, and ethics and philosophy. The categories selected and the wording of the category descriptions have been adapted to the context of this report and to ensure consistency of terms used within this report, but broadly reflect the content and language used in the JRC taxonomy. The adapted AI categories of the JRC taxonomy used for this analysis are provided below:

- **Reasoning:** the transformation of data into knowledge, or the inference of facts from data.
- **Perception:** the ability by a system to map elements in the environment it operates in through image, audio, and other sensors.
- **Communication:** the ability of a system to identify, process, make inferences and/or generate information in written and spoken communications.
- **Planning:** the design and execution of strategies, e.g., an organised set of actions, to achieve a goal.
- **Learning:** the ability of a system to automatically learn, decide, predict, adapt, and react to changes, improving from experience, without being explicitly programmed.

To undertake this mapping, up to two AI categories were assigned to each AI capability.[26] The results from each military task were then aggregated at the functional area level, and the instances of AI categories per functional area expressed in percentages, in order to create a visual summary of this data. The mapping below thus provides both a visual overview on current AI capabilities (figure 2) as well as feasible near-future capabilities (figure 3), grouped by their broader functional areas.

---

25 Sofia Samoili et al., AI Watch Defining Artificial Intelligence: Towards an Operational Definition and Taxonomy of Artificial Intelligence (Luxembourg: European Union, 2020), 11, https://publications.jrc.ec.europa.eu/repository/handle/JRC118163. It should also be noted that while the JRC taxonomy is used here, a number of other taxonomies exist, for example: National Security Commission on Artificial Intelligence, Final Report, 2021, 33, https://assets.foleon.com/eu-west-2/uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf. This exercise could therefore be repeated for each existing taxonomy and different mappings produced according to the different ways in which AI capabilities are broken down.

26 For example, the AI capability 'analysis of terrain traversability' was assigned two AI categories: 'perception' and 'reasoning'. This analysis was undertaken twice by the same person, compared, and where necessary adjusted, to ensure that the categorisation followed the same logic across all AI capabilities.

Figure 2. Domains of AI applications mapped against the functional areas—current capabilities

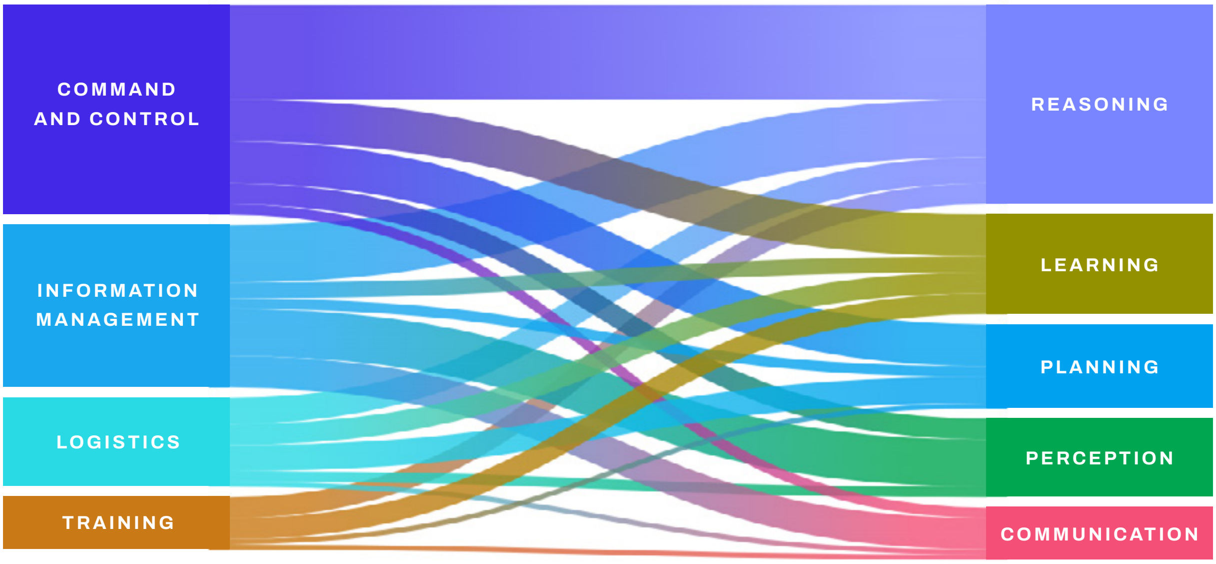
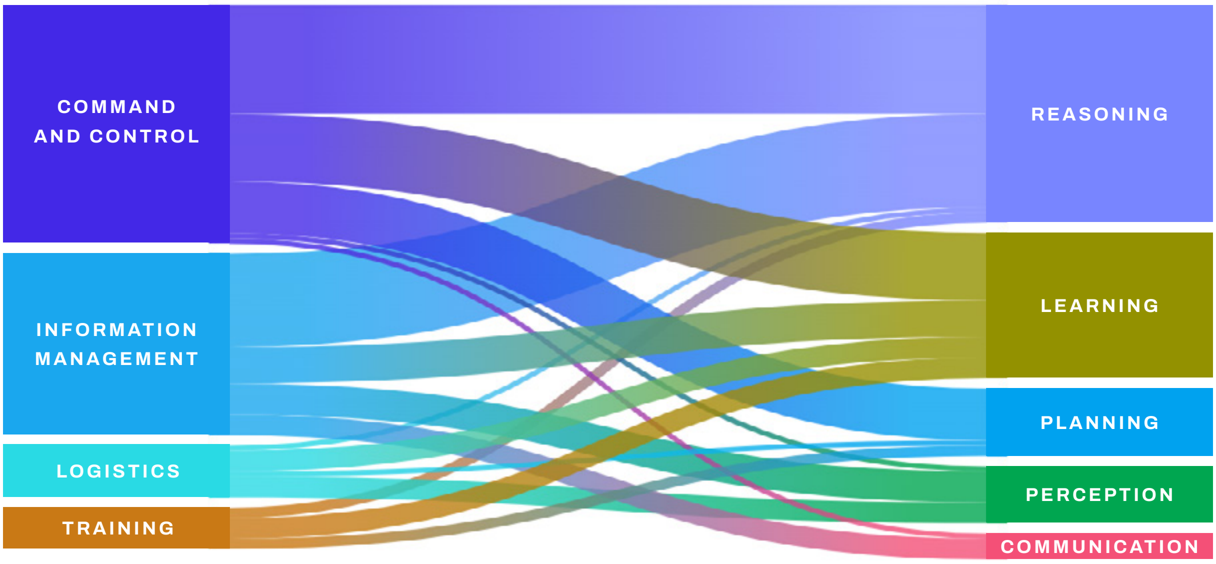


Figure 3. Domains of AI applications mapped against the functional areas—near-future capabilities



Note: The domains of AI applications as drawn from the JRC's taxonomy are shown to the right of each diagram. The functional areas, which include each individual current and near-future AI capabilities from Section 2.2, are shown on the left of each diagram.

2.2.2 Discussion on the mapping of current and near-future AI capabilities to military tasks

The mapping of AI capabilities against each of the military tasks, as well as against the domains of AI applications, demonstrates some interesting facets in terms of how AI for military purposes is anticipated to evolve into the near future. Notably, a wide range of AI capabilities are currently technically feasible. However, this should nonetheless be caveated by noting that the (future) existence of these capabilities does not necessarily imply or mean that they will be integrated into specific military tasks and military operations more widely. Indeed, there can be a number of difficulties regarding their implementation that may mean that, although a capability may exist, and is even developed and tested, it may ultimately not be introduced into operational use. Additionally, not all near-future capabilities outlined in Section 2.2 will develop and mature at the same pace and with the same timeline; some may become technologically mature at a faster pace than others. For example, the recent rapid advances in LLMs and generative AI means that related AI capabilities may mature more quickly.

This point notwithstanding, the data shows that a focus on AI capabilities centred around 'reasoning' (i.e., "the transformation of data into knowledge, or the inference of facts from data") and 'learning' (i.e., "the ability of a system to automatically learn, decide, predict, adapt and react to changes, improving from experience, without being explicitly programmed") may be expected in the near future. This aligns with the examination of specific near-future AI capabilities, where a lot of emphasis is placed on data fusion, analysis (including predictions and extrapolations), planning, and simulations.

Looking more closely at these near-future AI capabilities, two main trends can be identified. The first trend pertains to near-future AI capabilities which are an enhancement of existing capabilities. This notably includes being able to work with more data and data types, and having better reasoning capabilities—in effect, enhancing and improving upon what currently exists. While the AI enhancements foreseen within this first trend are more evolutionary than revolutionary, this does not mean that they require less effort in their adoption by militaries in terms of procurement policies, testing, training requirements and beyond.

The second trend regards the development of 'new' near-future AI capabilities, in other words, capabilities which are novel and go beyond an enhancement of existing capabilities. Specifically, the data demonstrates that ground-breaking revolutions in AI for military purposes are not expected in the near term, at least as regards these specific military tasks, particularly as there are fewer such capabilities falling in this particular category. The recent advances of generative AI, which includes LLMs, may however play an important role, particularly as it develops further, matures, and becomes incorporated with predictive AI capabilities.

The final point pertains to the increased use of AI to aid with data processing and synthesis, as well as the dependency of AI on data for its development and training. This demonstrates that issues of data integrity, quality, and veracity are going to remain key going forward. It also raises the question as to whether enough attention is being paid on these issues versus the AI capabilities themselves. Indeed, issues pertaining to data, as well as the broader enabling technology and infrastructure necessary to enable and achieve the

near-future AI capabilities, bring into question the potential operationalisation of AI capabilities.[27] Beyond data, this includes, for example, advancements in sensors, computing power, and other electronic devices,[28] but also in ensuring that all data collection and data processing systems are connected and interoperable with one another—as a fragmented system would hamper (an efficient) use of AI as foreseen in Section 2.2.[29]

27 For further discussion on this, see for example Kyle Miller and Andrew Lohn, “Onboard AI: Constraints and Limitations”, Center for Security and Emerging Technology, August 2023, https://doi.org/10.51593/2022CA008.

28 See for example Arslan Munir and Joonho Kong, “Artificial Intelligence and Data Fusion at the Edge”, IEEE Aerospace and Electronic Systems Magazine, 36, no. 7 (2021): 62–78.

29 Interview with an anonymous expert (14/09/2022).

3. Impact of AI in the Execution of Military Tasks

Alongside the mapping of AI capabilities to different military tasks is the need to understand what the impact is, or could be, of utilising AI to aid with these tasks. Discussions with experts demonstrated that the impact of AI was not necessarily linked to the type of task or broader functional area, but more with regard to the enhancement of AI more generally. Indeed, most of the impacts identified did not differ much or at all between functional areas—which makes sense as all functional areas are meant to occur in tandem during a military operation.

As such, this chapter first presents key elements emerging from expert discussions regarding the strength and opportunities that do or may emerge from the integration of AI capabilities into military tasks, before turning to the limitations and challenges. This chapter then concludes with a brief assessment of these strength and limitations.

3.1 Strengths and opportunities emerging from the integration of AI capabilities

'Big data' analysis

The ability of AI to improve data sorting and data analysis mechanisms could assist planning accuracy, situational awareness, more informed decision-making, and casualty reduction.[30] Increased ability to process large amounts of data could improve accuracy of assessments (as more data is available to make these) and could reduce unintended consequences. This type of capability could also be used to support and feed into early warning mechanisms for instances of conflicts, in addition to assisting during a military operation.

Speed of analysis and communication

With more data to be sorted and classified due to increased use of sensors collecting various types of data, the use of AI can lead to a faster assessment of such data than by human means, which could help increase the pace of analysis and thus decision-making. This has notably been raised with regards to C2, as the ability for AI to improve the use of information and assess large amounts of data could play a role in reducing uncertainty (such as regards, for example, terrain analysis). It should also be noted that increasing the speed of decision-making in upstream tasks may also have a knock-on effect and impact downstream tasks, including those relating to use of force. For example, more granular, multi-domain analysis of data and courses of action can enable or speed up subsequent decisions regarding target selection and target engagement. AI can also enable increased speed of communication along the chain of command, through its

30 Sayler, Artificial Intelligence and National Security.

abilities to synthesise and share information. This is also linked to improvement of knowledge-sharing between different entities, such as different units or even military branches, to ensure that decision-making entities have a more rounded understanding of the situation, as well as to help with collaboration.

Planning

AI can be employed to help with or complement strategic-level planning and the development of (better) tactics, such as through the development and use of scenarios and other gaming or red teaming capabilities. AI could additionally help detect deviations between the current situation and the plan and help calculate and present alternative solutions. The use of deep learning algorithms, for example, can extrapolate beyond the existing data and thus provide or inform unforeseen scenarios. Beyond training simulations, AI could also help identify an (or several) optimum plan when given a specific scenario, or provide a set of alternatives for action, thus aiding or complementing contingency planning.

Safety and security

The role AI can play with regard to improving cybersecurity and overcoming cyberthreats is one which transcends the military domain and is already much discussed. Discussions among experts noted that AI could also offer more control over the data, as the application of AI to cybersecurity could reduce the risk of data poisoning or interference. This, in turn, may lead to more confidence in both cyber and data security. Beyond the virtual sphere, AI could play a role in augmenting physical safety and security to a greater extent than would be possible through human or non-AI augmented means, such as by its support to training and simulation, its analysis of equipment wear and tear, preventative reconnaissance as well as personnel health (see task 17—Assess operational effectiveness of people and equipment). Additionally, through big data, AI could help assess linkages of digital and physical assets that must be protected or could be compromised. Identification of areas of weakness can thus serve as an (early) warning mechanism to take action.

Personnel efficiency

Experts argued that the use of AI could entail a reduction in the costs of logistics, due to fewer human errors. At the same time, experts noted that less human labour would be needed for certain tasks, enabling task optimisation for personnel away from ancillary tasks. The role of AI in providing support in tactical planning, as noted above, could also enable smaller staff at the battalion and brigade levels.

3.2 Limitations and challenges emerging from the integration of AI capabilities

For each strength and opportunity put forward regarding the use of AI in upstream tasks, however, a number of limitations and challenges emerge as well. The issues raised fall in three main categories: externalities that affect the proper use of AI; concern about AI in and of itself; and negative impacts resulting from the use of AI, with the majority of the issues centred around this third broad category. Many of these reflections are discussed in existing literature regarding the application of AI to weapon systems and specifically the use of lethal force. This demonstrates that such issues therefore have a broader remit, but also that these remain extant concerns with regard to the application of AI more generally, and particularly so regarding AI for military purposes.

Lack of (good quality) data

Data issues can hamper the efficiency and accuracy of AI algorithms from training all the way to use in operational contexts. In such instances, the issue goes beyond AI itself, and points to a system-wide challenge where use of AI is hampered through the lack of broader structures. This includes, but is not limited to, limited training datasets, which can impact the ability of AI algorithms to operate in real-world settings; a lack of coherence or fragmented data, because data capture methods, such as via sensors, are too few; poor data management systems whereby data-sharing is hampered or there is poor data hygiene. Issues may also emerge if data collection methods are not able to keep up with fast-paced changes happening on the ground. In cases such as these, new information can be missed or be delayed, resulting in wrong assessments or incomplete situational understandings. Finally, the use of AI to help with scenarios and simulations such as wargaming could run the risk of mirroring, whereby the AI system is only capable of repeating known information but cannot provide new insights.

'Black box' decision-making

The issue of the lack of transparency of AI decision-making is oft discussed, albeit mainly with regard to autonomy in weapon systems.[31] Yet this issue was also brought up in discussions focused on non-lethal AI capabilities. Indeed, a lack of understanding of how an AI has come to its conclusions and how it has decided whether or not something is of importance also has a large impact when discussing the application of AI to aid with the identification of targets, CDE calculations, or even undertaking preventative maintenance of military equipment. Even when weapons are not a direct part of the equation, the inability of AI to explain how it achieved its results can have unintended consequences, and even more so when upstream tasks impact on the decision to use weapons or weapon-bearing equipment. As noted by experts, the 'black box' issue can also make it harder to contest decisions made

31 See for example Svenmarck et al., Possibilities and Challenges for Artificial Intelligence in Military Applications; YuLong Zhang et al., "Application of Artificial Intelligence in Military: From Projects View", 2020 6th International Conference on Big Data and Information Analytics (BigDIA), Shenzhen, China, 2020: 113–116.

by AI which cannot explain itself—leading alternatively to either distrust or overreliance.[32]

Meaningful human control

The issue of human control is pervasive across all tasks, even those deemed to have a 'low-risk' impact. Indeed, even if the issue is not deciding on a target or whether to pull a trigger, questions remain around the extent to which analysis, the conception of pathways for action, or tactics could and should be done by AI alone—and therefore if and when to include meaningful human control. More broadly, there is a question around how an assessment of whether there needs to be meaningful human control for specific tasks is undertaken. In other words, for which tasks are there greater ethical, legal, or other imperatives for human control, and for which tasks may this be seen as hampering the efficacy of AI? Indeed, all military tasks are important and pertinent to the process or a military operation as a whole; but the question remains as to which may be seen as being more acceptable of errors from AI than others—if any. Overall, discussions regarding meaningful human control may be just as relevant to upstream tasks as to downstream ones.

Reasoning capabilities

Linked to the point on the 'black box' nature of AI decision-making is the fact that AI does not reason as humans do—but neither do humans reason like AI, given we can draw upon long-term experience and are also impacted by emotional triggers.[33] Data thus may not have the same meaning for humans and AI, as regards its content or importance, with the analysis therefore not being the same—or even erroneous, which can undermine trustworthiness. This is exemplified by the issue of 'hallucinations', which is particularly relevant to LLMs. Hallucinations refer to LLMs inventing facts due to misinterpreting the data, making incorrect associations between different data, or using poisoned data, the latter of which is discussed in more detail below.[34] Additionally, unpredictability of human behaviour may not be factored in by AI, particularly in regard to simulation and early warning mechanisms which are based on assumptions and calculations of possibilities of human actions under uncertainty in partially observed, high-dimensional, real-world scenarios intractable to machine modelling.

AI as a vulnerability

While AI can help improve cybersecurity, as noted in Section 3.1, it can also be a vulnerability. In particular, AI can become the victim of manipulation through adversarial attacks; it could also be fed (un)intentionally false or even poisoned data; it could also be subverted by hackers. Use of AI can also augment

---

32 It should however be noted that there are efforts to make AI decision-making less opaque, and research is ongoing in this area; see for example Angie Boggust et al., "Shared Interest: Measuring Human-AI Alignment to Identify Recurring Patterns in Model Behavior", In CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.

33 Taylor Webb, Keith J. Holyoak and Hongjing Lu, "Emergent Analogical Reasoning in Large Language Models", Nat Hum Behav (2023), https://doi.org/10.1038/s41562-023-01659-w.

34 Since the release of ChatGPT, a number of hallucination examples have emerged; see for example Tiffany Hsu, "What Can You Do When A.I. Lies About You?", New York Times, August 7, 2023, https://www.nytimes.com/2023/08/03/business/media/ai-defamation-lies-accuracy.html.

opportunities for adversaries to exploit weaknesses.[35] The impact of such vulnerability may not be immediate, and its effects can vary. Feeding false information or analyses can range from impacting the efficiency of a military operation—such as by slowing down logistical operations or affect analysis upon which life-or-death decisions are made.

Excessive reliance

Overreliance on AI could lead to only considering or gathering data to feed AI systems, or thinking only of inputs in terms of what is needed by an AI. This can therefore skew or bias data collection efforts—with an impact on the outputs. Excessive reliance on AI may also lead to ignoring or disregarding possible shortfalls of the technology; for example, overestimating what AI can achieve, and seeking to use it for issues beyond its capacity, or not vetting adequately the data that is fed to the system. Overreliance could also lead to a loss of context and nuance due to over-synthesis of information by AI, where culture, context, emotions, and unwritten social norms may not be adequately recognised. Incorporating AI into certain activities may also lead to changes in how task allocation is considered. Specifically, experts noted that use of AI may bring in more rigid thinking or boundaries around what machines can do over humans, or in terms of respective strengths. This could in turn affect flexibility and agility, particularly during fast-moving operations.

Skills degradation

Linked to the point above, another facet of AI use is the potential impact on human knowledge and skills. It has, for example, been noted that automation in aircraft piloting can lead to a degradation, if not loss, of skill;[36] the same argument has been made regarding the use of AI in the military context.[37] Notably, experts mentioned a potential for paucity of planning capability and skills among personnel, if such tasks become primarily the remit of AI. In this context, it should be highlighted that AI is not only dependent on data to function, but also electricity and computing power; in the loss of this, military operations may be weakened simply due to personnel no longer being accustomed or even trained to undertake certain tasks where AI use has become more significant. However, it remains at this stage difficult to understand how humans may react to the application of AI capabilities to different military tasks. Indeed, such reactions may not be homogenous, differing depending on individual characteristics such as age or background, how AI is embedded in operations, or the overarching military culture.

Impact to operational tempo

This is another argument which has been

35 Sayler, Artificial Intelligence and National Security.

36 See for example Andreas Haslbeck and Hans-Juergen Hoermann, "Flying the Needles: Flight Deck Automation Erodes Fine-Motor Flying Skills Among Airline Pilots", Human Factors, 58, no. 4 (2016): 533–545, https://doi.org/10.1177/0018720816640394; and Stephen M. Casner at al., "The Retention of Manual Flying Skills in the Automated Cockpit", Human Factors, 56, no. 8 (2014): 1506–1516, https://doi.org/10.1177/0018720814535628.

37 Most notably within France's Ministry of the Armed Forces' AI Task Force report: Ministry of the Armed Forces, Artificial Intelligence in Support of Defence, 2019, https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf.

raised with regard to the use of AI in military operations more generally,[38] with experts contributing to this study also mentioning this point with regard to the integration of AI capabilities to tasks not directly related to weapons use. In a similar vein to the existing argument, there is a fear that utilizing AI would generate a faster operational tempo, eventually exceeding human ability to keep up with events. However, experts also noted that this may depend on the context; for example, situations of deliberate targeting versus battlefield dynamics are of different scope and complexity, thereby demonstrating that the impact of AI is not necessarily 'one size fits all'.

(Lack of) harmonisation

Beyond the elements outlined above, there are also challenges raised with regard to military operations conducted jointly by different actors.[39] While joint operations currently need to ensure commonalities from doctrine to planning and execution, the addition of AI will also necessitate a common approach. Yet, the acceptability and use of AI may differ among actors—in terms of application areas, data needs, algorithmic differences (which could lead to different outputs), recommendations, analyses, and more. This begs the question as to how these differences will be managed, and how the use of AI would be harmonised—let alone accepted—depending on the appetite of different actors. Will it make it harder for actors to work together? Or in such cases, will actors have to forego the use of AI entirely, unless a solution is found?

Unknown impact

While we can theorise over the challenges AI may bring, as well as weaknesses its use can expose, the fact is that the extent and reality of its current and future applications, and therefore impact, still remains unknown. The use of AI may bring about ethical issues or concerns previously unforeseen around the reliability of mission planning. Additionally, the handover of control to AI, even for tasks deemed 'low risk'—such as data classification or summarisation—may result in unforeseen consequences, from whether and how weapons are used, or the pace and scale of a conflict overall.

3.3 Assessment and discussion regarding perceived strengths and challenges

Interestingly, some of the reflections on the 'strengths' of AI demonstrate that **the expectations assigned to AI may not be realistic in terms of the anticipated technological progress but also the realities of AI integration into operations**. For example, one of the perceived strengths of AI is that it can increase the speed of communication along the chain of command. But the few capabilities relevant for that particular sub-task (14—Dissemination of information across the chain of command and control) would not be so advanced as to necessarily increase the speed of communication across the entire chain of command. And while

38 See for example Scharre, "Military Applications of Artificial Intelligence"; Sayler, Artificial Intelligence and National Security; Morgan et al., Military Applications of Artificial Intelligence.

39 Also discussed further in Lin-Greenberg, "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making".

there is the anticipation that integration of AI would result in better synthesis or analysis of data, this does not take into account possible limitations around the adoption of AI, both from a technical standpoint as well as from the perspective of military technology approval and adoption.

Related to the above, **the expectations placed on AI are very high for certain tasks—and perhaps unrealistic, at least for the near-term future**. While AI does, in some regards, offer capabilities that exceed those of humans, there are still barriers, notably around limitations of AI itself, or the amount of data available, both in terms of training but also in practice. For example, there is an expectation that AI will be more accurate in its analysis of data than human-led efforts in the area, or able to develop superior tactics. However, beyond assuming AI progresses past narrow AI, this is also dependent on the quality and quantity of data that systems will have access to, and the infrastructure readiness of equipment.

Overall, remaining aware of the limitations of what AI can offer and not overpromising its capabilities is important. While there have been calls for caution around the anthropomorphism of AI,[40] similarly we should be careful not to mistakenly attribute omniscient abilities either, on the basis that AI is better able to deal with (big) data compared to humans.

Additionally, inferences on the impact of AI on the operational tempo is a recurrent one; however, unless humans are completely removed from all these processes, ultimately the rapidity of **the operational tempo will still be determined by humans and their roles in the observe, orient, decide, act (OODA) loop**. In other words, we still have the possibility of controlling the tempo, as well as the use of AI.

Further to this, other conundrums remain:

- The more 'advanced' AI capabilities which would enable improved analysis, predictions of behaviour, or evolutions of certain scenarios are also the areas where the lack of transparency and explainability is the greatest concern. Therefore, questions remain around what level of explainability and transparency will be deemed sufficient to use AI and whether this will differ depending on the military task.
- This also begs the question of how is a task deemed 'low risk' versus 'high risk'. What related issues may this bring in terms of risk acceptance simply because of where a task may sit—in other words, further upstream or downstream—when each task is also important in its own right?
- Finally, some of the limitations demonstrated by AI—such as vulnerability to poisoned or false data—are inherent for humans too. How is the acceptable error rate for humans versus machines decided? While some of these questions are discussed in debates regarding the use of AI in target selection and target engagement, there is nonetheless merit in widening the discussion to a wider set of military tasks, particularly given the impact upstream tasks, such as those featured in Section 2.2, have on downstream tasks.

---

40 See for example David Watson, "The Rhetoric and Reality of Anthropomorphism in Artificial Intelligence", Minds & Machines 29, 417–440 (2019). https://doi.org/10.1007/s11023-019-09506-6; Arleen Salles, Kathinka Evers and Michele Farisco, "Anthropomorphism in AI", AJOB Neuroscience, 11, no. 2 (2020): 88–95, https://doi.org/10.1080/21507740.2020.1740350.

4. Conclusions

In conclusion, this report demonstrates that there is a significant number of both current and near-future AI capabilities that map against a wide range of upstream military tasks. Yet, despite the existence of such AI capabilities, there have been fewer discussions at the multilateral level in regard to the application of AI to upstream tasks compared to downstream tasks, which notably include target selection and target engagement. This gap is particularly important given the recent rapid advances in generative AI, which are increasingly capable of seemingly cognitive roles. However, when examining the strengths and limitations identified regarding the impact of AI on these upstream military tasks, we find that there are many similarities with the discussion of downstream tasks.

While AI applications in upstream military tasks may not have the same repercussions in terms of conflict escalation and loss of life as downstream tasks, they would nonetheless have an impact on the conduct of a military operations and overall decision-making. This however raises the question as to whether the operationalisation of AI in upstream tasks may not be, in some cases, less controversial for decision makers than their inclusion in downstream tasks. This may be due to the inclusion of AI being less visible in upstream compared to downstream tasks—which may be a factor making the integration of AI in upstream tasks more likely. Yet, uncertainty as to not only what capabilities exist now and in the future but particularly whether and how they may be integrated and by whom can be a source of insecurity and also instability.

This report also suggests that, at the national level, it is important for States to understand the broad range of possible applications of AI in the military domain, and take this range of applications into account when designing national defence AI strategies, policies, and guidelines. It would also make sense to take this broader approach when discussing AI for military purposes in multilateral forums, to include reflections on AI integration among all military tasks. This is also of particular relevance with regard to discussions on AI governance and responsible AI, which would need to be conscious of not only focusing on AI applications to target selection and target engagement but also across all tasks relevant to a military operation.

References

Afina, Yasmin. "Intelligence is dead: long live Artificial Intelligence". Chatham House. July 14, 2022. https://www.chathamhouse.org/2022/07/intelligence-dead-long-live-artificial-intelligence.

Boggust, Angie, Benjamin Hoover, Arvind Satyanarayan and Hendrik Strobelt. "Shared Interest: Measuring Human-AI Alignment to Identify Recurring Patterns in Model Behavior". In CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.

Casner, Stephen M., Richard W. Geven, Matthias P. Recker, Jonathan W. Schooler. "The Retention of Manual Flying Skills in the Automated Cockpit", Human Factors, 56, no. 8 (2014): 1506–1516, https://doi.org/10.1177/0018720814535628.

Ekelhof, Merel and Giacomo Persi Paoli. The Human Element in Decisions about the Use of Force. 2020. UNIDIR: Geneva. https://unidir.org/publication/human-element-decisions-about-use-force.

Galán, José Javier, Ramón Alberto Carrasco, and Antonio LaTorre. "Military Applications of Machine Learning: A Bibliometric Perspective". Mathematics, 10, no. 1397 (2022). https://doi.org/10.3390/math10091397.

Government of the Netherlands. "Call to Action on Responsible Use of AI in the Military Domain". February 16, 2023. https://www.government.nl/ministries/ministry-of-foreign-affairs/news/2023/02/16/reaim-2023-call-to-action.

Government of the Netherlands. "REAIM Call to Action". February 16, 2023. https://www.government.nl/documents/publications/2023/02/16/reaim-2023-call-to-action.

Haslbeck, Andreas and Hans-Juergen Hoermann. "Flying the Needles: Flight Deck Automation Erodes Fine-Motor Flying Skills among Airline Pilots". Human Factors, 58, no. 4 (2016): 533–545. https://doi.org/10.1177/0018720816640394.

Hoffman, Wyatt and Heeu Millie Kim. Reducing the Risks of Artificial Intelligence for Military Decision Advantage. Center for Security and Emerging Technology. March 2023.

Horowitz, Michael C. "Artificial Intelligence, International Competition, and the Balance of Power." Texas National Security Review, 1, no.3 (2018): 36–57. https://doi.org/10.15781/T2639KP49.

Hsu, Tiffany. "What Can You Do When A.I. Lies About You?". New York Times, August 7, 2023. https://www.nytimes.com/2023/08/03/business/media/ai-defamation-lies-accuracy.html.

Hunter, Cameron and Bleddyn E. Bowen. "We'll never have a model of an AI major-general: Artificial Intelligence, command decisions, and kitsch visions of war". Journal of Strategic Studies (2023), https://doi.org/10.1080/01402390.2023.2241648.

Lin-Greenberg, Erik. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making". Texas National Security Review, 3, no. 2 (2020): 56–76. http://dx.doi.org/10.26153/tsw/8866.

Martínez-Plumed, Fernando, Emilia Gómez and José Hernández-Orallo. "Futures of Artificial Intelligence through Technology Readiness Levels". Telematics and Informatics, 58 (2021). https://doi.org/10.1016/j.tele.2020.101525.

Masuhr, Niklas. AI in Military Enabling Applications. CSS Analyses in Security Policy No. 251. October 2019. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse251-EN.pdf.

Maxwell, Paul. "Artificial Intelligence is the Future of Warfare (Just Not in the Way You Think)". April 20, 2020. https://mwi.usma.edu/artificial-intelligence-future-warfare-just-not-way-think/.

Miller, Kyle and Andrew Lohn. "Onboard AI: Constraints and Limitations". Center for Security and Emerging Technology. August 2023. https://doi.org/10.51593/2022CA008.

Ministry of the Armed Forces, Artificial Intelligence in Support of Defence, 2019, https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf.

Morgan, Forrest E., Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima and Derek Grossman. Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World. Santa Monica: RAND Corporation. 2020.

Report of the 2023 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, CCW/GGE.1/2023/2, May 23, 2023, https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_2_Advance_version.pdf.

Salles, Arleen, Kathinka Evers and Michele Farisco. “Anthropomorphism in AI”. AJOB Neuroscience, 11, no. 2 (2020): 88–95. https://doi.org/10.1080/21507740.2020.1740350.

Samoili, Sofia, Montserrat López-Cobo, Emilia Gómez, Giuditta De Prato, Fernando Martínez-Plumed, Blagoj Delipetrev. AI Watch Defining Artificial Intelligence: Towards an Operational Definition and Taxonomy of Artificial Intelligence. Luxembourg: European Union, 2020. https://publications.jrc.ec.europa.eu/repository/handle/JRC118163.

Sayler, Kelley M. Artificial Intelligence and National Security. Congressional Research Service Report. November 10, 2020. https://sgp.fas.org/crs/natsec/R45178.pdf.

Scharre, Paul. “Military Applications of Artificial Intelligence: Potential Risks to International Peace and Security”. In The Militarization of Artificial Intelligence, edited by Stanley Centre for Peace and Security, UNODA, Stimson. 2020.

Svenmarck, Peter, Linus Luotsinen, Mattias Nilsson and Johan Schubert. Possibilities and Challenges for Artificial Intelligence in Military Applications. NATO. 2018.

UN Web TV. “Artificial Intelligence: Opportunities and Risks for International Peace and Security - Security Council, 9381st Meeting”. July 18, 2023. https://media.un.org/en/asset/k1j/k1ji81po8p.

United Nations. “A New Agenda for Peace: Our Common Agenda Policy Brief 9”. 2023. https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf.

United Nations. “Guterres Calls for AI ‘that Bridges Divides’, Rather than Pushing Us Apart”. July 18, 2023. https://news.un.org/en/story/2023/07/1138827.

United Nations. “Multistakeholder Advisory Body on Artificial Intelligence”. https://www.un.org/techenvoy/content/artificial-intelligence.

Watson, David. “The Rhetoric and Reality of Anthropomorphism in Artificial Intelligence”. Minds & Machines 29, 417–440 (2019). https://doi.org/10.1007/s11023-019-09506-6.

Webb, Taylor, Keith J. Holyoak and Hongjing Lu. “Emergent Analogical Reasoning in Large Language Models”. Nature Human Behaviour (2023). https://doi.org/10.1038/s41562-023-01659-w.

Zhang, YuLong, ZiJie Dai, LongFei Zhang, ZhengYi Wang, Li Chen and YuZhen Zhou. “Application of Artificial Intelligence in Military: From Projects View.” 2020 6th International Conference on Big Data and Information Analytics (BigDIA), Shenzhen, China, 2020: 113–116.

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

UNIDIR

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG