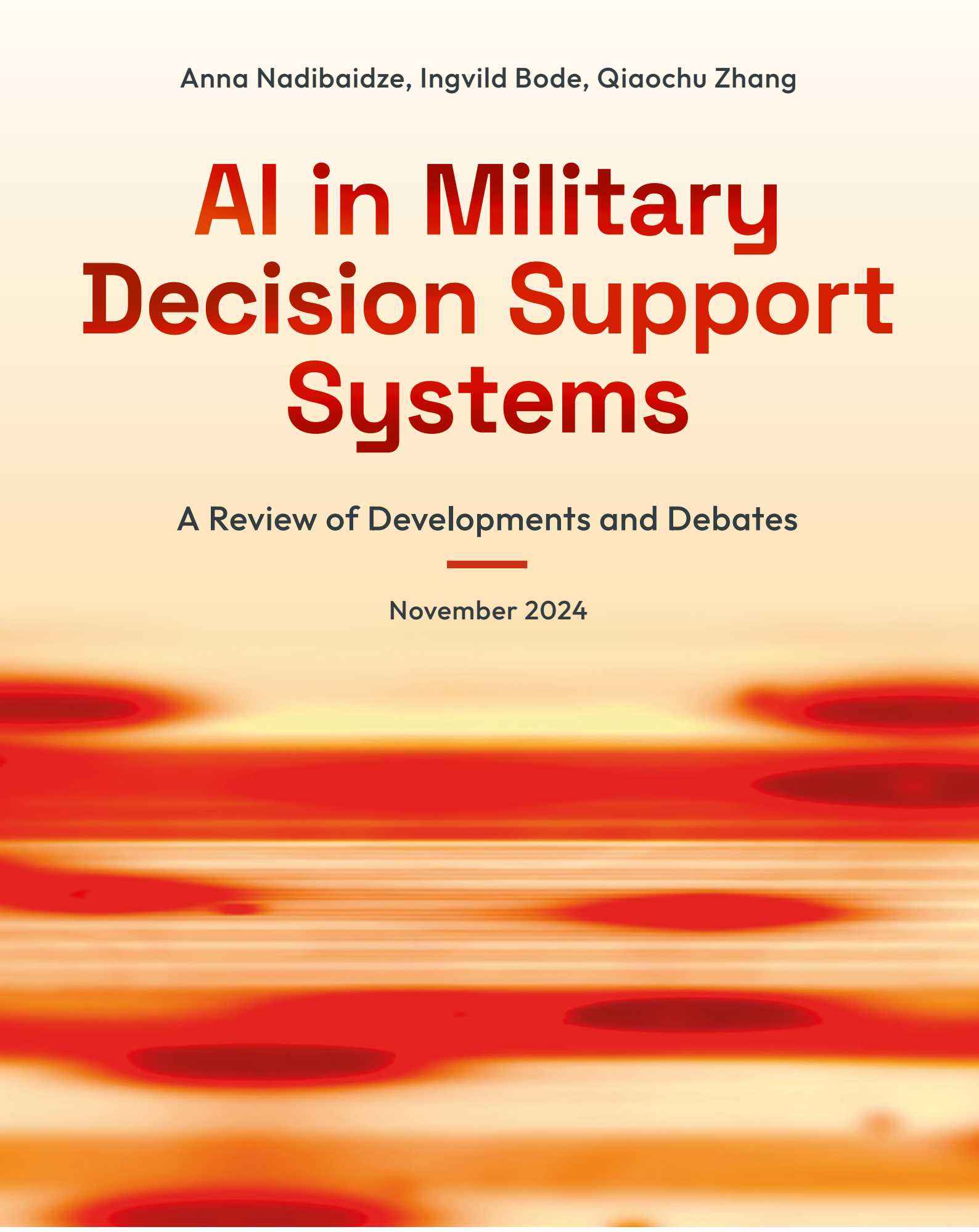
Anna Nadibaidze, Ingvild Bode, Qiaochu Zhang

AI in Military Decision Support Systems

A Review of Developments and Debates

November 2024



CENTER FOR WAR STUDIES

Published by the Center for War Studies, University of Southern Denmark, Campusvej 55, Odense M 5230, Denmark

AutoNorms

SDU

About the Center for War Studies

The Center for War Studies (CWS), established at the University of Southern Denmark in 2012, brings together academics from political science, law, history, and cultural studies to contribute to the major debates on the past, present, and future of war, as well as its impact on societies. We strive for interdisciplinary research that is relevant to policymakers and the society at large. We aim to contribute to ongoing debates on war and peace by illuminating their multiple dimensions. Through research excellence and societal relevance, we advance the understanding of the fundamental issue of war and peace. For more information about the CWS and its researchers, see www.sdu.dk/en/forskning/forskningsenheder/samf/cws.

Funding

European Research Council
Established by the European Commission

Research for this report was supported by funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 852123, the AutoNorms project).

About the AutoNorms project

AutoNorms is an international research project funded by the ERC and hosted by the CWS at the University of Southern Denmark. Led by Professor Ingvild Bode, the project explores how the development and use of autonomous weapon systems and other forms of weaponised AI change international norms on the use of force. AutoNorms develops a new theoretical approach to study how norms, understood as standards of appropriateness, manifest and change in practices. It investigates norm emergence and change across four contexts of practices (military, transnational political, dual-use, and popular imagination) in four states (China, Japan, Russia, and the United States). For more information about AutoNorms, see www.autonorms.eu.

Acknowledgements

The authors are grateful to Marta Bo, Laura Bruun, Anna Rosalie Greipl, Klaudia Klonowska, and Tom Watts for providing invaluable feedback for previous drafts of this report.

How to cite this report

Anna Nadibaidze, Ingvild Bode, and Qiaochu Zhang. (2024). *AI in Military Decision Support Systems: A Review of Developments and Debates* (Odense: Center for War Studies).

Cover image credit: Vidsplay on StockSnap

Contents

Executive summary

Reports from war zones underline that artificial intelligence (AI) technologies are increasingly integrated into military decision-making. Armed forces are developing and employing AI-based systems as part of the complex and multi-layered process of decision-making that relates to the use of force. Such uses of AI in security and warfare are associated with opportunities and challenges which deserve further scrutiny. To contribute to ongoing discussions on AI-based decision support systems (AI DSS), **this report provides a review of 1) the main developments in relation to AI DSS (at the time of writing in September 2024), focusing on specific examples of existing systems; and 2) the main debates about opportunities and challenges related to various uses of AI DSS, with a focus on issues of human-machine interaction in warfare.**

While acknowledging that the development of AI DSS is a global, apparently persistent, and long-standing trend, the report focuses on mapping and analysing specific examples as part of three main, most recently reported, cases: **the United States' Project Maven, the Russia-Ukraine war (2022-), and the Israel-Hamas war (2023-).** We treat these cases as indicative of possible uses of AI DSS, as well as representative of some of the varied opportunities and challenges associated with the integration of AI into military decision-making. Potential opportunities of AI DSS include increased speed, scale, and efficiency of decision-making which might lead to strategic or humanitarian advantages in a battlefield context. With increased speed and scale, however, also come various risks and concerns around how humans interact with AI DSS in military decision-making on the use of force.

This report highlights how challenges raised by AI DSS are often linked to human-machine interaction and the distributed agency between humans and machines, which raises legal, ethical, and security risks. These include concerns regarding non-compliance with international (humanitarian) law, the erosion of moral agency, and unintended consequences. While the assumption for AI DSS is that humans (will) remain the ultimate decision-makers on the use of force, in certain situations **there are risks of humans not exercising sufficient levels of involvement and critical thinking in the targeting process**. Ultimately, opportunities and challenges associated with AI DSS also depend on contexts of use and how humans interact with machines within those contexts.

To develop these discussions further, we recommend that stakeholders in the global debate about military applications of AI focus on questions of human-machine interaction and work towards addressing the challenges associated with distributed agency in warfare. This concern spans across discussions on AI DSS and AI in weapon systems. Ways forward in the debate include **1) ensuring a qualitatively high level of human judgement and critical assessment of algorithmic outputs via practical guidance and training** and **2) pursuing multistakeholder and cross-disciplinary global governance initiatives to sustain and strengthen the role of humans in the use of force, including via legally binding norms and/or a bottom-up standard-setting process**.

1 Introduction

Accounts of armed forces integrating artificial intelligence (AI) technologies into their decision-making processes on the use of force have been growing. Such reports are coming from war zones around the globe, including the latest Israel-Hamas war (2023-) and the Russia-Ukraine war (2022-). The employment of computerized and automated tools in targeting decision-making is not a new phenomenon. However, many militaries are expanding the scope and speed of incorporating more complex data-driven techniques into the processes of determining courses of action, including when it comes to the use of force. These developments raise questions about the changing roles played by humans and machines, or human-machine interaction, in warfare.

The global debate about AI in the military domain, including at the United Nations (UN) Group of Governmental Experts on emerging technologies in the area of lethal autonomous weapon systems (GGE on LAWS), has long focused on AI and autonomy at the tail end of the targeting process—in other words, in weapon systems. This focus is evidenced by extensive policy, academic, and regulatory discussions on autonomous weapon systems (AWS), defined as weapon systems which, once activated, select and apply force to targets without human intervention.[1]

The dominant focus on AWS has overshadowed multiple other uses of AI-based technologies in the military domain which might be more influential than autonomy in weapon systems

However, the dominant focus on AWS has overshadowed multiple other uses of AI-based technologies in the military domain which might be more influential than autonomy in weapon systems.[2] The development of AI technologies designed to assist humans in military decision-making on the use of force is equally important to examine in detail. As recent events and discussions highlight, AI-based decision support systems (AI DSS) used to recognize patterns in substantial amounts of data, predict scenarios, or recommend possible courses of action, deserve greater attention in the context of investigating AI technologies in security and warfare.[3]

This report contributes to ongoing debates on AI DSS by reviewing main developments and discussions surrounding these systems and their reported uses. It takes stock of what is known about AI DSS in military decision-making on the use of force, including in ongoing war zones around the globe. Section 2 provides a brief overview of the roles that AI DSS can play in use-

1 International Committee of the Red Cross, "ICRC Position on Autonomous Weapon Systems," May 12, 2021, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

2 Merel A.C. Ekelhof, "AI Is Changing the Battlefield, but Perhaps Not How You Think: An Analysis of the Operationalization of Targeting Law and the Increasing Use of AI in Military Operations," in *Research Handbook on Warfare and Artificial Intelligence*, ed. Robin Geiß and Henning Lahmann (Cheltenham: Edward Elgar, 2024), 162; Anthony King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," *Journal of Global Security Studies* 9, no. 2 (2024): https://doi.org/10.1093/jogss/ogae009; Shashank Joshi, "How AI Is Changing Warfare," *The Economist*, June 20, 2024, https://www.economist.com/briefing/2024/06/20/how-ai-is-changing-warfare.

3 ICRC and Geneva Academy, *Expert Consultation Report on AI and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts* (Geneva: ICRC, 2024); Arthur Holland Michel, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision-Making* (Geneva: ICRC, 2024); Weng Zhou and Anna Rosalie Greipl, "Artificial Intelligence in Military Decision-Making: Supporting Humans, Not Replacing Them," *ICRC Humanitarian Law & Policy Blog*, August 29, 2024, https://blogs.icrc.org/law-and-policy/2024/08/29/artificial-intelligence-in-military-decision-making-supporting-humans-not-replacing-them/; Taylor Kate Woodcock, *Decision-Support Systems and Human-Machine Interaction: REAIM Breakout Session* (The Hague: Asser Institute, 2023).

of-force decision-making. Section 3 reviews main developments that we treat as indicative of trends in AI DSS in the military domain. It focuses on three concrete empirical cases, namely the United States (US)' Project Maven initiative, as well as systems reportedly used in the Russia-Ukraine war (2022-) and the Israel-Hamas war (2023-). Section 4 discusses opportunities and challenges associated with these developments, drawing inspiration from ongoing debates in the media and expert communities. The report concludes with some recommendations on potential ways forward to address the challenges discussed and with some questions raised by AI DSS that deserve further attention in the global debate on AI in the military domain.

This report aims to provide an empirically rich springboard to pursue deeper discussions on the issue of AI DSS in the military

1.1 Methodology

This report is based on an extensive review of sources including academic scholarship, policy reports, media articles, and online publications. This review was complemented by observations and discussions that the authors gained in various settings, such as meetings and events.[4]

At the same time, the report involves data limitations. For instance, it is often challenging to pinpoint the exact technologies integrated into the systems mentioned in section 3. Moreover, without privileged access it is difficult to identify the precise role of AI DSS in a particular use-of-force situation. However, these challenges do not prohibit us from drawing important insights and highlighting key aspects of AI DSS in the military domain. The information presented in this report should be seen as indicative of trends rather than as a definitive description. With this report, we therefore aim to provide an empirically rich springboard to pursue deeper discussions on the issue of AI DSS in the military.

1.2 A note on terminology

The term 'AI' is difficult and controversial to define, not least because it is used as an umbrella term for various processes, fields of study, or even ideologies.[5] In this report, we treat this term as a reference to "computational techniques that extract statistical patterns from large datasets based on the adjustment of relevant parameters according to either internally or externally generated feedback".[6] The term 'AI' may encompass algorithms relying on machine learning, deep learning, and neural networks, which are described as data-driven techniques because they are capable of "adapting to their environment and improving performance based on past experiences and training rather than a pre-programmed model of the world".[7] This report, therefore, does not focus on automated processes or computerized systems which have been part of military decision-making for decades.[8] Rather, it explores developments and implications in relation to more recent trends in the sphere of 'learning' algorithms and

4 Relevant events include the UN GGE on LAWS meetings (6-10 March 2023 and 4-8 March 2024, Geneva), the seminar "Smart War? Promises and Pitfalls of Military AI" held at the Royal Danish Defence College (2 May 2024, Copenhagen), the Vienna Conference on Autonomous Weapons Systems (29-30 April 2024, Vienna), and the Responsible AI in the Military Domain Summits (15-16 February 2023, The Hague and 9-10 September 2024, Seoul).

5 Ingvild Bode and Tom Watts, *Loitering Munitions and Unpredictability: Autonomy in Weapon Systems and Challenges to Human Control* (Odense & London: Center for War Studies & Royal Holloway Centre for International Security, 2023), 13; Arthur Holland Michel, *Recalibrating Assumptions on AI: Towards an Evidence-Based and Inclusive AI Policy Discourse* (London: Chatham House, 2023).

6 Lucy Suchman, "The Uncontroversial 'Thingness' of AI," *Big Data & Society* 10, no. 2 (2023): 2, https://doi.org/10.1177/20539517231206794.

7 Vincent Boulanin and Maaike Verbruggen, *Mapping the Development of Autonomy in Weapons Systems* (Stockholm: Stockholm International Peace Research Institute, 2017), 91; ICRC and Geneva Academy, *Expert Consultation Report on AI*, 8.

8 Holland Michel, *Decisions, Decisions, Decisions*, 55-59.

systems running on models that operate like 'black boxes', where the process leading from input to output is often challenging to understand.[9]

Further, terms such as 'support', 'aid', or 'assist' deserve a note of caution because they assume that using AI-based systems would inherently support the human role in decision-making in a positive way, for instance by providing information that would advance human efficiency in taking a course of action, thereby strengthening the exercise of human agency. This appears to *a priori* assume that AI DSS have positive, zero-sum outcomes for human decision-makers in a military context. However, there are also many instances where the use of AI-based systems appears to undermine or diminish, rather than advance, help, and positively impact the role of the human (see section 4). In this report, we refer to the term AI DSS given that it is commonly used in the debate and the literature. At the same time, we do not automatically assume the 'supportive' function of these systems.

9 Boulanin and Verbruggen, *Mapping the Development of Autonomy in Weapons Systems*, 17; Arthur Holland Michel, *The Black Box, Unlocked* (Geneva: United Nations Institute for Disarmament Research, 2020).

2 AI in Military Decision-Making on the Use of Force

2.1 Decision support systems (DSS) in the military domain

Decision support systems (DSS) can be defined as "model-based set[s] of procedures for processing data and judgements to assist decision-makers situated at different levels in the chain of command to solve semi-structured and unstructured decision tasks".[10] As this broad definition indicates, military decision-making covers a broad array of different tasks and domains from maintenance and logistics, to personnel and weapon management, and up to the use of force.[11] This report focuses on military decision-making related to targeting and the use of force.

Targeting can be thought of as the application of capabilities (such as weapons) against targets (such as people or objects) to "generate effects in order to achieve specific objectives".[12] Targeting is part of the use of force, a process that consists of accomplishing a mission while ensuring compliance with legal obligations and using resources in accordance with the broader purpose(s) set by the political leadership. Use-of-force decision-making can be described as an "iterative logical planning method to select the best course of action for a given battlefield situation" which is typically conducted at different levels and involves various actors.[13] This is a complex exercise that may last for different periods of time and comprise multiple stages such as designating, identifying, analysing, tracking, vetting, and approving targets.[14] These steps usually occur in a cycle and require processing large amounts of information. Militaries can potentially use DSS as part of each step and task in this networked process.

DSS are intended to assist humans with tasks such as identifying adverse forces and weaponry, as well as evaluating their capabilities, features, and vulnerabilities. They can be used to gather, process, and analyse data such as geographic information, communications, biometric data, signatures, audio signals, and satellite imagery. Human commanders can employ DSS to visualize

10 Elena Susnea, "Decision Support Systems in Military Actions: Necessity, Possibilities and Constraints," *Journal of Defense Resources Management* 3, no. 2 (2012): 132.

11 ICRC and Geneva Academy, *Expert Consultation Report on AI*, 7–8.

12 Paul A.L. Ducheine, Michael N. Schmitt, and Frans P.B. Osinga, "Introduction," in *Targeting: The Challenges of Modern Warfare*, ed. Paul A.L. Ducheine, Michael N. Schmitt, and Frans P.B. Osinga (The Hague: T.M.C. Asser Press, 2016), 2.

13 Herwin Meerveld et al., "The Irresponsibility of Not Using AI in the Military," *Ethics and Information Technology* 25, no. 1 (2023): 14, https://doi.org/10.1007/s10676-023-09683-0.

14 Merel Ekelhof and Giacomo Persi Paoli, *The Human Element in Decisions about the Use of Force* (Geneva: United Nations Institute for Disarmament Research, 2020); Merel A.C. Ekelhof, "Lifting the Fog of Targeting: 'Autonomous Weapons' and Human Control through the Lens of Military Targeting," *Naval War College Review* 71, no. 3 (2018): 67–100.

specific information on maps, consider various factors or contingencies, develop and evaluate military strategies, assess the likelihood of scenarios and the feasibility of responses, allocate resources, or calculate the potential effects of deploying specific weapons (sometimes referred to as weaponeering), among others.

Militaries have used varieties of DSS and computerized tools in processes related to the use of force for decades. For instance, in the context of air defence systems, DSS can assist with detecting objects (and potential targets) in the sky.[15] Traditional DSS are based on automation and therefore follow pre-programmed sequences of actions.[16] Automated DSS typically integrate rule-based algorithms that consistently yield the same output for a given input. As an illustration, decision-makers can use DSS to calculate the range of an aircraft by employing a straightforward formula that includes variables such as fuel levels and speed.[17] The use of automated DSS therefore precedes the advent of AI.

2.2 AI technologies in military DSS

The integration of AI and machine learning technologies into DSS is said to 'enhance' these systems by making them more adaptable to varying environments through 'learning' from large volumes of data. Based on technological developments in the sphere of AI (broadly defined), militaries actively develop AI DSS for a variety of purposes. They plan to integrate these systems at different levels of decision-making in warfare, i.e., the strategic, tactical, and operational levels, and activities that relate to the use of force, such as intelligence, surveillance, and reconnaissance (ISR), command and control, and target recognition.[18]

At the strategic level, applications of AI DSS include course of action analysis, early warning, tracking, guidance, and simulations such as those used in wargaming models.[19] AI DSS can assist with recreating potential scenarios to predict how adversaries might respond and evaluate the likely effects and damage of deploying specific weapons against targets. The use of AI DSS as part of these tasks could contribute to developing or adapting military strategies. However, few details exist about uses of AI DSS at the strategic level. As of September 2024, most reported examples of AI DSS in use-of-force decision-making have been at the operational and tactical levels (see section 3).

At the operational level, AI DSS can be used to manage a range of tasks including target detection, validation, nomination, and prioritization. Decision-makers can employ AI DSS to detect objects and persons, process data and intelligence, or assess the lawfulness of potential targets.[20] Some machine learning-based systems can be used to predict behaviours or characteristics, for instance suspected links with terrorist organizations or an individual's seniority within such an organization, based on contacts with other individuals that are part of the network.

15 Ingvild Bode and Tom Watts, *Meaning-Less Human Control: Lessons from Air Defence Systems on Meaningful Human Control for the Debate on AWS* (Oxford & Odense: Drone Wars UK & Center for War Studies, 2021).

16 Alan F.T. Windfield, *Robotics: A Very Short Introduction* (Oxford: Oxford University Press, 2012), 12.

17 Holland Michel, *Decisions, Decisions, Decisions*, 18–20.

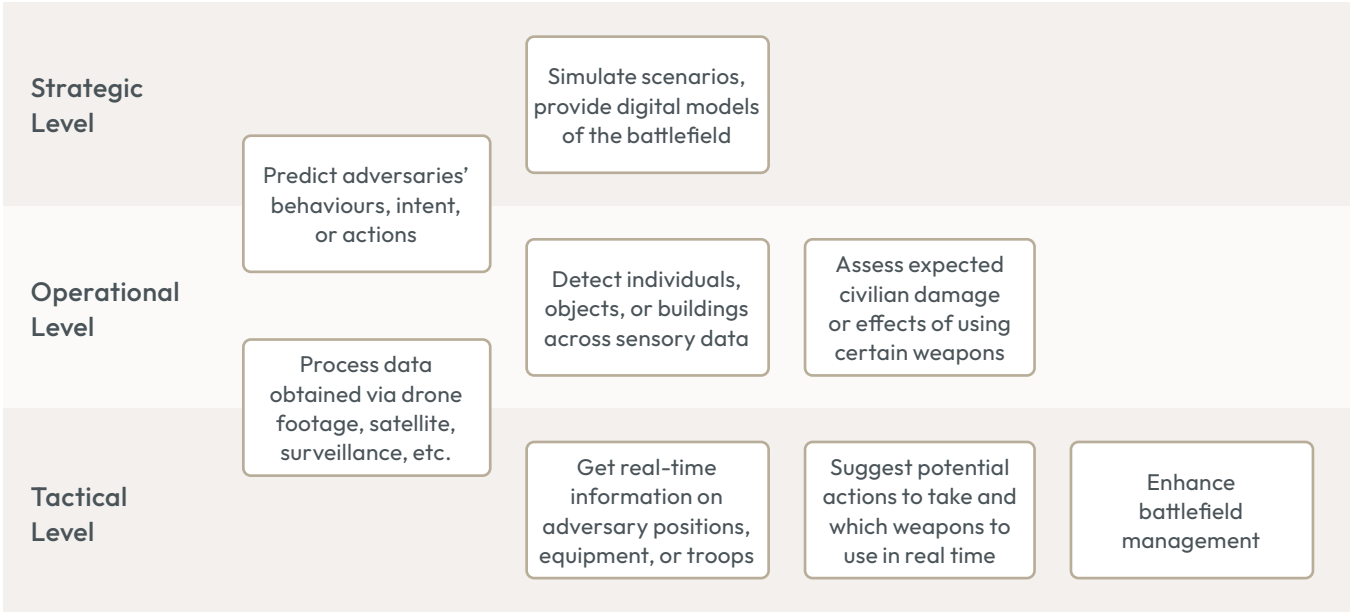
18 ICRC and Geneva Academy, *Expert Consultation Report on AI*, 13–14; Philip Kerbusch, Bas Keijser, and Selmar Smit, "Roles of AI and Simulation for Military Decision Making," *NATO Science & Technology*, STO-MP-IST-160.

19 Tobias Vestner, "From Strategy to Orders: Preparing and Conducting Military Operations with Artificial Intelligence," in *Research Handbook on Warfare and Artificial Intelligence*, ed. Robin Geiß and Henning Lahmann (Cheltenham: Edward Elgar, 2024), 116–35.

20 August Cole et al., *Artificial Intelligence in Military Planning and Operations: Ethical Considerations* (Oslo: Peace Research Institute Oslo, 2024).

At the tactical level, DSS can integrate AI technologies to acquire and provide real-time information and actionable recommendations for specific, tactical decisions in battle. Commanders can use AI DSS to determine the 'optimal' weapons by processing real-time intelligence and assessing factors such as location, weapon effectiveness, civilian damage minimization, as well as adherence to the relevant rules of engagement (RoE). AI DSS at both the tactical and operational levels typically integrate data from multiple sources, including satellite imagery, geolocation data, and communication intercepts. While some systems present information without suggesting a course of action, others provide actionable intelligence which can potentially significantly alter a military decision on the use of force.

Figure 1 Potential uses of AI DSS (selected examples)



Militaries often mention the integration of AI DSS into the OODA loop decision-making model, which stands for 'observe, orient, decide and act'. Developed by US Air Force Colonel John Boyd, the OODA loop outlines the continuously ongoing military decision-making process, which evolves as events occur. The 'observe' phase involves gathering relevant data and information, which is then analysed and processed during the 'orient' phase. In the 'decide' phase, commanders select the best course(s) of action, and in the 'act' phase, personnel implement or reassess the action based on the situation.[21] In theory, AI DSS can be utilized throughout the OODA loop. For example, decision-makers can use AI DSS to gather and analyse real-time data from various intelligence sources during the 'observe' and 'orient' phases, then receive recommendations for a course of action in the 'decide' phase, and subsequently 'act' upon their decision. By integrating AI DSS, militaries seek to accelerate the OODA loop cycle and enable more efficient decision-making.[22] However, as we explore in section 4, the use of AI DSS also risks introducing significant uncertainties and concerns within this process.

21 ICRC and Geneva Academy, *Expert Consultation Report on AI*, 11–13; James Johnson, *The AI Commander: Centaur Teaming, Command, and Ethical Dilemmas* (Oxford: Oxford University Press, 2024), 89–92; Kerbusch, Keijser, and Smit, "Roles of AI and Simulation for Military Decision Making"; Owen J. Daniels, "Speeding Up the OODA Loop with AI," in *Delivering NATO Air & Space Power at the Speed of Relevance* (Joint Air and Space Power Conference 2021 Read Ahead), 159–167.

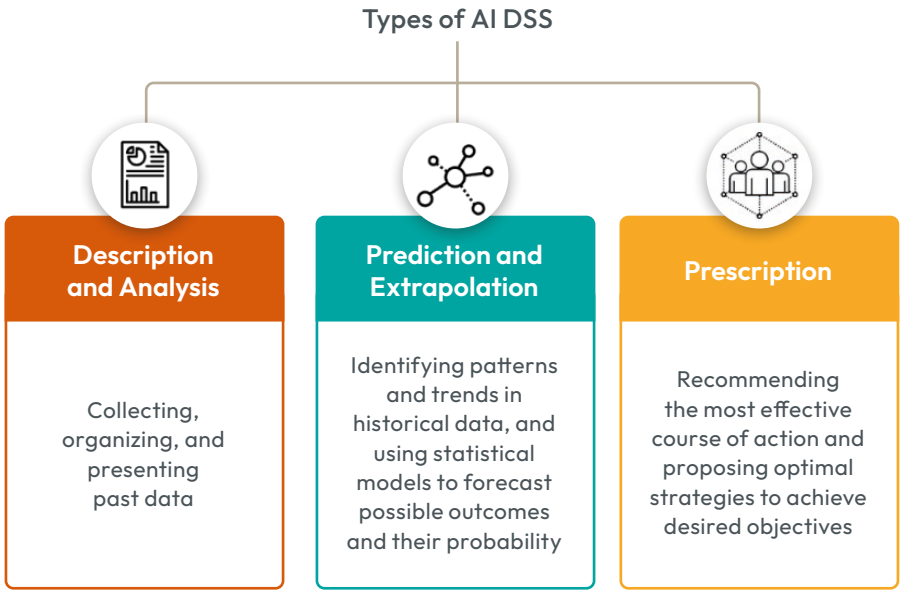
22 Vincent Boulanin, "Risks and Benefits of AI-Enabled Military Decision-Making," in *Research Handbook on Warfare and Artificial Intelligence*, ed. Robin Geiß and Henning Lahmann (Cheltenham: Edward Elgar, 2024), 101; Dominik Steiger, "Employment of AI in Decisions on the Use of Force," in *Research Handbook on Warfare and Artificial Intelligence*, ed. Robin Geiß and Henning Lahmann (Cheltenham: Edward Elgar, 2024), 136–60.

While not all AI DSS are designed for decisions that directly relate to the use of force, it is important to consider how the use of such systems might have a *"cascading effect"* on decisions that ultimately become relevant for targeting and the use of force.[23] For example, AI DSS can assist with logistical tasks such as coordinating the deployment of personnel and managing the transport of weaponry, equipment, and troops. While these decisions are not directly related to the use of force, they contribute to the effectiveness of military operations and indirectly influence how force is applied.[24] In addition, AI DSS help process intelligence that plays a crucial role in the targeting process.[25] Therefore, even AI DSS that are not linked to a weapon system raise "considerable concern" about how human–machine interactions may result in the selection and engagement of targets.[26]

It is important to consider how the use of AI DSS might have a "cascading effect" on decisions that ultimately become relevant for targeting and the use of force

Due to the wide range of AI DSS use cases, which are too numerous to categorize individually, this section instead groups them into three main types based on their primary design functions. These types are not mutually exclusive, as many systems can perform multiple functions. However, we find it useful to think of the following three types: **1) description and analysis, 2) prediction and extrapolation, and 3) prescription (see figure 2).**[27] Section 3 will discuss recent developments by referring to these three categories.

Figure 2 Three main types of AI DSS



23 See Arthur Holland Michel's remarks at the event "Artificial Intelligence in Military Decision Making: Legal and Humanitarian Implications" organized by the ICRC on 14 May 2024, https://www.icrc.org/en/event/event-artificial-intelligence-military-decision-making-legal-and-humanitarian-implications.

24 ICRC and Geneva Academy, *Expert Consultation Report on AI*, 7.

25 Intelligence personnel are estimated to "perform approximately 85 to 90 percent of targeting". See Ekelhof, "Lifting the Fog of Targeting," 63.

26 Klaudia Klonowska, "Article 36: Review of AI Decision-Support Systems and Other Emerging Technologies of Warfare," in *Yearbook of International Humanitarian Law, Volume 23 (2020)*, ed. Terry D. Gill et al., vol. 23, Yearbook of International Humanitarian Law (The Hague: T.M.C. Asser Press, 2022), 125.

27 ICRC and Geneva Academy, *Expert Consultation Report on AI*, 9.

2.3 The role of humans in the use of AI DSS

The main purpose of AI DSS is to assist and inform humans, who remain 'in' or 'on' the loop of decisions on the use of force.[28] The use of AI DSS therefore represents a form of human–machine interaction,[29] also referred to as human–machine teaming or human–system integration.[30] While AWS also represent a form of human–machine interaction, AI DSS are typically distinguished by a higher level of human involvement. In a context of using AWS, humans are not completely removed from decision-making on the use of force, but there is a risk of increasing "distance in time, space and understanding between human decisions and the consequences of these decisions on the battlefield".[31] In a context of using AI DSS, humans interact more directly with AI DSS, and the systems can be considered "epistemic tools" in the decision-making process.[32] In theory, humans are expected to remain the ultimate decision-makers on the use of force, for instance by selecting, authorizing, or vetoing targets.

However, as research on AI and autonomy in weapon systems demonstrates, a human 'in' or 'on' the loop does not guarantee a specific, high quality of human involvement in military use-of-force decision-making.[33] This is especially the case given that human–machine interaction in AI DSS is a complex phenomenon that extends beyond simple one-to-one interactions. In practice, it often involves multiple layers of interconnected human and machine 'agents' (in a technical sense), operating within what militaries call the 'kill chain', or the dynamic targeting cycle.[34] Multiple, interconnected AI DSS can be engaged at different stages of the decision-making process. These systems form so-called 'kill webs': complex networks of sensors, hardware, data, and software that humans need to navigate while deciding on courses of action.[35]

A human 'in' or 'on' the loop does not guarantee a specific, high quality of human involvement in military use-of-force decision-making

AI DSS are not inherently weapon systems. While AI DSS can be integrated into physical components, they are not necessarily connected to infrastructure that enables them to translate their outputs into physical actions.[36] However, it is likely that AI DSS are used jointly with weapon systems integrating AI or autonomous technologies.[37] While AI DSS and AWS share similar underlying concerns regarding the exercise of human agency and human–machine interaction, the broader and more extensive use cases of AI DSS potentially present additional complexities.

28 Noel Sharkey, "Staying in the Loop: Human Supervisory Control of Weapons," in *Autonomous Weapons Systems: Law, Ethics, Policy*, ed. Nehal Bhuta et al. (Cambridge: Cambridge University Press, 2016), 23–38.

29 Ingvild Bode and Anna Nadibaidze, "Symposium on Military AI and the Law of Armed Conflict: Human-Machine Interaction in the Military Domain and the Responsible AI Framework," *Opinio Juris*, April 4, 2024, https://opiniojuris.org/2024/04/04/symposium-on-military-ai-and-the-law-of-armed-conflict-human-machine-interaction-in-the-military-domain-and-the-responsible-ai-framework/.

30 On human-machine teaming see Margarita Konaev, Tina Huang, and Husanjot Chahal, *Trusted Partners: Human-Machine Teaming and the Future of Military AI* (Washington, DC: Center for Security and Emerging Technology, 2021); Jean-Marc Rickli, Federico Mantellassi, and Quentin Ladetto, *What, Why and When? A Review of the Key Issues in the Development and Deployment of Military Human-Machine Teams* (Geneva: Geneva Centre for Security Policy, 2024).

31 Boulanin, "Risks and Benefits of AI-Enabled Military Decision-Making," 110.

32 Jannik Zeiser, "Owning Decisions: AI Decision-Support and the Attributability-Gap," *Science and Engineering Ethics* 30, no. 4 (2024): 5, https://doi.org/10.1007/s11948-024-00485-1.

33 Bode and Watts, *Meaning-Less Human Control*; Bode and Watts, *Loitering Munitions and Unpredictability*; Ingvild Bode, "Practice-based and Public-deliberative Normativity: Retaining Human Control over the Use of Force," *European Journal of International Relations* 29, no. 4 (2023), 990–1016, https://doi.org/10.1177/13540661231163392.

34 Jennifer Rooke, "Shortening the Kill Chain with Artificial Intelligence," *The AutoNorms Blog*, November 28, 2021, https://www.autonorms.eu/shortening-the-kill-chain-with-artificial-intelligence/.

35 Arthur Holland Michel, "Inside the Messy Ethics of Making War with Machines," *MIT Technology Review*, August 16, 2023, https://www.technologyreview.com/2023/08/16/1077386/war-machines/; see also Elke Schwarz's remarks at the seminar "Smart War? The Promises and Pitfalls of Military AI" organized by the Royal Danish Defence College on 2 May 2024, https://www.fak.dk/da/nyheder/2024/se-eller-gense-seminaret-smart-war-the-promises-and-pitfalls-of-military-ai/.

36 We thank Anna Rosalie Greipl for highlighting this point.

37 Klonowska, "Article 36," 135.

Therefore, although current AI DSS designs incorporate human involvement in military decision-making, there are ongoing concerns about the extent to which human decision-makers can exercise meaningful judgement, critically evaluate recommendations from these systems, and avoid becoming mere 'rubber stamps' or engaging in only 'symbolic involvement', especially in the fast-moving contexts of battlefield. As we discuss in section 4, integrating AI technologies into DSS might "give the (sometimes incorrect) impression of only assisting rather than replacing the role of humans" in military decision-making on the use of force.[38]

Multiple, interconnected AI DSS can be engaged at different stages of the decision-making process

38 Marta Bo and Jessica Dorsey, "Symposium on Military AI and the Law of Armed Conflict: The 'Need' for Speed – The Cost of Unregulated AI Decision-Support Systems to Civilians," *Opinio Juris*, April 4, 2024, https://opiniojuris.org/2024/04/04/symposium-on-military-ai-and-the-law-of-armed-conflict-the-need-for-speed-the-cost-of-unregulated-ai-decision-support-systems-to-civilians/.

3 Review of Developments and Reported Cases

This section examines some of the recent developments related to AI DSS, at the time of writing in September 2024. The cases discussed below were chosen based on their prominence in the literature and debates in academic, policy and media publications, as well as the accessibility of information about them. The review is based on reports available via sources including media and press articles, journalistic investigations, press releases or information shared by governments, international organizations, or private companies, reports published by think tanks and research institutes, monographs, and peer-reviewed articles. It should be noted that there is a substantial difference in information available about how some of these systems are being employed or have been used.

Moreover, given that we cannot verify these accounts independently, we caution against making definitive statements about the exact types of technologies, associated technological capabilities, and uses of these techniques, e.g., the precise stage or task where these systems played a role. We also do not portray our study as an extensive catalogue of AI DSS or their technical characteristics. Rather, we treat the developments we examine as indicative of trends in military AI DSS and the potential implications of these trends, which we review in section 4.

3.1 The United States' Project Maven

The US Department of Defense (DoD) has a long-standing interest in automating the processing of large amounts of data and intelligence analysis for military decision-making. One prominent historical illustration of these trends in the US military includes the Skynet system (see box 1). A more recent and widely discussed case is the "Algorithmic Warfare Cross-Functional Team" programme, also known as Project Maven. Project Maven is a DoD initiative aimed at using computer vision and machine learning algorithms to identify targets in real time based on previously collected data such as drone footage. As with many AI-based systems, technologies developed under Maven can be used for various purposes, including military planning and targeting.

The main initial objective behind Maven was to help process large amounts of data, especially video imagery gathered by US drones in the Middle East, which by 2019 totalled more than 4 million hours of footage.[39] Before Maven, humans analysed these videos manually. The initiative also aimed to make use of algorithmic technologies developed in the private sector to automate the process of target recognition, utilizing algorithms that would be constantly re-trained

The main initial objective behind Maven was to help process large amounts of data, especially video imagery gathered by US drones in the Middle East, which by 2019 totalled more than 4 million hours of footage

39 Cansu Canca, "AI Ethics and Governance in Defence Innovation: Implementing AI Ethics Framework," in *The AI Wave in Defence Innovation*, ed. Michael Raska and Richard A. Bitzinger (Abingdon and New York: Routledge, 2023), 61.

with 'better' data.[40] Established in April 2017 under the leadership of then Deputy Defense Secretary Robert Work, Maven became operational by the end of that same year, supporting military intelligence units as part of US operations against the Islamic State in Iraq and Syria.[41]

Box 1 Skynet

The National Security Agency (NSA)'s data analytical system Skynet can be described as a "surveillance program that uses phone metadata to track the location and call activities of suspected terrorists".[42] It reportedly collected metadata from Pakistan's mobile phone network and processed this data via machine learning algorithms to analyse patterns and identify potential couriers related to terrorist organizations, or agents who pass on messages to and from these organizations.[43] The system scanned through Pakistani citizens' patterns of daily life routines such as travels, contacts, or visits, as it would be too time-consuming to analyse millions of phone and travel records manually. A 'score' was released for all individuals based on this analysis, with high scores attributed to suspected couriers and low scores given to civilians. Such scores were used as an informational basis of, for instance, drone strikes and counter-terrorism operations— although it must be added that data analytical programmes such as Skynet have likely been only one part of the process of identifying targets.[44]

Initially, thousands of people participated in labelling, cataloguing, and curating the data needed for the Maven system.[45] The project also involved the participation of Google, as the DoD was looking to collaborate with leading researchers in computer vision technology, which were typically based at Big Tech companies rather than at traditional defence contractors. However, after a protest by the company's employees in 2018, Google did not renew the Maven contract.[46] Maven, often branded as the DoD's "flagship AI effort", has remained active after the Google-related controversy and is currently managed by the Chief Digital and Artificial Intelligence Office and the National Geospatial-Intelligence Agency (NGA).[47]

The NGA describes its role as "integrating state-of-the-art computer vision and AI capabilities into analytic workflows", including for locating objects, directing "analysts to abnormal or significant activity in near real-time", detecting

40 Julia Press, "Inside Project Maven, the US Military's Mysterious AI Project," *Bloomberg*, February 29, 2024, https://www.bloomberg.com/news/articles/2024-02-28/inside-project-maven-the-us-military-s-flagship-ai-project-big-take-podcast?sref=62t700ZI.

41 Paul Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence* (New York: W. W. Norton, 2023), 58; Gregory C. Allen, "Project Maven Brings AI to the Fight against ISIS," *Bulletin of the Atomic Scientists*, December 21, 2017, https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/#post-heading.

42 Kim Zetter, "So, the NSA Has an Actual Skynet Program," *WIRED*, May 8, 2015, https://www.wired.com/2015/05/nsa-actual-skynet-program/.

43 Christian Grothoff and J.M Porup, "The NSA's SKYNET Program May Be Killing Thousands of Innocent People," *Ars Technica*, February 16, 2016, https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/; Martin Robbins, "Has a Rampaging AI Algorithm Really Killed Thousands in Pakistan?" *The Guardian*, February 18, 2016, https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan; Klonowska, "Article 36," 137.

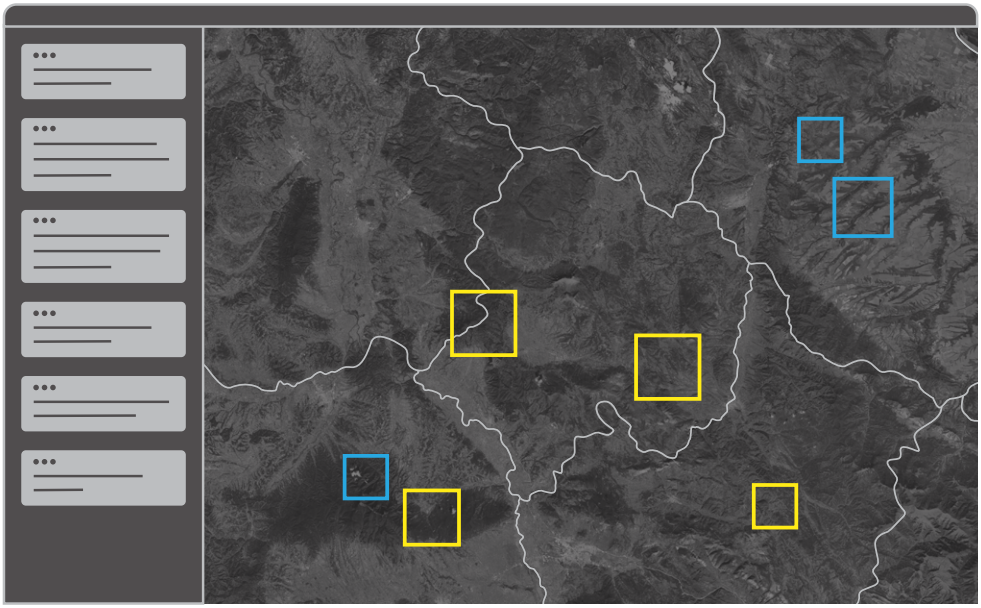
44 The Intercept, "SKYNET: Courier Detection via Machine Learning," May 8, 2015, https://theintercept.com/document/skynet-courier/; The Intercept, "SKYNET: Applying Advanced Cloud-Based Behavior Analytics," May 8, 2015, https://theintercept.com/document/skynet-applying-advanced-cloud-based-behavior-analytics/; John Naughton, "Death by Drone Strike, Dished out by Algorithm," *The Observer*, February 21, 2016, https://www.theguardian.com/commentisfree/2016/feb/21/death-from-above-nia-csa-skynet-algorithm-drones-pakistan.

45 Press, "Inside Project Maven"; Richard H. Shultz and Richard D. Clarke, "Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare," *Modern War Institute at West Point*, August 25, 2020, https://mwi.westpoint.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/.

46 Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," *The New York Times*, June 1, 2018, https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

47 Theresa Hitchens, "Pentagon's Flagship AI Effort, Project Maven, Moves to NGA," *Breaking Defense*, April 27, 2022, https://breakingdefense.com/2022/04/pentagons-flagship-ai-effort-project-maven-moves-to-nga/; Brandi Vincent, "Amid a High-Stakes Transition, Questions Linger about Project Maven's Future Management," *DefenseScoop*, September 9, 2022, https://defensescoop.com/2022/09/09/amid-a-high-stakes-transition-project-mavens-future-management-remains-unclear%EF%BF%BC/.

anomalies, and identifying targets.[48] NGA Director Frank Whitworth has claimed that the accuracy of models they use "meet or exceed human detection, classification, and tracking performance".[49] Several private companies are or have reportedly been involved in designing the platform used by Maven and working on enhancing it, including Palantir Technologies, Amazon, Anduril, and Microsoft.[50]



Maven's system now uses more types of data: not just satellite imagery and drone videos but also infrared sensors, geolocation tags, and multispectral sensors, among others. The processed information is then presented in the Maven Smart System, an interface which "brings together multiple data feeds" and where "commanders can view the whole battlefield at a glance".[51] For instance, some yellow boxes would highlight potential targets such as ships or military bases, while other, blue boxes would delineate no-strike zones, such as civilian infrastructure.[52] Subsequently, the officers would make decisions on potential courses of action to take, which may include using force.

Schuyler Moore, Chief Technology Officer for the US Central Command, told *Bloomberg* that the US relied on the Maven system to carry out more than 85 air strikes in Iraq and Syria on military targets in February 2024, following 12 months of digital exercises. This statement was accompanied with emphasizing that Maven outputs were used for finding potential targets, not taking the decisions to strike, and that the recommendations were double-checked by humans.[53] US military officials constantly point out that there are no plans to delegate targeting decisions to such systems, as the objective is to assist in identifying targets. They tend to emphasize that the intended focus is on

48 National Geospatial-Intelligence Agency, "Remarks as Prepared for NGA Director Vice Adm. Frank Whitworth for 2024 GEOINT Symposium," May 7, 2024, https://www.nga.mil/news/1715096839917_Remarks_as_delivered_by_NGA_Director_Vice_Adm_Fran.html.

49 National Geospatial-Intelligence Agency.

50 Katrina Manson, "AI Warfare Is Already Here," *Bloomberg*, February 28, 2024, https://www.bloomberg.com/features/2024-ai-warfare-project-maven/; Lee Fang, "Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract," *The Intercept*, March 9, 2019, https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/; Courtney Albon, "Palantir Wins Contract to Expand Access to Project Maven AI Tools," *DefenseNews*, May 30, 2024, https://www.defensenews.com/artificial-intelligence/2024/05/30/palantir-wins-contract-to-expand-access-to-project-maven-ai-tools/.

51 Manson, "AI Warfare Is Already Here."

52 Manson.

53 Katrina Manson, "US Used AI to Help Find Middle East Targets for Airstrikes," *Bloomberg*, February 26, 2024, https://www.bloomberg.com/news/articles/2024-02-26/us-says-it-used-ai-to-help-find-targets-it-hit-in-iraq-syria-and-yemen.

developing human–machine teams to improve the process of military decision-making.[54] With this objective in mind, the US military has been implementing various other initiatives to integrate AI into targeting decision-making. Notably, in 2021 US Secretary of the Air Force Frank Kendall stated that the Air Force "deployed AI algorithms for the first time to a live operational kill chain", reportedly to support intelligence officers.[55]

Box 2 Developments in the private sector

Private sector actors, both Big Tech companies and startups, play a prominent role in developing military AI DSS. Some companies develop AI DSS specifically for defence purposes.

For instance, in March 2024 the US Army awarded the software company Palantir an agreement of approximately 178 million US dollars to develop and deliver prototypes of the Tactical Intelligence Targeting Access Node (TITAN) ground station system. The US Army expects TITAN to "provide intelligence support to targeting and situational awareness and understanding, ultimately reducing the sensor-to-shooter timeline and enabling Multi-Domain Operations".[56]

Another example is defence tech company Anduril's Lattice software, advertised as a platform to analyse multiple feeds of data with the help of AI and machine learning techniques. Anduril claims that Lattice "accelerates complex kill chains by orchestrating machine-to-machine tasks at scales and speeds beyond human capacity".[57]

Meanwhile, other systems might be developed initially for other purposes but later adapted for military use. This could be the case for large language models. Notably, the company OpenAI, which developed the generative AI software ChatGPT, removed its policy that its models may not be used for "weapons development" and "military and warfare" in January 2024.[58]

Generally, there is a significant degree of overlap between types of AI DSS used for civilian and military purposes. For example, AI DSS developed to sustain preparedness for computer emergency response teams ahead of potential cyberattacks on key state infrastructure may well apply in similar ways in relation to military infrastructure.[59] It should also be acknowledged that while some systems, tools, or projects might be already deployed in ongoing military operations, many remain at development and testing stages.

54 See US Department of Defense, "Lt. Gen. Jack Shanahan Media Briefing on A.I.-Related Initiatives within the Department of Defense," August 30, 2019, https://www.defense.gov/News/Transcripts/Transcript/Article/1949362/lt-gen-jack-shanahan-media-briefing-on-ai-related-initiatives-within-the-depart/; Paul Mcleary, "Pentagon's Big AI Program, Maven, Already Hunts Data in Middle East, Africa," *Breaking Defense*, May 1, 2018, https://breakingdefense.com/2018/05/pentagons-big-ai-program-maven-already-hunts-data-in-middle-east-africa/; Palantir, "Accelerating Decision Making: National Geospatial-Intelligence Agency at AIPCon5," *YouTube*, September 19, 2024, https://www.youtube.com/watch?v=XzKnUt6NAbw.

55 David Hambling, "Artificial Intelligence Is Now Part of U.S. Air Force's 'Kill Chain'," *Forbes*, October 28, 2021, https://www.forbes.com/sites/davidhambling/2021/10/28/ai-now-part-of-us-air-force-kill-chain/; Rooke, "Shortening the Kill Chain with Artificial Intelligence."

56 Shawn Nesaw, "Army Tactical Intelligence Targeting Access Node (TITAN) Ground Station Prototype - Award," *Defense Visual Information Distribution Service*, March 6, 2024, https://www.dvidshub.net/news/465449/army-tactical-intelligence-targeting-access-node-titan-ground-station-prototype-award; see also Courtney Albon and Colin Demarest, "Army Chooses Palantir to Build Next-Generation Targeting System," *C4ISRNET*, March 6, 2024, https://www.c4isrnet.com/artificial-intelligence/2024/03/06/army-chooses-palantir-to-build-next-generation-targeting-system/.

57 Anduril, "Lattice for Command and Control," https://www.anduril.com/command-and-control/.

58 Eva Dou, Nitasha Tiku, and Gerrit De Vynck, "Pentagon Explores Military Uses of Large Language Models," *The Washington Post*, February 20, 2024, https://www.washingtonpost.com/technology/2024/02/20/pentagon-ai-llm-conference/.

59 Marc-André Kaufhold et al., "'We Do Not Have the Capacity to Monitor All Media': A Design Case Study on Cyber Situational Awareness in Computer Emergency Response Teams," in *Proceedings of the CHI Conference on Human Factors in Computing Systems* (CHI '24: CHI Conference on Human Factors in Computing Systems, Honolulu HI USA: ACM, 2024), 1–16, https://doi.org/10.1145/3613904.3642368.

3.2 The Russia-Ukraine war (2022-)

After illegally annexing Crimea in 2014, Russia fully invaded Ukraine on 24 February 2022. Some experts describe Russia's ongoing full-scale invasion of Ukraine as a "testing ground" or "living lab" for AI warfare[60] due to the unprecedented role that AI technologies play in weapon systems (especially drones), intelligence analysis, or cybersecurity, among other areas.[61] AI technologies are not used all the time and for every task, but the scale of the use is noticeably different from previous armed conflicts. Tech and robotics companies from Ukraine and abroad have mobilized to supply AI-powered and increasingly more autonomous drones to the Ukrainian armed forces in their defence against Russia's aggression.[62]

Many Ukrainian startups, as well as foreign corporate actors such as tech companies, are developing software and AI models to locate and identify Russian targets

Both Ukraine and Russia have been developing and using uncrewed aerial vehicles with various levels of AI-based autonomy in their operations, although Russia's AI capabilities have proven to be far from the level previously advertised by Russian officials.[63] In contrast to extensive reporting about aerial drones, not much detailed information is publicly available about the role of AI DSS used by either Ukraine or Russia. However, existing reports allow us to broadly depict the direction that AI DSS development and use might be taking.

One more well-known example is the Ukrainian armed forces' use of AI-based software provided by the company Palantir for various purposes, including clearing landmines, collecting evidence of Russian war crimes, and taking targeting decisions on the battlefield. Reports describe systems used by Ukrainian commanders as providing a "digital model of the battlefield" used to detect adversary forces, positions, objects, and other key information, although employing a "limited array of sensors and AI tools".[64] The Palantir MetaConstellation tool aggregates data from commercial satellites, heat sensors, and drone footage.[65] Users of MetaConstellation reportedly can put in specific demands, such as to see a specific location at a particular time.[66] NATO advisors located outside Ukraine are using similar systems, which are said to be based on various sources of data and intelligence and to be constantly updated to improve the algorithms' effectiveness.[67] Palantir CEO Alexander Karp claimed that the company's software is "responsible for most of the targeting in Ukraine", while Ukrainian Minister of Digital Transformation Mykhailo Fedorov mentioned that Ukrainian armed forces used such systems to put together data about Russian troops, with this data then informing military decision-making on the use of force.[68]

60 Vera Bergengruen, "How Tech Giants Turned Ukraine into an AI War Lab," *TIME*, February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/; Robin Fontes and Jorrit Kamminga, "Ukraine A Living Lab for AI Warfare," *National Defense Magazine*, March 24, 2023, https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare.

61 Margarita Konaev, *Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability* (Arlington, VA: Center for Naval Analyses, 2023), 1; Jean-Marc Rickli and Federico Mantellassi, *The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare* (Geneva: Geneva Centre for Security Policy, 2024).

62 See, for instance, Gian Volpicelli, Veronika Melkozerova, and Laura Kayali, "'Our Oppenheimer Moment' — In Ukraine, the Robot Wars Have Already Begun," *Politico Europe*, May 16, 2024, https://www.politico.eu/article/robots-coming-ukraine-testing-ground-ai-artificial-intelligence-powered-combat-war-russia/; Max Hunder, "Ukraine Rushes to Create AI-Enabled War Drones," *Reuters*, July 18, 2024, https://www.reuters.com/technology/artificial-intelligence/ukraine-rushes-create-ai-enabled-war-drones-2024-07-18/; Paul Mozur and Adam Satariano, "A.I. Begins Ushering In an Age of Killer Robots," *The New York Times*, July 2, 2024, https://www.nytimes.com/2024/07/02/technology/ukraine-war-ai-weapons.html.

63 Anna Nadibaidze, "Russia's 'Low-Tech' War on Ukraine Discredited Its Military Modernization Narrative," *Network for Strategic Analysis*, March 3, 2023, https://ras-nsa.ca/russias-low-tech-war-on-ukraine/.

64 David Ignatius, "How the Algorithm Tipped the Balance in Ukraine," *The Washington Post*, December 19, 2022, https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/.

65 George Grylls, "Kyiv Is Outflanking Russia with Ammunition from Big Tech," *The Times*, December 24, 2022, https://www.thetimes.co.uk/article/ukraine-is-outflanking-russia-with-ammunition-from-big-tech-lxp6sv3qz; Ignatius, "How the Algorithm Tipped the Balance in Ukraine."

66 Bruno Maçães, "How Palantir Is Shaping the Future of Warfare," *TIME*, July 10, 2023, https://time.com/6293398/palantir-future-of-warfare-ukraine/.

67 Ignatius, "How the Algorithm Tipped the Balance in Ukraine."

68 Jeffrey Dastin, "Ukraine Is Using Palantir's Software for 'targeting,' CEO Says," *Reuters*, February 2, 2023, https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/.

There are also many domestic Ukrainian software developments in the sphere of AI DSS, notably as part of the Brave1 initiative established by the Ministry of Digital Transformation.[69] Some of these systems have been in use since Russia's first invasion in 2014. For instance, the system Kropyva, developed by a volunteer group called Army SOS in 2014 to assist with tactical planning and calculations for artillery, is reportedly used by 90–95% of Ukrainian gunners.[70] Intelligence and reconnaissance personnel can enter coordinates of adversary targets into an Android application on a tablet, which are then automatically transmitted to the nearest artillery battery.[71] Described as an "Uber for artillery",[72] Kropyva provides situational awareness by "computing ballistic calculations" based on drone footage, radars, and other sources.[73]

Another system described as an "Uber-style technology" is the GIS Arta, or Geographic Information System of Artillery.[74] A group of Ukrainian developers created GIS Arta to allow real-time sharing of information about adversary locations collected from satellite, internet, or radio sources, among others.[75] The exact types of techniques such systems integrate—and whether these encompass AI or rather automated technologies—are, however, uncertain. Some experts have referred to them as "traditional software".[76] This uncertainty demonstrates the challenges in defining and verifying the technologies involved and details about their uses. As pointed out throughout this report, such complexities and definitional ambiguities should be more openly discussed in media, policy, and academic debates.

Destroyed Russian military vehicle in 2022 in the Sumy region, Ukraine.
Source: Ministry of Defense of Ukraine, via Wikimedia Commons.

69 Vitaliy Goncharuk, *Survival of the Smartest? Defense AI in Ukraine* (Hamburg: Defense AI Observatory, 2024), 18.

70 Taisa Melnyk, "IT Chaos in the Ukrainian Armed Forces. Hundreds of Thousands of Soldiers Use Different Software Programs Developed by Volunteers. Is Such Decentralization Dangerous? [IT-хаос на службі ЗСУ. Сотні тисяч військових користуються різним софтом, який розробили волонтери. Чи небезпечна така децентралізація]," *Forbes UA*, November 14, 2022, https://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu-sotni-tisyach-viyskovikh-koristuyutsya-riznim-softom-yakiy-rozrobili-volonteri-chi-nebezpechna-taka-detsentralizatsiya-14112022-9700.

71 Taisa Melnyk, "'Stinging Nettle'. How Ukrainian Artillery Software Affects the Course of the War [Жалюча «Кропива». Як українське програмне забезпечення для артилеристів впливає на перебіг війни]," *Forbes UA*, July 24, 2022, https://forbes.ua/innovations/zhalyucha-kropiva-yak-ukrainske-programne-zabezpechennya-dlya-artileristiv-vplivae-na-khid-viyni-22072022-7054; Maçães, "How Palantir Is Shaping the Future of Warfare."

72 Tom Cooper, "Kropyva: Ukrainian Artillery Application," *Medium*, June 10, 2022, https://medium.com/@x_TomCooper_x/kropyva-ukrainian-artillery-application-e5c6161b6c0a.

73 Goncharuk, *Survival of the Smartest? Defense AI in Ukraine*, 31.

74 Charlie Parker, "Uber-Style Technology Helped Ukraine to Destroy Russian Battalion," *The Times*, May 14, 2022, https://www.thetimes.com/world/russia-ukraine-war/article/uk-assisted-uber-style-technology-helped-ukraine-to-destroy-russian-battalion-5pxnh6m9p.

75 Mark Bruno, "'Uber For Artillery' – What Is Ukraine's GIS Arta System?," *The Moloch*, August 24, 2022, https://themoloch.com/conflict/uber-for-artillery-what-is-ukraines-gis-arta-system/.

76 Gregory Allen quoted in Holland Michel, "Inside the Messy Ethics of Making War with Machines."

In October 2023, Fedorov wrote about the AI-based system Griselda, developed as part of Brave1 to collect intelligence and process information coming from "satellites, drones, social networks, media, and even hacked enemy databases".[77] Griselda is already in use conjointly with systems such as Kropyva and others by Ukrainian gunners and tankers. As Fedorov wrote, "it takes 28 seconds from the time the information appears in the system to the time it is received".[78]

Another Ukrainian system is the Delta platform, created by the Ministry of Defence together with NATO partners for the purposes of battlefield management and military planning. Delta supplies Ukrainian commanders with real-time information and maps, which combined with other intelligence, form the basis of decisions on "where and how Ukrainian troops should attack".[79] Beyond limited available information about Delta following its launch in February 2023,[80] it is not entirely clear exactly how often Delta is being used and with what results.[81] Overall, many Ukrainian startups, as well as foreign corporate actors such as tech companies, are developing software and AI models to locate and identify targets. This extends to, for example, collecting information about Russian troops who appear to be low on supplies and/or morale from drone footage or social media posts (for instance, complaints from Russian soldiers), to passing this information to the Ukrainian armed forces.[82]

Not much is known about specific AI DSS that are or might be used by the Russian military in its ongoing invasion of Ukraine. Russia's interest towards computational and digital technologies in military command and decision-making dates back decades.[83] Russian state-controlled media mentions some systems, such as the automated Acacia-M, designed to send real-time data analysis about the state of the battlefield and adversary positions to the commander, specifically to support combat and targeting decisions. In 2018 it was reported that these systems would be adopted by the end of 2019.[84] At the same time, the Russian military community is debating the Russian army's ability to efficiently use such systems in its invasion of Ukraine.[85] In August 2023, state corporation Rostec presented the automated control system Acacia-E, claiming that it would use information received from digital radio stations, allowing it to track up to 2,000 air targets at the same time,

77 Militarnyi, "Ukraine Develops Intelligence System Based on Artificial Intelligence," October 20, 2023, https://mil.in.ua/en/news/ukraine-develops-intelligence-system-based-on-artificial-intelligence/.

78 Militarnyi; Mykhailo Fedorov on Telegram, "High Quality Intelligence for the Military Thanks to AI [Якісні розвіддані для військових завдяки штучному інтелекту]," October 20, 2023, https://t.me/zedigital/3756.

79 Lara Jakes, "For Western Weapons, the Ukraine War Is a Beta Test," *The New York Times*, November 15, 2022, https://www.nytimes.com/2022/11/15/world/europe/ukraine-weapons.html.

80 Ministry of Defence of Ukraine, "According to the Proposal of the Minister of Defence Oleksii Reznikov, the Government Decided to Introduce the Delta System into the Armed Forces [За поданням міністра оборони Олексія Резнікова Уряд прийняв рішення щодо запровадження системи Delta в Силах оборони]," February 4, 2023, https://www.mil.gov.ua/news/2023/02/04/oleksiya-reznikova-uryad-prijnyav-rishennya-shhodo-zaprovadzhennya-sistemi-delta-v-silah-oboroni/.

81 Pavel Aksenov, "What is the Digital System Delta That Ukraine has Adopted, and Why It Is Needed [Что такое цифровая система Delta, которую Украина приняла на вооружение, и зачем она нужна]," *BBC News Russian*, February 4, 2023, https://www.bbc.com/russian/features-64526570.

82 The Economist, "How Ukraine Is Using AI to Fight Russia," April 8, 2024, https://www.economist.com/science-and-technology/2024/04/08/how-ukraine-is-using-ai-to-fight-russia; David E. Sanger, "In Ukraine, New American Technology Won the Day. Until It Was Overwhelmed," *The New York Times*, April 23, 2024, https://www.nytimes.com/2024/04/23/us/politics/ukraine-new-american-technology.html.

83 Anna Nadibaidze, *Russian Perceptions of Military AI, Automation, and Autonomy* (Philadelphia, PA: Foreign Policy Research Institute, 2022); Samuel Bendett, "Military AI Developments in Russia," in *The AI Wave in Defence Innovation*, ed. Michael Raska and Richard A. Bitzinger (Abingdon and New York: Routledge, 2023), 179–98.

84 Alexey Ramm and Alexandr Kruglov, "The Ministry of Defence Will Deploy the 'Acacia' for 21 billion [Минобороны развернет «Акацию» за 21 млрд]," *Izvestia*, July 5, 2018, https://iz.ru/761052/aleksei-ramm-aleksandr-kruglov/minoborony-razvernet-akatciiu-za-21-mlrd; Roger McDermott, "Moscow Showcases Breakthrough in Automated Command and Control," *Eurasia Daily Monitor* 16, no. 164 (2019), https://jamestown.org/program/moscow-showcases-breakthrough-in-automated-command-and-control/.

85 Aksenov, "What is the Digital System Delta."

while updating the information every 3–10 seconds.[86] However, it is unclear whether the Russian army intends to or is able to use this system.

Another Russian system is the RB-109A Bylina complex for electronic warfare command and control, a system of receivers used to detect, and subsequently determine, ways to jam adversary radars and radio signals.[87] These systems can reportedly be used to analyse the battlefield in real time and 'decide' on how to best suppress targets (without necessarily involving a human operator), and then pass on this information to command.[88] Russian state-controlled media suggests that Bylina integrates AI algorithms to detect adversary planes, ships, and satellites, among others, and establish communication with the headquarters.[89] Reports about Russia using (and losing) these systems in its full-scale invasion of Ukraine have appeared since October 2023.[90]

3.3 The Israel-Hamas war (2023-)

Background: Israel's development of AI systems

Israel has a long track record of military-technological experimentation and innovation—not least resulting from the close ties between the state's military, academia, intelligence services, and technology sectors.[91] Israeli defence contractors have led the development of various weapon systems integrating autonomous and AI technologies, including loitering munitions such as the IAI Harpy and Harop, but also air defence systems such as the Iron Dome.[92] Israeli experimentation in this space has also extended to AI DSS—including prior to the widely circulated reports about such systems in the conflict in Gaza that followed Hamas' attacks on 7 October 2023.[93]

Notably, representatives of the Israeli Defence Forces (IDF) characterized the May 2021 conflict in the Gaza Strip as 'the first AI war', claiming that "this is the first time [AI] was used broadly across an operation".[94] They referred to AI integrated into decision support rather than weapon systems. Reporting indicates that the IDF developed several AI DSS in the context of "establish[ing] an advanced AI technological platform that centralised all data on terrorist groups in the Gaza Strip onto one system that enabled the analysis and

86 Rostec, "Rostec Showcased New Capabilities of the 'Acacia-E' Automated Control System at 'ARMY-23' [Ростех показал на «Армии-2023» новые возможности автоматизированной системы управления «Акация-Э»]," August 15, 2023, https://rostec.ru/news/rostekh-pokazal-na-armii-2023-novye-vozmozhnosti-avtomatizirovannoy-sistemy-upravleniya-akatsiya-e/.

87 David Axe, "Russia Sent Its New A.I. Drone-Killer to Ukraine. A Ukrainian Drone Blew It Up," *Forbes*, January 13, 2024, https://www.forbes.com/sites/davidaxe/2024/01/13/russia-sent-its-new-ai-drone-killer-to-ukraine-a-ukrainian-drone-blew-it-up/.

88 Roger McDermott, "Russia's Armed Forces Test and Refine Electronic Warfare Capability," *Eurasia Daily Monitor* 17, no. 59 (April 29, 2020), https://jamestown.org/program/russias-armed-forces-test-and-refine-electronic-warfare-capability/.

89 Alexey Ramm and Bogdan Stepovoy, "A Stunning Effect: When the Troops Will Receive the 'Bylina' Electronic Warfare System [Оглушительный эффект: когда войска получат системы РЭБ «Былина»]," *Izvestia*, October 6, 2023, https://iz.ru/1584777/aleksei-ramm-bogdan-stepovoi/oglushitelnyi-effekt-kogda-voiska-poluchat-sistemy-reb-bylina.

90 Axe, "Russia Sent Its New A.I. Drone-Killer to Ukraine."

91 Tal Mimran et al., "Israel-Hamas 2024 Symposium - Beyond the Headlines: Combat Deployment of Military AI-Based Systems by the IDF," *Lieber Institute West Point*, February 2, 2024, https://lieber.westpoint.edu/beyond-headlines-combat-deployment-military-ai-based-systems-idf/.

92 Reporting about the May 2021 conflict indicates that the Iron Dome used AI "to determine rocket trajectories based on radar information, intercepting those headed for densely populated areas". See Takeshi Kumon, "The First AI Conflict? Israel's Gaza Operation Gives Glimpse of Future," *NIKKEI Asia*, June 28, 2021, https://asia.nikkei.com/Politics/International-relations/The-first-AI-conflict-Israel-s-Gaza-operation-gives-glimpse-of-future.

93 Tal Mimran and Gal Dahan, "Artificial Intelligence in the Battlefield: A Perspective from Israel," *Opinio Juris*, April 20, 2024, https://opiniojuris.org/2024/04/20/artificial-intelligence-in-the-battlefield-a-perspective-from-israel/; Tal Mimran and Lior Weinstein, "The IDF Introduces Artificial Intelligence to the Battlefield - a New Frontier?," *Lieber Institute West Point*, March 1, 2023, https://lieber.westpoint.edu/idf-introduces-ai-battlefield-new-frontier/.

94 Kumon, "The First AI Conflict?"; see also Yonah Jeremy Bob, "IDF Unit 8200 Commander Reveals Cyber Use to Target Hamas Commander," *The Jerusalem Post*, February 13, 2023, https://www.jpost.com/israel-news/article-731443.

extraction of intelligence".[95] Reports from 2021 mentioned various types of data sources that the IDF has been collecting and that became the basis for AI DSS training, such as signal, visual, and geographical intelligence.[96] These reports also named three specific AI DSS used by the IDF: Alchemist, Depth of Wisdom, and Gospel.[97]

The Alchemist system "used AI and machine learning to alert troops in the field to possible attacks by Hamas and PIJ [Palestinian Islamic Jihad]" and was reportedly "used by every unit commander in the field [...] on a user-friendly tablet", while Gospel is described as integrating "AI to generate recommendations for troops in the research division of Military Intelligence, which used them to produce quality targets and then passed them on to the [Israeli Air Forces] to strike".[98] Depth of Wisdom has been said to serve the descriptive function of mapping the tunnel network under the Gaza Strip,[99] presenting "a full picture of the network both above and below ground with details, such as the depth of the tunnels, their thickness and the nature of the routes".[100]

An IDF Intelligence Corps senior officer emphasized the quantitative impact of systems such as Gospel on target generation, saying the use of these systems produced "hundreds of targets relevant to developments in the fighting, allowing the military to continue to fight as long as it needs to with more and more new targets".[101] Pro-governmental reporting at the time described the use of such AI DSS as advancing Israel's intelligence picture of Hamas targets, increasing the precision of targeting through reducing civilian loss of life, and reducing the overall duration of the fighting.[102]

Israel's AI DSS appear to have been developed and refined by the IDF's Target Administration Division (also referred to as Targets Center in other publications),[103] created in 2019 by then IDF chief of staff Lt. Gen. Aviv Kochavi for the purpose of increasing the speed and scale of target generation. Speaking at a conference in December 2022, Kochavi argued that the IDF Target Administration Division focused on connecting "existing advanced sensors and sources ... to advanced artificial intelligence" and that this process has led to the IDF identifying "as many targets in a month as it did in a year".[104] Kochavi was head of military intelligence during the Gaza War in 2014 and has since been focusing on increasing the pace of target generation, stating: "If, for example, the military had fewer than 300 targets in Lebanon in 2006, now there are thousands".[105] This indicates that using AI DSS to increase what is referred to as Israel's "target bank" has long been a primary focus of the IDF.[106]

95 Anna Ahronheim, "Israel's Operation against Hamas Was the World's First AI War," *The Jerusalem Post*, May 27, 2021, https://www.jpost.com/arab-israeli-conflict/gaza-news/guardian-of-the-walls-the-first-ai-war-669371.

96 Ahronheim.

97 Ahronheim.

98 Ahronheim; see also Anna Ahronheim, "The Road to the AI IDF," *The Jerusalem Post*, July 25, 2021, https://www.jpost.com/israel-news/the-idf-and-the-ai-game-changer-674636.

99 Omar Yousef Shehabi and Asaf Lubin, "Israel - Hamas 2024 Symposium - Algorithms of War: Military AI and the War in Gaza," *Lieber Institute West Point*, January 24, 2024, https://lieber.westpoint.edu/algorithms-war-military-ai-war-gaza/.

100 Ahronheim, "Israel's Operation against Hamas Was the World's First AI War."

101 Quoted in Ahronheim.

102 Ahronheim.

103 Yaakov Lappin, "IDF Identifies 'as Many Targets in a Month as It Did in a Year'," *Jewish News Syndicate*, December 4, 2022, https://www.jns.org/idf-identifies-as-many-targets-in-a-month-as-it-did-in-a-year/; see also Emanuel Fabian, "IDF Says It's Using AI to Quickly Identify and Strike New Hamas Targets," *The Times of Israel*, November 2, 2023, https://www.timesofisrael.com/liveblog_entry/idf-says-its-using-ai-to-quickly-identify-and-strike-new-hamas-targets/.

104 Lappin.

105 Yaakov Katz and Anna Ahronheim, "Aviv Kochavi: The IDF Chief of Staff in a Political Minefield," *The Jerusalem Post*, January 7, 2021, https://www.jpost.com/israel-news/aviv-kochavi-the-idf-chief-of-staff-in-a-political-minefield-654565.

106 Michael N. Schmitt and John J. Merriam, "The Tyranny of Context: Israeli Targeting Practices in Legal Perspective," *University of Pennsylvania Journal of International Law* 37, no. 1 (2015): 74–75.

After the 7 October 2023 attacks: Gospel, Lavender, and Where's Daddy

Compared to reports from 2021 and prior to that, the reported uses of AI DSS by the IDF in Gaza from November 2023 have drawn substantially more attention and scrutiny. Most of the publicly available information about AI DSS employed by Israel to generate targets in Gaza stems from in-depth investigative reporting conducted by journalists of the *+972* magazine in partnership with the *Local Call* outlet.[107] These reports are based on a combination of interviews with IDF 'whistleblowers', official IDF statements, as well as "Palestinian testimonies, data, and documentation".[108] Of these, the report published in April 2024 on the Lavender system offered the most detailed, albeit still limited, information specific to the functioning of the AI DSS employed.

On 7 October 2023, Palestinian militants associated with Hamas and PIJ entered Israeli territory, conducting an attack that resulted in the deaths of more than 1,100 civilians, children, and security personnel, abducting more than 240 hostages, and conducting widespread sexual violence.[109] In response, Israel commenced military operations in the Gaza Strip. The IDF has reportedly used at least three AI DSS in Gaza: Gospel (also referred to as 'Habsora'), Lavender, and Where's Daddy. Using such systems made it possible for the IDF to generate targets at a higher rate and greater speed. Official IDF numbers indicate that the Israeli military attacked 15,000 targets in the first 35 days of its offensive—an unprecedently high number compared to its previous major military operations in Gaza.[110]

Official IDF numbers indicate that it attacked 15,000 targets in the first 35 days of its offensive—an unprecedently high number compared to its previous major military operations in Gaza

IDF authorities have recognized the use of AI tools in target identification.[111] As an Israeli colonel quoted by *The Jerusalem Post* suggested, "the AI targeting capabilities had for the first time helped the IDF cross the point where they can assemble new targets even faster than the rate of attacks".[112] The high number of targets that the IDF attacked therefore appears to have been made possible through using AI DSS in ways that "produce targets at a fast pace and works by improving accurate and high-quality intelligence material according to needs".[113]

There is limited information available about what kinds of data Gospel, Lavender, and Where's Daddy systems process and how. Reportedly, Gospel marks buildings and structures of interest to the IDF, Lavender marks individuals that could be potential targets, while Where's Daddy is a tracking system for whether persons on the target list had entered their homes.[114] The data fed into the systems appears to come from various surveillance means across the Gaza Strip. Critical reporting has pointed out how vast amounts of surveillance data that Israel has been collecting in Gaza over decades "has been

107 Yuval Abraham, "'A Mass Assassination Factory': Inside Israel's Calculated Bombing in Gaza," *+972 Magazine*, November 30, 2023, https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/; Yuval Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza," *+972 Magazine*, April 3, 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/; see also Bethan McKernan and Davies, "'The Machine Did It Coldly': Israel Used AI to Identity 37,000 Hamas Targets," *The Guardian*, April 3, 2024, https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes.

108 Abraham, "'A Mass Assassination Factory': Inside Israel's Calculated Bombing in Gaza."

109 France 24, "Israel Social Security Data Reveals True Picture of Oct 7 Deaths," December 15, 2023, https://www.france24.com/en/live-news/20231215-israel-social-security-data-reveals-true-picture-of-oct-7-deaths.

110 Abraham, "'A Mass Assassination Factory': Inside Israel's Calculated Bombing in Gaza"; see also Harry Davies, Bethan McKernan, and Dan Sabbagh, "'The Gospel': How Israel Uses AI to Select Bombing Targets in Gaza," *The Guardian*, December 1, 2023, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets.

111 Fabian, "IDF Says It's Using AI to Quickly Identify and Strike New Hamas Targets."

112 Yonah Jeremy Bob, "IDF Bombs Whole Gaza Neighborhoods to Hit Hamas Targets - Official," *The Jerusalem Post*, October 11, 2023, https://www.jpost.com/israel-news/defense-news/article-767706.

113 IDF spokesperson quoted in Abraham, "'A Mass Assassination Factory': Inside Israel's Calculated Bombing in Gaza."

114 Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza"; see also Human Rights Watch, "Questions and Answers: Israeli Military's Use of Digital Tools in Gaza," September 10, 2024, https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza.

a vital fuel for the rise of Israel's vaunted technology sector",[115] including, most probably, the training of the AI DSS that have drawn so much media attention.[116]

Gospel reportedly processes data to provide Israeli forces with "automatic recommendations for attacking private residences where people suspected of being Hamas or Islamic Jihad operatives live", privileging "quantity over quality".[117] Some describe it as a system that generates suggestions for buildings that might be potential military objectives.[118] There are different takes on how the target lists—reportedly classified into four categories[119]—are treated. The IDF states that Gospel provides recommendations of targets for intelligence researchers based on "rapid and automatic extraction of intelligence", and that these suggested targets are further examined by operational and legal advisory teams.[120] However, available reporting on Gospel suggests that this process results in lists of potential targets that are then considered by military personnel "according to a checklist".[121] An inside source goes on to describe this as a factory-like process: "there is no time to delve deep into the target. The view is that we are judged according to how many targets we manage to generate".[122] Subsequently, other military personnel "will go over the targets before each attack, but [...] need not spend a lot of time on them".[123]

Reporting on Lavender goes into more detail in describing how the system processes surveillance data about Gaza's 2.3 million inhabitants to estimate "the likelihood that each particular person is active in the military wing of Hamas or PIJ" using a scale from 1-100.[124] Such estimates are reportedly the result of machine learning processes. Lavender is trained on data that contains known, particular characteristics identifying Hamas/PIJ operatives and attempts to find similar characteristics in the available data, thereby generating more suspected operatives.[125] According to reports, the procedure of generating 'human targets' departs significantly from previous IDF practice. Sources characterized previous practice as a human-labour intensive process of verifying whether a potential 'human target' was indeed a senior Hamas operative, cross-checking their private address, as well as locating "when he was home in real time".[126]

Investigations from +972 suggest that IDF intelligence personnel only checked samples of the Lavender-generated target list in this way for the first two weeks of the latest war (2023-) and ceased to do so when the sample-check was reported to have an accuracy rate of 90%.[127] At that point, the Lavender-generated target list was apparently taken as "an order" that required no further

115 MENAFN, "The Future of AI Warfare Is Taking Place in Israel without Oversight," August 14, 2023, https://menafn.com/1106851881/The-Future-of-AI-Warfare-Is-Taking-Place-in-Israel-Without-Oversight; see also Emad Moussa, "Israeli AI Is Turning Palestine into a Dystopian Reality," *The New Arab*, June 22, 2023, https://www.newarab.com/opinion/israeli-ai-turning-palestine-dystopian-reality.

116 Brianna Rosen, "Unhuman Killings: AI and Civilian Harm in Gaza," *Just Security*, December 15, 2023, https://www.justsecurity.org/90676/unhuman-killings-ai-and-civilian-harm-in-gaza/; Human Rights Watch, "Questions and Answers: Israeli Military's Use of Digital Tools in Gaza"; Lucy Suchman, "The Algorithmically Accelerated Killing Machine," *AI Now Institute*, January 24, 2024, https://ainowinstitute.org/publication/the-algorithmically-accelerated-killing-machine.

117 Abraham, "'A Mass Assassination Factory': Inside Israel's Calculated Bombing in Gaza"; Abraham quoted in France 24, "Understanding How Israel Uses 'Gospel' AI System in Gaza Bombings," December 12, 2023, https://www.france24.com/en/tv-shows/perspective/20231212-understanding-how-israel-uses-gospel-ai-system-in-gaza-bombings.

118 Michael N. Schmitt, "Israel-Hamas 2024 Symposium - The Gospel, Lavender, and the Law of Armed Conflict," *Lieber Institute West Point*, June 28, 2024, https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/.

119 Human Rights Watch, "Questions and Answers: Israeli Military's Use of Digital Tools in Gaza."

120 Davies, McKernan, and Sabbagh, "'The Gospel'"; Mimran and Dahan, "Artificial Intelligence in the Battlefield."

121 Source quoted in Abraham, "'A Mass Assassination Factory': Inside Israel's Calculated Bombing in Gaza."

122 Source quoted in Abraham.

123 Abraham.

124 Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza."

125 Abraham.

126 Abraham.

127 Abraham.

cross-checks by military personnel.[128] Military personnel reportedly initially spent 20 seconds on each target, "mak[ing] sure the Lavender-marked target is male".[129] In response to these reports, the IDF released a statement in June 2024 asserting that both Gospel and Lavender are "merely tools that help intelligence analysts cross-reference existing intelligence sources comprehensively and effectively" and insisting that target identification is always conducted by human analysts.[130] Some analysts describe Lavender as intended to be an "intelligence repository which allows users to visualize persons of interest", but in practice, it has been potentially used as a "validation tool" by the IDF in the latest phase of the Israel-Hamas war.[131]

The tracking system "Where's Daddy" appears to use mobile phone location data and target lists generated by other AI DSS at the tactical level.[132] This points to increasing trends of machine-machine interaction that are also becoming visible in the military domain. Reports from February 2023 indicate that the IDF had already developed unmanned, tracking systems to be used in conjunction with, for example, Alchemist and Gospel.[133] Col. Yoav, then commander of the Artificial Intelligence Center of IDF Unit 8200, said that the unnamed system "knows how to locate dangerous people based on the input of a list of previously incriminated people"—a functionality that is clearly reminiscent of what has been reported about Where's Daddy?[134] Yoav highlighted drastically reduced time frames associated with the use of the system "[...] a process that used to take hundreds of hours now takes mere seconds".[135]

Damage following an Israeli airstrike in Gaza City on October 9, 2023. **Source:** Palestinian News & Information Agency (Wafa) in contract with APAimages, via Wikimedia Commons.

128 Abraham.

129 Abraham.

130 Israel Defense Forces, "The IDF's Use of Data Technologies in Intelligence Processing," June 18, 2024, https://www.idf.il/210062; see also "Israel Defence Forces' Response to Claims about Use of 'Lavender' AI Database in Gaza" published in *The Guardian*, April 3, 2024, https://www.theguardian.com/world/2024/apr/03/israel-defence-forces-response-to-claims-about-use-of-lavender-ai-database-in-gaza.

131 Christopher Elliott, "Expedient or Reckless? Reconciling Opposing Accounts of the IDF's Use of AI in Gaza," *Opinio Juris*, April 26, 2024, https://opiniojuris.org/2024/04/26/expedient-or-reckless-reconciling-opposing-accounts-of-the-idfs-use-of-ai-in-gaza/.

132 Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza."

133 Cybertech, "IDF Used Artificial Intelligence to Expose Hamas Commanders, Says Top IDF Commander," *Israel Defense*, February 14, 2023, https://www.israeldefense.co.il/en/node/57246.

134 Cybertech.

135 Yuval Mann, "Israeli Officer Reveals How AI Is Being Utilized in Fight against Terror," *Ynetnews*, February 14, 2023, https://www.ynetnews.com/business/article/hk0drb00po.

Box 3 Select developments around the world

Many other actors strive to develop AI-based systems for decision-making on the use of force. However, details about the technological capabilities of AI DSS, how these are intended to be used, and the extent of their integration into targeting decisions are often scarce in the open-source domain.

China

While it is challenging to point towards specific AI technologies used by the Chinese military, China's Ministry of National Defence has been dedicated to developing systems that "autonomously carry out the cycle of reconnaissance, identification, strike, and evaluation until the corresponding operational objectives are achieved".[136] China's efforts to develop AI DSS are evident through the establishment of specialized institutions. For instance, the China Electronics Technology Group Corporation (CETC), a state-owned military corporation, partnered with Baidu to establish the "Joint Laboratory for Intelligent Command and Control Technology" in Nanjing, aimed at investigating the use of AI technologies in DSS.[137] In 2018, the China Institute of Command and Control formed the Intelligent Command and Control Systems Engineering Specialist Committee to coordinate AI development in military command and control by bringing together experts from various of disciplines.[138]

In publicly available statements and debates, the Chinese military emphasizes the coordination and cooperation between DSS and weapon systems to build a cloud-based network, particularly leveraging quantum computing.[139] The Chinese Navy, in collaboration with China Shipbuilding Industry Corporation, has reportedly developed and integrated AI DSS in their nuclear submarine.[140] Moreover, in the 2020 Military Intelligent Technology and Equipment Expo in Beijing, the CETC introduced the "Live Combat Simulation System" which simulates combat scenarios involving a broad range of weaponry.[141] This system appears to conduct a form of computerized weaponeering analysis to predict the types of injuries and secondary effects caused by different weapon systems.[142]

136 Dong Wei and Gao Kai, "The Intelligentization of Warfare Calls for Intelligentized Command [智能化战争呼唤指挥智能化]," *China National Defense News via the Ministry of National Defence*, June 26, 2019, http://www.mod.gov.cn/gfbw/jmsd/4844369.html.

137 CETC No. 28 Research Institute, "The CETC No. 28 Research Institute and Baidu Have Established the Laboratory for Intelligent Command and Control to Advance Military-Civil Integration into New Technological Fields [中国电科28所与百度公司成立'智能指挥控制技术联合实验室' 推动军民融合向新技术领域纵深迈进]," *Sohu*, January 23, 2018, https://www.sohu.com/a/218485100_779538#google_vignette.

138 Elsa Kania, "Artificial Intelligence in Future Chinese Command Decision Making," in *Artificial Intelligence, China, Russia, and the Global Order*, ed. Nicholas D. Wright (Maxwell Air Force Base: Air University Press, 2019), 153–61.

139 Chen Zhihua, Zhang Yong, and Liu Yuanhang, "Artificial Intelligence Shapes New Characteristics of Operational Command [人工智能塑造作战指挥要素新特点]," *China Social Sciences Net*, April 11, 2023, https://www.cssn.cn/jsx/jsx_xxqj/202304/t20230411_5619180.shtml; Huang Ping, Zhang Haoyue, and Shen Qiyou, "Unveiling the Secrets of Intelligent Unmanned Swarm Operations [揭开智能化无人集群作战的面纱]," *China Military Online*, August 25, 2020, http://www.81.cn/pl_208541/jdt_208542/9889510.html.

140 Elsa B. Kania, "Chinese Sub Commanders May Get AI Help for Decision-Making," *Defense One*, February 12, 2018, https://www.defenseone.com/ideas/2018/02/chinese-sub-commanders-may-get-ai-help-decision-making/145906/.

141 Ma Jun and Liu Yang, "Exploring the China Military Intelligent Equipment Exhibition: New Technologies and Equipment Such as Intelligentized Command, Intelligentized Recognition, and Intelligentized Control Have Become a Reality [探访中国军事智能装备展：智能化指挥、智能化识别、智能化控制等新技术和装备已成为现实]," *Global Times*, September 23, 2020, https://world.huanqiu.com/article/3zzfZeNbfKP; Zhao Wei, Ye Jun and Wang Bin, "AI-based Command, Control, and Decision-making [基于人工智能的智能化指挥决策和控制]," *Information Security and Communication Confidentiality*, 2 (2022), 2–8.

142 Ma Jun and Liu Yang, "Exploring the China Military Intelligent Equipment Exhibition."

France

The French Armed Forces Ministry is actively implementing AI and machine learning solutions, including the big data platform ARTEMIS, co-designed by companies Thales and Atos to process large amounts of data collected via sensors and military equipment such as drones. The platform would, among other use cases, assist with administrative tasks such as health planning for soldiers and scheduling the availability of military personnel, be used in a maritime context to analyse locations of vessels, and help analysts of the French marines to "decide better and faster", as stated by the French Directorate General of Armaments.[143]

NATO

In 2023 the NATO Science and Technology Organization tested a new system called ANTICIPE, developed by French company Thales and intended to "aid decision-making in an operational setting".[144] ANTICIPE integrates a wargaming tool and information from various sources such as social media processed via machine learning algorithms.

The United Kingdom

The UK Royal Navy worked with companies such as Microsoft, Amazon Web Services, BAE Systems, and Anduril to develop Project StormCloud, a network of systems, software, drones, and cloud technology designed to "enhance missions ranging from warfare operations to humanitarian assistance".[145] The demonstration of StormCloud in 2022 featured software which "identified objects on the ground and suggested which weapon to strike which target", described by a participant as "the world's most advanced kill chain" (quoted in *The Economist*).[146] The UK Ministry of Defence has also highlighted the use of machine learning techniques to analyse satellite imagery, detect, and identify objects as part of its Project SPOTTER.[147]

AI DSS appear to integrate various sources of data, are employed a different steps of targeting decision-making, and often speed up the process of target generation

In summary, this section offered a brief overview of various reported uses of AI DSS and their main functions according to the information available. At the same time, these reports offer important insights into the main trends of AI DSS development and use around the world. Notably, AI DSS appear to integrate various sources of data, are employed at different steps of targeting decision-making, and often speed up the process of target generation. The table below reviews the main functions of the systems mentioned in this section and illustrates how these systems fit into the three broad types of AI DSS identified in section 2 (see figure 2), based on the functions attributed to them. It is important to note that these functions are not mutually exclusive, and that a system might correspond to different types of AI DSS.

143 French Directorate General of Armaments, "ARTEMIS-IA : Massive Data Processing for Defence [ARTEMIS-IA : traitement massif de données pour la défense]," *YouTube*, November 25, 2021, https://www.youtube.com/watch?v=DunRRGOYCAM; Alice Vitard, "Artemis.IA, the Military's Big Data Platform, Enters the Industrialization Phase [Artemis.IA, la plateforme de big data des armées, entre en phase d'industrialisation]," *L'usine digitale*, July 18, 2022, https://www.usine-digitale.fr/article/artemis-ia-la-plateforme-de-big-data-des-armees-entre-en-phase-d-industrialisation.N2027197.

144 NATO Science & Technology Organization, "Using Artificial Intelligence to Enhance Military Decision-Making," *YouTube*, April 3, 2024, https://www.youtube.com/watch?v=A2ZAHrT3UwM; see also Ian Reynolds and Yasir Atalan, Calibrating NATO's Vision of AI-Enabled Decision Support," *Center for Strategic and International Studies*, July 8, 2024, https://www.csis.org/analysis/calibrating-natos-vision-ai-enabled-decision-support.

145 Royal Navy, "Royal Navy Works with Tech Giants to Embrace Innovation at Debut Event," June 17, 2022, https://www.royalnavy.mod.uk/news-and-latest-activity/news/2022/june/17/220617-royal-navy-stormcloud.

146 Joshi, "How AI Is Changing Warfare."

147 UK Ministry of Defence, *Defence Artificial Intelligence Strategy* (London: UK MoD, 2022), 43.

Table 1 Examples of AI DSS and overview of their main functions

Name of system	Used by	Main functions (according to available information)	Relevant types of AI DSS
Skynet	The US	To process data to analyse patterns and identify couriers passing messages to and from terrorist organizations	**Description and analysis** of collected data **Prediction** of individuals' networks and roles based on the data
Project Maven	The US	To process information, find potential targets, and present the information to decision-makers	**Description and analysis** of collected data **Recommendation** of potential targets (double-checked by humans)
Palantir's MetaConstellations software	Ukraine	To detect adversary positions, objects and key information, to inform decision-making	**Description and analysis** of collected data
Kropyva	Ukraine	To automate command and control, tactical operations and artillery calculations, to locate adversary positions	**Description and analysis** of collected data
GIS Arta	Ukraine	To assign missions to artillery based on optimized factors	**Description and analysis** of collected data
Griselda	Ukraine	To collect intelligence, process information, and locate adversary positions	**Description and analysis** of collected data
Acacia-M	Russia	To send real-time data analysis about the state of the battlefield and adversary positions to the commander	**Description and analysis** of collected data
Bylina EW complex	Russia	To analyse the battlefield, find most efficient ways to jam radars/radios, and detect adversary positions	**Description and analysis** of collected data
Alchemist	Israel	To collect intelligence, process information, and alert troops about possible attacks	**Description and analysis** of collected data
Gospel	Israel	To process data to analyse patterns and identify target objects (e.g., buildings)	**Description and analysis** of collected data **Identification** of potential targets (double-checked by humans)
Lavender	Israel	To process data to analyse patterns and identify human targets	**Description and analysis** of collected data **Identification** of potential targets (double-checked by humans)
Where's Daddy	Israel	To geo-track previously identified targets and recommend timing for the use of force	**Description and analysis** of collected data

4 Opportunities and Challenges Associated with AI DSS

The developments explored in section 3 have inspired a wide range of discussions surrounding the opportunities associated with AI DSS and how they are being used, but also various risks and challenges that arise from such practices. This section provides an overview of different perspectives on both opportunities and concerns, while drawing on illustrations from section 3, with a particular focus on the issue of human-machine interaction in warfare. As the uses of specific AI DSS in the ongoing Israel-Hamas war (2023-) are by far the most well-reported in open-source documentation, many of the examples in the following will be drawn from this case. This case is also illustrative of the challenges raised by using AI DSS where hostilities are conducted in urban and populated areas.

4.1 Opportunities

Potential strategic opportunities

From a military perspective, the main opportunities associated with integrating AI DSS into military decision-making on the use of force are greater speed and scale. The command and control process requires considering significant amounts of information about a certain situation, accounting for various scenarios, and constantly monitoring new information coming in, while addressing uncertainties which might affect how military personnel perform decision-making tasks. With more data being collected via surveillance, drone footage, satellite imagery, and many other types of sources, it could take days, weeks, months, or years for human analysts to go through all the necessary information and make decisions taking everything into consideration. Drawing on computation, AI, and machine learning techniques to assist with processing and analysing the volumes of intelligence and information from and across different sources is at the core of developing AI DSS.[148] As noted by Lt. Gen. Jack Shanahan (US Air Force, retired), the inaugural Director of Project Maven, "AI's most valuable contributions will come from how we use it to make better and faster decisions"[149]—a belief that is echoed across other parts of the world.[150]

Drawing on AI and machine learning techniques to assist with processing and analysing the volumes of intelligence from across different sources is at the core of developing AI DSS

148 Boulanin, "Risks and Benefits of AI-Enabled Military Decision-Making," 105–6.

149 US Department of Defense, "Lt. Gen. Jack Shanahan Media Briefing."

150 For overviews of various initiatives in military applications of AI, see Michael Raska and Richard A. Bitzinger, eds., *The AI Wave in Defence Innovation* (Abingdon and New York: Routledge, 2023); Heiko Borchert, Torben Schütz, and Joseph Verbovszky, eds., *The Very Long Game: 25 Case Studies on the Global State of Defense AI* (Cham: Springer Nature Switzerland, 2024).

Militaries, as many other large bureaucratic organizations, are looking to improve the efficiency of their work and ensure that their tasks are streamlined.[151] This extends to logistics, human resources, and maintenance, among others, but is particularly relevant for combat and targeting because speed and efficiency are considered key factors of success on the battlefield. Employing AI-based systems which would process information faster is often linked to speeding up the so-called OODA loop (see section 2), thereby allowing commanders to make faster decisions, and subsequently, militaries reaching their objectives more rapidly—importantly, in comparison to their adversaries.[152] Military officials refer to this as gaining a strategic or 'decision advantage', conceptualized as "processing large amounts of information quickly to be able to act first" on the battlefield.[153] For instance, NGA Director Frank Whitworth said that "being able to sift through the barrage of data and discern a target from non-target – with high accuracy, based on unique behavior, at the speed of conflict – is key to maintaining our decision advantage".[154] Moreover, observers have been drawing lessons from Ukrainian experiences of conducting strikes on Russian positions based on intelligence processes with AI DSS. According to Ukrainian officials, integrating data analysis from such systems has important strategic value and has assisted the Ukrainian army in liberating several cities, including Kyiv, from Russian forces.[155]

It should be added that the efficiency of AI technologies in military operations is associated with teaming humans and machines together, rather than relying on AI technologies used in isolation. One of the key values of human-machine teaming is considered to be the potential to enhance situational awareness, or the militaries' understanding of a battlefield situation.[156] These efficiency and speed gains come from pairing AI DSS "with human analysts who possess detailed understanding of the operational environment", not AI being a "standalone tool" or replacing humans.[157] This line of thinking rests on the proposition that humans using AI DSS represents a militarily advantageous combination—the best of both worlds.

Potential humanitarian opportunities

Experts also highlight potential humanitarian opportunities of using AI DSS. Disposing of the right tools for more efficient decision-making could increase the chances of complying with international law, for instance by presenting relevant information for decisions on proportionality, distinction, or precautions. As the International Committee of the Red Cross points out, AI- and machine learning-based systems "can facilitate faster and broader collection and analysis of available information", which "may enable better decisions by humans in conducting military operations in compliance with

151 Meerveld et al., "The Irresponsibility of Not Using AI in the Military," 13.

152 For instance, the IDF's Gospel system is described as imitating "what a group of intelligence officers used to do in the past" in a "much more efficient" way. Mimran quoted in Geoff Brumfiel, "Israel Is Using an AI System to Find Targets in Gaza. Experts Say It's Just the Start," *NPR*, December 14, 2023, https://www.npr.org/2023/12/14/1218643254/israel-is-using-an-ai-system-to-find-targets-in-gaza-experts-say-its-just-the-st.

153 Bo and Dorsey, "The 'Need' for Speed – The Cost of Unregulated AI Decision-Support Systems to Civilians"; see also NATO Science and Technology Organization, "Using Artificial Intelligence to Enhance Military Decision-Making."

154 NGA, "Remarks as Prepared for NGA Director Vice Adm. Frank Whitworth for 2024 GEOINT Symposium"; see also Whitworth in Palantir, "Accelerating Decision Making."

155 Ignatius, "How the Algorithm Tipped the Balance in Ukraine"; see also King, "Digital Targeting," 13.

156 Tate Nurkin and Julia Siegel, *Battlefield Applications for Human-Machine Teaming: Demonstrating Value, Experimenting with New Capabilities and Accelerating Adoption* (Washington, DC: Atlantic Council, Scowcroft Center for Strategy and Security, 2023).

157 Eric Robinson, Daniel Egel, and George Bailey, *Machine Learning for Operational Decisionmaking in Competition and Conflict: A Demonstration Using the Conflict in Eastern Ukraine* (Santa Monica, CA: RAND Corporation, 2023), 49; Kenneth Payne, "Artificial Intelligence and the Nature of War," in *Beyond Ukraine: Debating the Future of War*, ed. Tim Sweijs and Jeffrey H. Michaels (London: Hurst, 2024), 223–40.

IHL [international humanitarian law, which governs armed conflict] and minimizing risks for civilians".[158] If they provide context-specific and relevant information, AI DSS could facilitate ethical and legally-compliant decision-making.[159]

Integrating AI DSS into the planning of operations can assist in the protection of human rights, especially civilians' rights, before, during, and following armed conflicts. AI tools are not 'silver bullets' in conflict prevention or harm mitigation, considering the complex and multi-faceted nature of warfare. However, some uses of AI DSS can contribute to reducing harm done to civilians. This includes, among others, analysing satellite imagery and other types of data with the objective of issuing early warnings to civilians in risk zones so that they can flee or evaluating expected damage on infrastructure such as powerplants.[160] While not strictly related to the use of force, AI DSS can be also used in de-mining operations, as is the case in Ukraine, where Ukrainian authorities use Palantir's Artificial Intelligence Platform (AIP) for decision-making in humanitarian demining.[161]

AI tools are not 'silver bullets' in conflict prevention or harm mitigation, considering the complex and multi-faceted nature of warfare. However, some uses of AI DSS can contribute to reducing harm done to civilians

A sign warning about landmines in 2022 in the Kharkiv region, Ukraine.
Source: State Emergency Service of Ukraine in Kharkiv Oblast, via Wikimedia Commons.

More generally, academic and policy debates note that some uses of AI DSS might be less concerning than others, not only in a strategic sense but also in terms of compliance with principles such as precautions. For some tasks, especially in controlled scenarios with predictable conditions, the stakes will be relatively low. For other use cases and contexts, however, AI DSS raise several challenges and concerns that deserve to be debated further.

158 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (Geneva: ICRC, 2019), 32; Anna Rosalie Greipl, "Artificial Intelligence in Urban Warfare: Opportunities to Enhance the Protection of Civilians?" *The Military Law and the Law of War Review* 61, no. 2 (2023): 191–211, https://doi.org/10.4337/mllwr.2023.02.03.

159 Franziska Poszler and Benjamin Lange, "The Impact of Intelligent Decision-Support Systems on Humans' Ethical Decision-Making: A Systematic Literature Review and an Integrated Framework," *Technological Forecasting and Social Change* 204 (2024): 123403, https://doi.org/10.1016/j.techfore.2024.123403; Niyi Ogunbiyi, Artie Basukoski, and Thierry Chaussalet, "An Exploration of Ethical Decision Making with Intelligence Augmentation," *Social Sciences* 10, no. 2 (2021): 57, https://doi.org/10.3390/socsci10020057.

160 Branka Panic and Paige Arthur, *AI for Peace* (Boca Raton: CRC Press, 2024); Larry Lewis and Andrew Ilachinski, *Leveraging AI to Mitigate Civilian Harm* (Arlington, VA: Center for Naval Analyses, 2022); Anna Rosalie Greipl, "Artificial Intelligence for Better Protection of Civilians during Urban Warfare," *Lieber Institute West Point*, March 26, 2024, https://lieber.westpoint.edu/artificial-intelligence-better-protection-civilians-urban-warfare/.

161 Palantir, "Palantir and Ministry of Economy of Ukraine Sign Demining Partnership," March 4, 2024, https://investors.palantir.com/news-details/2024/Palantir-and-Ministry-of-Economy-of-Ukraine-Sign-Demining-Partnership/; Vera Bergengruen, "Ukraine Is Using AI to Help Clear Millions of Russian Landmines," *TIME*, November 2, 2023, https://time.com/6330445/demining-ukraine/.

4.2 Challenges and risks

The following sub-sections summarize challenges and risks associated with AI DSS in use-of-force decision-making. While these sections do not offer detailed scrutiny of all arguments, they include references to studies which expand on each of the issues mentioned.

Dynamics of human-machine interaction in AI DSS

One of the most discussed issues in relation to AI DSS relates to the role of humans in their interactions with machines. The extent to which humans can exercise meaningful forms of control over the use of force has long been a key concern in the debate about weapon systems integrating autonomy and AI for legal, ethical, normative, and security reasons.[162] Just to name one, retaining human accountability for outcomes of military actions is necessary for ensuring compliance with IHL. Guaranteeing a meaningful role for the human in practice has been the topic of ongoing discussions. Some of the questions as part of these debates also have relevance in the case of AI DSS. After all, military personnel interact with AI DSS throughout the targeting process, a process that involves users sharing or offloading some 'cognitive' functions to systems in the sense of "delegating 'thinking' tasks to AI technologies".[163]

Processes of human-machine interaction in the context of using AI DSS are bound to affect the exercise of human agency in the use of force

Processes of human-machine interaction are bound to affect the exercise of human agency in the use of force. Human agency can be broadly defined as the capacity to understand the context, make deliberate decisions, and act upon these decisions in a way that responsibility is ensured.[164] For instance, when a system presents a human with one option or a set of limited options, it makes it challenging to choose other pathways. This raises concerns about the space and time left for humans to exercise agency in use-of-force decision-making and the conduct of war, which is a deeply human, social, and political process.[165]

Human-machine interaction challenges associated with AI DSS

162 On the issue of human control, see Vincent Boulanin et al., *Limits of Autonomy in Weapon Systems: Identifying Practical Elements of Human Control* (Stockholm: Stockholm International Peace Research Institute & ICRC, 2020); Lena Trabucco, "What Is Meaningful Human Control Anyway? Cracking the Code on Autonomous Weapons and Human Judgment," *Modern War Institute at West Point*, September 21, 2023, https://mwi.westpoint.edu/what-is-meaningful-human-control-anyway-cracking-the-code-on-autonomous-weapons-and-human-judgment/.

163 Sandra Grinschgl and Aljoscha C. Neubauer, "Supporting Cognition with Modern Technology: Distributed Cognition Today and in an AI-Enhanced Future," *Frontiers in Artificial Intelligence* 5 (2022): 1, https://doi.org/10.3389/frai.2022.908261.

164 Ingvild Bode, *Human-Machine Interaction and Human Agency in the Military Domain* (Centre for International Governance Innovation Policy Brief, forthcoming).

165 Brad Boyd, "Agent Smith Is Not Your Targeteer," *Killer Robot Cocktail Party*, April 19, 2024, https://killerrobotcocktailparty.substack.com/p/agent-smith-is-not-your-targeteer.

U.S. Army photo by CPT Alex Werden. The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

Biases are likely to be exacerbated by the increased speed of decision-making integrating AI DSS

Increased and routine interactions with AI DSS have potential to challenge "independent and subjective judgements" by humans.[166] Distinguishing between human and machine agency has become increasingly difficult, making it important to examine dynamics of human-machine interaction as part of a socio-technical system, rather than a binary separation between 'human' and 'AI' capabilities.[167] Such a dichotomous view is noticeable, for instance, in the anthropomorphizing of AI DSS, such as the headline "the machine did it coldly" in a *Guardian* article about Israel's use of Lavender.[168] However, concerns associated with AI DSS are not about robots replacing humans in decision-making, but making "human decision-making too robotic, essentially transforming human operators themselves into 'killer robots'" due to distributed agency in use-of-force decision-making.[169]

Human decision-making in interaction with AI technologies is also subject to a range of well-documented cognitive biases, including automation bias (see next sub-section on trust-related issues).[170] Bo and Dorsey define cognitive action bias as "the human tendency to take action, even when inaction would logically result in a better outcome".[171] Such biases are likely to be exacerbated by the increased speed of decision-making. Speed is often considered as one of

166 Klaudia Klonowska, "Designing for Reasonableness: The Algorithmic Mediation of Reasonableness in Targeting Decisions," *Lieber Institute West Point*, February 23, 2024, https://lieber.westpoint.edu/designing-reasonableness-algorithmic-mediation-reasonableness-targeting-decisions/.

167 Anna Rosalie Greipl, "Artificial Intelligence Systems and Humans in Military Decision-Making; Not Better or Worse but Better Together," *Lieber Institute West Point*, June 14, 2024, https://lieber.westpoint.edu/artificial-intelligence-systems-humans-military-decision-making-better-worse/; Erica Harper, "Will AI Fundamentally Alter How Wars Are Initiated, Fought and Concluded?" *ICRC Humanitarian Law & Policy Blog*, September 26, 2024, https://blogs.icrc.org/law-and-policy/2024/09/26/will-ai-fundamentally-alter-how-wars-are-initiated-fought-and-concluded/.

168 McKernan and Davies, "'The Machine Did It Coldly'."

169 Charli Carpenter, "The Real 'Killer Robots' Are Already Here—and They're Us," *World Politics Review*, April 23, 2024, https://www.worldpoliticsreview.com/killer-robots-ai-israel-gaza/.

170 Ingvild Bode and Ishmael Bhila, "The Problem of Algorithmic Bias in AI-Based Military Decision Support Systems," *ICRC Humanitarian Law & Policy Blog*, September 3, 2024, https://blogs.icrc.org/law-and-policy/2024/09/03/the-problem-of-algorithmic-bias-in-ai-based-military-decision-support-systems/.

171 Bo and Dorsey, "The 'Need' for Speed – The Cost of Unregulated AI Decision-Support Systems to Civilians."

the opportunities of using AI DSS, but it also shortens the timeframe available to exercise human agency.[172] There are suggestions that such trends of human-machine interaction are already happening, especially in situations characterized by intense pressure and faster targeting processes.

The Ukrainian armed forces' experience suggests that "in practice, there are only two to five seconds between target identification and engagement, which is hardly enough for a human operator to make a balanced decision… this bears the risk that involving a 'human in the loop' becomes a 'formality' that might render the target-engagement cycle more difficult".[173] A senior US targeting expert told *Bloomberg* that using the Maven system allows him to "sign off on as many as 80 targets in an hour of work, versus 30 without it", describing the "process of concurring with the algorithm's conclusions in a rapid staccato: Accept. Accept. Accept".[174] Similarly, there are suggestions that IDF personnel have been more likely to accept target recommendations provided by AI DSS, especially in situations of pressure.[175] In investigative reporting on the Lavender system, a source states that IDF personnel treated AI DSS outputs "as if it were a human decision".[176]

There is a risk that AI DSS are treated as "boxes that need to be checked", further undermining the possibility and/or willingness to verify the outputs and reflect upon them critically

These reports put significant question marks behind the quality of human agency exercised by military personnel in handling target recommendations based on algorithmic outputs. As section 2 notes, operators are likely to use AI DSS as part of a complex network of multiple systems—as the IDF's use of several AI DSS illustrates. Even when the use of DSS is not speedy, the increased complexity raises risks of humans acting upon some outputs without exercising the judgement appropriate for the context. This could also be related to the graphic design of AI DSS interfaces and how they present information, for instance the colours used. Human-machine interaction and distributed agency encompass a variety of issues, which are interconnected with various concerns explored in the sub-sections below.

Issues related to trust

Another challenge relates to humans' trust in the outputs of computerized tools. Operators could over-trust outputs from AI DSS without engaging in the necessary critical legal and strategic reflections about the implications of a certain military decision, even when knowing that relying on the system's outputs might lead to mistakes or unintended results. Trust in automated and AI systems, also known as automation bias, is a well-documented phenomenon in research across various fields such as healthcare, transport, and aviation.[177] By relying too much on a system's output without critically assessing it, especially in conditions of speed and complexity, humans risk 'rubber stamping' decisions and courses of action. This is especially likely when the system's output confirms or matches the human user's existing beliefs, perceptions, or stances.

172 Klaudia Klonowska, "Israel-Hamas 2024 Symposium: AI-Based Targeting in Gaza: Surveying Expert Responses and Refining the Debate," *Lieber Institute West Point*, June 7, 2024, https://lieber.westpoint.edu/ai-based-targeting-gaza-surveying-expert-responses-refining-debate/.

173 Goncharuk, *Survival of the Smartest? Defense AI in Ukraine*, 11.

174 Manson, "AI Warfare Is Already Here."

175 Brumfiel, "Israel Is Using an AI System to Find Targets in Gaza. Experts Say It's Just the Start."

176 Quoted in Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza."

177 Shannon E. French and Lisa N. Lindsay, "Artificial Intelligence in Military Decision-Making: Avoiding Ethical and Strategic Perils with an Option-Generator Model," in *Emerging Military Technologies*, ed. Bernhard Koch and Richard Schoonhoven (Leiden: Brill | Nijhoff, 2022), 53–60; David Lyell and Enrico Coiera, "Automation Bias and Verification Complexity: A Systematic Review," *Journal of the American Medical Informatics Association* 24, no. 2 (2017): 423–31, https://doi.org/10.1093/jamia/ocw105; Michael C .Horowitz and Lauren Kahn, "Bending the Automation Bias Curve: A Study of Human and AI-Based Decision Making in National Security Contexts," *International Studies Quarterly* 68, no. 2 (2024): sqae020, https://doi.org/10.1093/isq/sqae020; Antonio Coco, "Exploring the Impact of Automation Bias and Complacency on Individual Criminal Responsibility for War Crimes," *Journal of International Criminal Justice* 21 (2023): 1077–96, https://doi.org/10.1093/jicj/mqad034.

U.S. Department of Defense photo by Spc. Jeffery Harris. The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

Military decision-makers do not use 'ready-made' AI DSS that were 'out there' and developed somehow distinctly, separately from social and military processes. Rather, a range of actors made key choices about parameters of designing and using the systems

There is a risk that AI DSS are treated as "boxes that need to be checked",[178] further undermining the possibility and/or willingness to verify the outputs and reflect upon them critically. For instance, some experts argue that although not intended as such, in practice systems such as Gospel and Lavender became tools "whose suppositions are promptly greenlit by target engagement authorities without much deliberation".[179] The "20 seconds" that IDF military personnel reportedly allocated to checking each target would not allow sufficient time to question and examine the intelligence data that the system's output is based on—despite the fact that such outputs contain known error margins.[180] Such dynamics are not only related to the use of AI systems, but also the whole social context, for instance the pressure to retaliate against Hamas' terrorist attacks,[181] highlighting the importance of treating this phenomenon as socio-technical.

Targeting doctrines and rules of engagement

AI, as other technologies, including those used in the military domain, are "products of their time".[182] They mirror the societies in which they are developed and used. Military decision-makers therefore do not use 'ready-made' AI DSS that were 'out there' and developed somehow distinctly, separately from social and military processes. Rather, a range of actors made key choices about parameters of designing and using the systems. Such choices should also be considered within a social context, which in the military sphere includes targeting doctrines and RoE. The case of the IDF's reported uses of AI DSS particularly illustrates these dynamics.

Before striking targets, all militaries are legally obliged to make assessments of proportionality, prohibiting "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and

178 Holland Michel, *Decisions, Decisions, Decisions*, 48.

179 Elliott, "Expedient or Reckless?"

180 Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza."

181 Kenneth Payne, "IDF AI?" *Ken's Substack*, December 12, 2023, https://www.kennethpayne.uk/p/idf-ai.

182 Wanda J. Orlikowski, "The Duality of Technology: Rethinking the Concept of Technology in Organizations," *Organization Science* 3, no. 3 (1992): 398.

direct military advantage anticipated".[183] Usually, such calculations are based on, typically software-assisted, estimates rather than firm knowledge of the exact numbers. Proportionality calculations underline the uneasy practice of balancing between humanitarian concerns and military impetus that characterizes the operational application of IHL and can stand in direct contrast with ethical concerns.

In other words, based on IHL, while targeting civilians and civilian objects is unlawful, killing civilians is not categorically unlawful but can be militarily justifiable. In this context, Crootof has argued how ways of using new weapon technologies such as AI DSS may exacerbate an "accountability chasm" that is inherent in how IHL "explicitly permits many acts that foster incidental harm".[184] What is considered as a militarily 'acceptable' civilian loss of life and destruction of civilian infrastructure is a factor of both broader targeting doctrines and specific RoE.

Israeli targeting doctrine has reportedly long been informed by the "deliberate application of disproportionate force, such as the destruction of an entire village, if deemed to be the source of rocket fire".[185] This so-called Dahiya Doctrine has been officially acknowledged by the IDF repeatedly, and has characterized IDF operations in Gaza since 2008.[186] The Dahiya Doctrine has been subject to significant critique for the ways in which it advocates the disproportionate application of force, civilian loss of life, and the destruction of civilian infrastructure.[187] For example, an in-depth UN report about the 2014 IDF air and ground operation in the Gaza Strip (7 July–26 August 2014) found that the IDF had conducted air strikes against "residential and other buildings" with as many as 742 people killed in their homes according to UN numbers.[188]

Some voices have suggested that IDF targeting practice after 7 October 2023 marks a doubling down or an even more adverse progression from the Dahiya Doctrine.[189] Reports further indicate changing RoE in how the IDF designates 'human targets' after 7 October with significant effects on the proportionality assessments underlying its targeting decisions. Previous doctrine restricted the designation of 'human target' to senior military leaders.[190] The IDF's October 2023 operation in Gaza reportedly no longer differentiated between levels of seniority among suspected Hamas operatives, designating all suspected operatives as 'human targets'.[191]

Reporting also points out that the scale of what the IDF counts as 'acceptable' numbers of civilians killed in the context of each attack against suspected Hamas-affiliated targets is significantly higher than previously.[192] Speaking shortly after the start of the Israeli offensive in Gaza, an IDF spokesperson noted that "while

183 International Committee of the Red Cross, "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)," August 8, 1977, art. 51 (5) (b), http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079.

184 Rebecca Crootof, "AI and the Actual IHL Accountability Gap," *Centre for International Governance Innovation*, November 28, 2022, https://www.cigionline.org/articles/ai-and-the-actual-ihl-accountability-gap/.

185 Paul Rogers, "Israel's Disproportionate Force Is a Long-Established Tactic - with a Clear Aim," *The Guardian*, December 5, 2023, https://www.theguardian.com/commentisfree/2023/dec/05/israel-disproportionate-force-tactic-infrastructure-economy-civilian-casualties.

186 Rogers.

187 Ayse Isin Kirenci, "'Cheap Stupid Bombs': What's the Dahiya Doctrine in Israel's War on Gaza?" *TRT World*, December 21, 2023, https://www.trtworld.com/middle-east/cheap-stupid-bombs-whats-the-dahiya-doctrine-in-israels-war-on-gaza-16332266.

188 United Nations Human Rights Council, *Report of the Independent International Commission of Inquiry on the Syrian Arab Republic*, UN Document A/HRC/27/60 (New York: United Nations, August 13, 2014), 32.

189 Quoted in Kirenci, "'Cheap Stupid Bombs': What's the Dahiya Doctrine in Israel's War on Gaza?"

190 Quoted in Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza."

191 Abraham, "'A Mass Assassination Factory': Inside Israel's Calculated Bombing in Gaza."

192 Abraham.

U.S. Air Force photo by Senior Airman Courtney Sebastianelli. The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

balancing accuracy with the scope of damage, right now we're focused on what causes maximum damage".[193] The IDF has been shown to strike "targets that are not distinctly military in nature", including private residences and public infrastructure.[194] This RoE choice appears to have been a continuation of previous targeting doctrine as similar IDF practices were already scrutinized in 2014. In these cases, human reliance on AI DSS outputs to generate targets comes with a distinctly higher risk of misidentification based on, for example, faulty, incomplete, or unrepresentative data (more on data-related issues below).

The use of AI DSS in general terms appears to allow militaries to generate unprecedented numbers of targets at higher speed. If then combined with targeting doctrines and RoE that 'allow' high civilian casualty rates, the use of AI DSS can have severe security and humanitarian effects. In Gaza, the IDF's military operations, which involve the use of AI DSS, have led to the widespread destruction of civilian infrastructure such as hospitals and an estimated civilian death toll of 41,020 (as of September 2024).[195] Another study estimates the civilian death toll to realistically be around 186,000 as official numbers do not account for those buried under destroyed buildings as well as indirect deaths associated with key health and food infrastructure having been destroyed.[196] These impacts are not, however, the outcome of the computational tools' outputs or their technical characteristics. Rather, they are the outcome of configurations of human-machine interactions which are part of a broader context, encompassing visions of war-making as well as strategic and institutional cultures.[197]

193 Quoted in Bethan McKernan and Quique Kierszenbaum, "'We're Focused on Maximum Damage': Ground Offensive into Gaza Seems Imminent," *The Guardian*, October 10, 2023, https://www.theguardian.com/world/2023/oct/10/right-now-it-is-one-day-at-a-time-life-on-israels-frontline-with-gaza. For discussions on the IDF's targeting practices, see Noah Sylvia, "The Israel Defense Forces' Use of AI in Gaza: A Case of Misplaced Purpose," *RUSI Commentary*, July 4, 2024, https://rusi.org/explore-our-research/publications/commentary/israel-defense-forces-use-ai-gaza-case-misplaced-purpose; John Merriam, "Israel – Hamas 2023 Symposium – Inside IDF Targeting," *Lieber Institute West Point*, October 20, 2023, https://lieber.westpoint.edu/inside-idf-targeting/.

194 Abraham, "'A Mass Assassination Factory': Inside Israel's Calculated Bombing in Gaza."

195 United Nations Office for the Coordination of Humanitarian Affairs, "Reported Impact Snapshot Gaza Strip 11 September 2024 at 15:00," September 11, 2024, https://www.unocha.org/publications/report/occupied-palestinian-territory/reported-impact-snapshot-gaza-strip-11-september-2024-1500.

196 Rasha Khatib, Martin McKee, and Salim Yusuf, "Counting the Dead in Gaza: Difficult but Essential," *The Lancet* 404, no. 10449 (2024): 237–38.

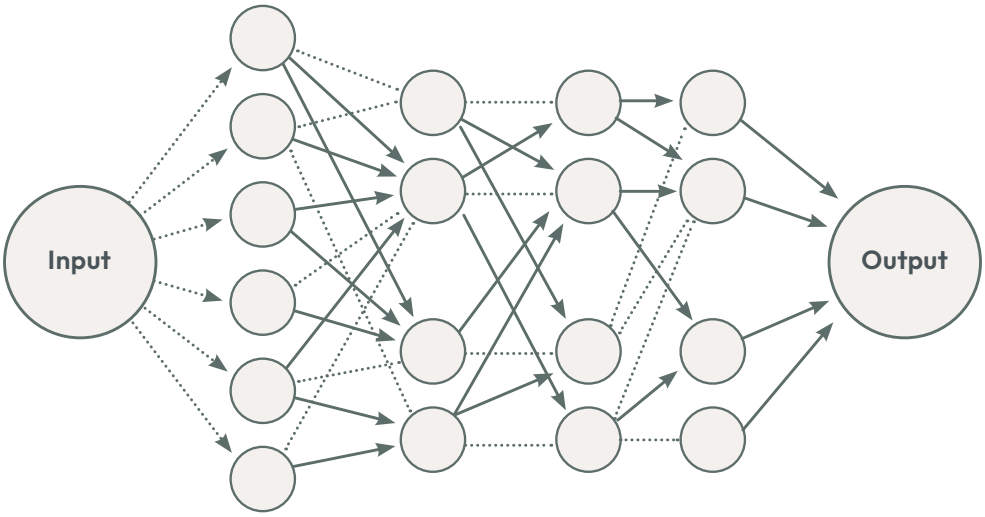
197 Jon R. Lindsay, "War Is from Mars, AI Is from Venus: Rediscovering the Institutional Context of Military Automation," *Texas National Security Review* 7, no. 1 (2024): 29–48.

Data-related issues and technical malfunctions

Many concerns relate to some technical aspects of AI DSS, especially in relation to data and malfunctions of algorithmic systems, which are common and documented across a variety of areas, not only in the military.[198] The 'performance' of AI DSS relies heavily on data availability and quality. In the military context, relevant training data is challenging to find. War is a complex, uncertain, and dynamic phenomenon. Data collected from previous contexts will often be historical, different, insufficient, or simply wrong.[199] This is a problem highlighted in relation to the data used to train the Skynet algorithm (see box 1) so that the system can adequately score profiles of individuals: there are not that many "known couriers" to set as "ground truths" which would allow algorithms to produce the score.[200]

The 'performance' of AI DSS relies heavily on data availability and quality. War is a complex, uncertain, and dynamic phenomenon. Data collected from previous contexts will often be historical, different, insufficient, or simply wrong

Many AI DSS analyse data linked to past behaviour categorized in numerical ways, such as frequency and duration of phone calls. Based on this data output, or "assembly of probable indices" such as "the number and frequency of contacts, regardless of their nature", decision-makers make estimates about someone's affiliations or identities, and therefore the legitimacy of targets.[201] In the case of Skynet, experts have highlighted the unclarity of the criteria used to identify suspected terrorist couriers.[202] For instance, Ahmad Muaffaq Zaidan, chief of *Al Jazeera*'s Islamabad office, was tracked and wrongly identified as a member of Al Qaeda due to his travel and phone call patterns. Zaidan's travels matched the 'suspicious' patterns and received a high score from the system, although this was related to his journalist work by meeting his contacts and reporting news in those regions. For some, this case represents a failure of the system and how it was used by the humans involved,[203] while others (including the NSA) rather saw this case as the algorithm working as it was designed.[204]



198 See the AI and Algorithmic Incidents and Controversies Repository, https://www.aiaaic.org/aiaaic-repository/ai-and-algorithmic-incidents-and-controversies.

199 Lindsay, "War Is from Mars, AI Is from Venus," 39; Boulanin, "Risks and Benefits of AI-Enabled Military Decision-Making," 103.

200 Grothoff and Porup, "The NSA's SKYNET Program May Be Killing Thousands of Innocent People."

201 Grégoire Chamayou, *Drone Theory* (London: Penguin Books, 2015), 49–51.

202 Klonowska, "Article 36," 138.

203 Grothoff and Porup, "The NSA's SKYNET Program May Be Killing Thousands of Innocent People."

204 Robbins, "Has a Rampaging AI Algorithm Really Killed Thousands in Pakistan?"

A common argument put forward in the debate to support the use of AI DSS is that human decision-making is prone to exhibit bias and tends to make incorrect decisions, especially when humans are overloaded with information. Notwithstanding this reality of human biases, AI-based systems will not necessarily enable humans to make unbiased decisions. AI systems and the data they use can include, reproduce, and reinforce human, societal, and political biases,[205] given that "bias is inherent in society and thus it is inherent in AI as well".[206] Algorithmic bias is a broad and well-documented phenomenon that spans across the entire lifecycle of an AI DSS—and one that is not easily solved or mitigated via technical means. Rather than presenting either humans or machines as more objective than the other, the debate should focus on the interactions between both sides and the types of interactions needed to ensure that appropriate decisions are made.[207] Different types of biases and assumptions related to both humans and AI DSS (whether data, design, development or use) deserve to be part of these considerations.[208]

Additionally, AI systems display a difficulty to adapt to new, changing conditions beyond those that they were trained on. The messy and constantly changing reality of warfare means that some uses of AI DSS would not be legally, ethically, or strategically appropriate.[209] Data-related and technical limitations such as brittleness involve security risks such because they potentially exacerbate the already existing uncertainties of warfare and military decision-making.

In the case of Project Maven, for example, military officials recognize that the system has a high error rate. As described in a *Bloomberg* report, human analysts at the US 18th Airborne Corps, which has been experimenting with Maven, could identify a tank 84% of the time, while Maven did it correctly 60% of the time, or 30% on a cloudy or snowy day.[210] When the conditions change from the ones the algorithms were trained on, the efficiency rate drops—perfectly illustrating the known 'brittleness' problem that AI algorithms typically exhibit. This unreliability constitutes a security risk that needs to be considered during development, testing, and evaluation of AI systems.[211] Focusing on developing safe and reliable systems without hasting to put them in the field is a key concern in relation to AI DSS.[212] This also helps strengthen systems against adversarial and hacking attacks from other actors.

Unreliability constitutes a security risk that needs to be considered during development, testing, and evaluation of AI DSS

205 Ingvild Bode, "Falling under the Radar: The Problem of Algorithmic Bias and Military Applications of AI," *ICRC Humanitarian Law & Policy Blog*, March 14, 2024, https://blogs.icrc.org/law-and-policy/2024/03/14/falling-under-the-radar-the-problem-of-algorithmic-bias-and-military-applications-of-ai/; Bode and Bhila, "The Problem of Algorithmic Bias in AI-Based Military Decision Support Systems."

206 Sinead O'Connor and Helen Liu, "Gender Bias Perpetuation and Mitigation in AI Technologies: Challenges and Opportunities," *AI & SOCIETY* 39 (2024): 2045–2057, https://doi.org/10.1007/s00146-023-01675-4.

207 See Georgia Hinds' remarks at the event "Artificial Intelligence in Military Decision Making: Legal and Humanitarian Implications" organized by the ICRC on 14 May 2024, https://www.icrc.org/en/event/event-artificial-intelligence-military-decision-making-legal-and-humanitarian-implications; see also Greipl, "Artificial Intelligence Systems and Humans in Military Decision-Making."

208 Holland Michel, *Decisions, Decisions, Decisions*.

209 Georgia Hinds, "Symposium on Military AI and the Law of Armed Conflict: A (Pre)Cautionary Note About Artificial Intelligence in Military Decision Making," *Opinio Juris*, April 4, 2024, https://opiniojuris.org/2024/04/04/symposium-on-military-ai-and-the-law-of-armed-conflict-a-precautionary-note-about-artificial-intelligence-in-military-decision-making/.

210 Manson, "AI Warfare Is Already Here."

211 For a broader discussion about security risks and AI in the military, see Ioana Puscas, *AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures* (Geneva: United Nations Institute for Disarmament Research, 2023); for a discussion on a risk-based approach to military AI systems, see Jack Shanahan, "Symposium on Military AI and the Law of Armed Conflict: A Risk Framework for AI-Enabled Military Systems," *Opinio Juris*, April 1, 2024, https://opiniojuris.org/2024/04/01/symposium-on-military-ai-and-the-law-of-armed-conflict-a-risk-framework-for-ai-enabled-military-systems/;

212 French and Lindsay, "Artificial Intelligence in Military Decision-Making," 63–65.

Due to such technical issues, some military personnel might not tend to extensively trust AI-based systems. As *Bloomberg* reported, a US targeting official said he would not *fully* trust the Maven system even if it "would be faster", because "that would introduce errors".[213] Some argue that a "trust gap", algorithmic aversion, or dismissal of information provided by AI DSS because of, for instance, the system outputs being different from humans' expectations, can be an issue in some contexts where AI DSS result in more precise and efficient outputs.[214] Whether automation bias will remain a constant phenomenon is also a matter of debate. For instance, some argue that more knowledge and awareness about the errors of algorithmic technologies might lead people to trust AI systems less.[215]

Legal challenges: compliance with IHL

The combination of technical challenges and issues of human-machine interaction explored in the sub-sections above raises a number of legal concerns,[216] especially (but not only) in relation to IHL.[217] One of the most important issues to examine is what humans' employment of AI DSS means for the former's ability to comply with international law. In armed conflict, and in targeting decisions, humans bear responsibilities such as distinguishing between combatants and civilians in a particular situation (distinction), assessing whether a decision would lead to 'excessive' loss of civilian life (proportionality), as well as taking the necessary precautions to minimize risk for civilians (precautions). Principles and rules underpinning IHL are fundamentally human-centric and require holding human agents, not AI systems, accountable for any violations. Humans remain legally accountable and responsible for the ways in which they make decisions, whether these processes involve AI DSS or not. Legal compliance therefore requires the possibility to attribute conduct to humans.

One of the most important issues to examine is what the employment of AI DSS means for humans' ability to comply with international (humanitarian) law

Officially, the use of AI DSS involves humans approving or rejecting target recommendations, which suggests a clear line of accountability if something goes wrong. However, as some suggest, the opaqueness and 'black box' aspects of AI algorithms challenge the operator's or the analyst's understanding of the system and its output, i.e., how the AI DSS arrived at a particular recommendation. Combined with the possible over-trust (automation bias), this raises questions about how to hold humans who do not have the requisite space to exercise agency legally (or morally) responsible and accountable.[218]

In a situation of increased speed and scale, there is a risk of accountability gaps, defined as "when a human decision-maker uses a decision-tool that presupposes values that have a significant influence on the outcome of the decision and that they haven't endorsed as their own values".[219] At the same time, whether a

213 Manson, "AI Warfare Is Already Here."

214 Konaev, Huang, and Chahal, *Trusted Partners*, 16; see also Paul Lushenko, "Trust but Verify: US Troops, Artificial Intelligence, and an Uneasy Partnership," *Modern War Institute at West Point*, January 16, 2024, https://mwi.westpoint.edu/trust-but-verify-us-troops-artificial-intelligence-and-an-uneasy-partnership/.

215 John Tramazzo, "Is AI Nominating Targets...Bad?" *Killer Robot Cocktail Party*, March 22, 2024, https://killerrobotcocktailparty.substack.com/p/guest-post-is-ai-nominating-targetsbad.

216 This sub-section raises a limited number of legal concerns. For more detailed discussions, see, for example, ICRC and Geneva Academy, *Expert Consultation Report on AI*; Taylor Kate Woodcock, "Human/Machine(-Learning) Interactions, Human Agency and the International Humanitarian Law Proportionality Standard," *Global Society* 38, no. 1 (2024): 100–121, https://doi.org/10.1080/13600826.2023.2267592.

217 Ruben Stewart and Georgia Hinds, "Algorithms of War: The Use of Artificial Intelligence in Decision Making in Armed Conflict," *ICRC Humanitarian Law & Policy Blog*, October 24, 2023, https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-intelligence-decision-making-armed-conflict/.

218 Atay Kozlovski, "When Algorithms Decide Who Is a Target: IDF's Use of AI in Gaza," *Tech Policy Press*, May 13, 2024, https://www.techpolicy.press/when-algorithms-decide-who-is-a-target-idfs-use-of-ai-in-gaza/.

219 Zeiser, "Owning Decisions," 7; see also Arthur Holland Michel, *The Accountability Surface of Militaries Using Automated Technologies* (Centre for International Governance Innovation, 2024).

commander is legally required to understand *all* the details of how AI DSS function, for instance in the nomination or recommendation of targets, is a topic of debate.[220]

AI DSS such as Gospel and Lavender are most often not considered inherently unlawful.[221] Legal concerns stem from not only either human behaviour or from technical characteristics of AI DSS, but also from how intelligence analysts and operators 'team' together with AI DSS. Reports on how these systems might have been used by the IDF, especially the speed and scale of Israel's operations in Gaza, have raised questions about "legal compliance, specifically related to the duty to take feasible precautions, crucial to ensure compliance with the rules of distinction and proportionality and ultimately aimed at minimising civilian harm".[222] To remain compliant with distinction and precautions rules, targeting processes require context-specific human judgements. However, these judgements are challenging to 'convert' into "technical indicators"[223] and therefore "unlikely to be satisfactorily defined" by AI-based systems that analyse data based on previous, historical patterns in datasets.[224] These limitations of AI DSS should be considered to ensure the exercise of human agency in use-of-force decision-making, especially when it involves a context of urban warfare with risks of harm to civilians and civilian objects.

As we highlight in section 3, it is difficult to pinpoint the exact use and application of AI DSS in specific use-of-force situations. This makes it even more important for institutions that are responsible for upholding (international) legal principles to possess the necessary capabilities to verify information on how AI DSS were used. Information is key to attribute responsibility.[225] Finally, it is important to add that AI DSS can be used not only in war zones but also as part of law enforcement, detention, and broader intelligence collection. Therefore, other bodies of law beyond IHL, notably international human rights law, are also relevant for the discussion.

Box 4 Legal reviews of AI DSS under Article 36

States parties to the Additional Protocol I to the 1949 Geneva Conventions are required, by Article 36 of this protocol, to conduct legal reviews of new weapons, means, or methods of warfare to determine whether their use would infringe upon international legal commitments, especially the duty to prevent disproportionate harm to civilians and civilian objects.[226] While AI DSS can be described as digital tools rather than weapons, they can be part of means through which warfare is conducted and therefore should also be subject to legal reviews.[227] Given that there is no universal way of conducting these reviews, they remain challenging to enforce.

220 Tramazzo, "Is AI Nominating Targets...Bad?"

221 Schmitt, "The Gospel, Lavender, and the Law of Armed Conflict."

222 Bo and Dorsey, "The 'Need' for Speed – The Cost of Unregulated AI Decision-Support Systems to Civilians"; Lauren Gould, Linde Arentze, and Marijn Hoijtink, "Gaza War: Artificial Intelligence Is Changing the Speed of Targeting and Scale of Civilian Harm in Unprecedented Ways," *The Conversation*, April 23, 2024, https://theconversation.com/gaza-war-artificial-intelligence-is-changing-the-speed-of-targeting-and-scale-of-civilian-harm-in-unprecedented-ways-228050; For the IDF response to legal concerns, see Israel Defense Forces, "The IDF's Use of Data Technologies in Intelligence Processing"; Mimran and Dahan, "Artificial Intelligence in the Battlefield."

223 Laura Bruun, Marta Bo, and Netta Goussac, *Compliance with International Humanitarian Law in the Development and Use of Autonomous Weapon Systems* (Stockholm: Stockholm International Peace Research Institute, 2023), 5.

224 Klonowska, "Article 36," 138; Woodcock, "Human/Machine(-Learning) Interactions."

225 This point is based on remarks delivered by Dustin Lewis at the breakout session "How to Ensure Responsible Use of AI in Military Decision-Making" at the Responsible AI in the Military Domain Summit in Seoul, 10 September 2024.

226 ICRC, "Article 36 – New Weapons," *International Humanitarian Law Databases*, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36, see also ICRC, *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach* (Geneva: ICRC, 2019); Vincent Boulanin and Maaike Verbruggen, *Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies* (Stockholm: Stockholm International Peace Research Institute, 2017).

227 Klonowska, "Article 36."

Ethical challenges: humanity in warfare and systematic killing

Related to but also distinct from legal challenges are concerns about the moral and ethical implications of using AI DSS in targeting. One major concern, voiced particularly in relation to Israel's military operations in Gaza and their exacerbation of an already existing humanitarian crisis, is the de-humanization of the targeting process. While *humans* are part of the decision-making process, the question is whether *humanity*, i.e., "a commitment to decency and restraint, and rejection of overly expansive categories of targetable enemies", is still present, especially if AI-based systems suggest, generate, or nominate targets.[228] There are risks that the use of AI DSS could reshape—or is arguably already reshaping—moral agency in warfare. This could be, as noted above, due to over-relying on the system's outputs or not having enough time to engage in the appropriate moral deliberations about the consequences of the decision.[229] If the use of AI DSS prioritizes speed and quantity of targets over the quality of decision-making, as some developments in the IDF's use of these technologies suggest,[230] the space for moral agency—reflecting on principles such as restraint and non-systematization of violence—shrinks considerably. This concern for the loss of moral agency is reinforced by reports surrounding Israel's employment of AI DSS. As one IDF whistleblower noted with reference to the Lavender system, "I had zero added-value as a human, apart from being a stamp of approval".[231]

There are risks that the use of AI DSS could reshape—or is arguably already reshaping—moral agency in warfare

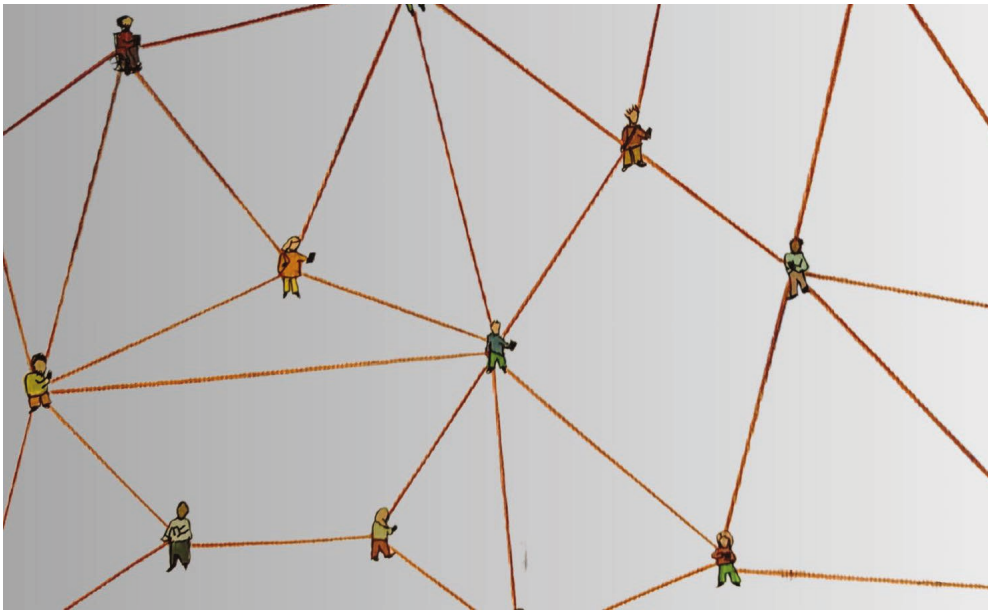


Image by Jamillah Knowles & Reset.Tech Australia / Better Images of AI / Detail from Connected People / CC-BY 4.0

228 Neil C. Renic and Elke Schwarz, "Inhuman-in-the-Loop: AI-Targeting and the Erosion of Moral Restraint," *Opinio Juris*, December 19, 2023, https://opiniojuris.org/2023/12/19/inhuman-in-the-loop-ai-targeting-and-the-erosion-of-moral-restraint/; see also Marijn Hoijtink and Robin Vanderborght, "Israel's Use of AI in Gaza War is Morally Unacceptable," *Intimacies of Remote Warfare*, December 12, 2023, https://intimacies-of-remote-warfare.nl/podcasts-documentaries/op-ed-israels-use-of-ai-in-gaza-war-is-morally-unacceptable/.

229 Elke Schwarz quoted in Samuel Sigal, "Some Say AI Will Make War More Humane. Israel's War in Gaza Shows the Opposite," *Vox*, May 8, 2024, https://www.vox.com/future-perfect/24151437/ai-israel-gaza-war-hamas-artificial-intelligence.

230 See Abraham quoted in France 24, "Understanding How Israel Uses 'Gospel' AI System."

231 Quoted in McKernan and Davies, "'The Machine Did It Coldly'"; see also Shehabi and Lubin, "Algorithms of War"; Kozlovski, "When Algorithms Decide Who Is a Target."

Another related concern is the risk of AI DSS being used for systematic killing, a process that precedes modern AI developments and is not limited to technologies, but that risks being accelerated due to "particular technical characteristics of AI" such as its classification of the world into data patterns.[232] The reliance on AI DSS could allow humans to feel less morally responsible for their decisions. The use of such systems therefore risks becoming part of a box-checking exercise for ethics review, which would be insufficient and inappropriate for decisions relating to targeting, especially in a context of urban warfare with affected civilians.[233] This also leads to questions about the violation of the human rights and dignity of those affected by the decisions, which has also been a key debate in relation to AWS, given that both AWS and AI DSS are criticized for enabling the treatment of humans as 'data points'.[234]

As this section demonstrated, challenges and risks surrounding AI DSS are encompassed by the overarching issue of human-machine interaction and distributed agency among humans and machines, which raises legal, ethical, and security concerns. At the same time, it is worth adding that the debate on the concerns of using AI DSS is often based on the type of system and the specific tasks it is used for within the targeting process (see section 2)—which are not often easily defined or categorizable, especially when information about the uses is limited.

For instance, some argue that humans using AI DSS to identify targets which they can then vet or correct in case of a mistake is not necessarily problematic, while employing an AI DSS to nominate targets would be unsafe, especially if there is insufficient time to correct errors.[235] Meanwhile, in the views of others, an AI DSS nominating targets is not inherently problematic, because ultimately, the decision to strike is taken by a human as "staffs and commanders will (and must) always vet and validate targets, regardless of the nomination source".[236] Such differences in views are just another reason for pursuing the debate on the role of AI in military decision-making further.

232 Neil C. Renic and Elke Schwarz, "Crimes of Dispassion: Autonomous Weapons and the Moral Challenge of Systematic Killing," *Ethics & International Affairs* 37, no. 3 (2023): 333–34, https://doi.org/10.1017/S0892679423000291.

233 Alexander Blanchard, "The Road Less Travelled: Ethics in the International Regulatory Debate on Autonomous Weapon Systems," *ICRC Humanitarian Law & Policy Blog*, April 25, 2024, https://blogs.icrc.org/law-and-policy/2024/04/25/the-road-less-travelled-ethics-in-the-international-regulatory-debate-on-autonomous-weapon-systems/; Matthias Klaus, "Transcending Weapon Systems: The Ethical Challenges of AI in Military Decision Support Systems," *ICRC Humanitarian Law & Policy Blog*, September 24, 2024, https://blogs.icrc.org/law-and-policy/2024/09/24/transcending-weapon-systems-the-ethical-challenges-of-ai-in-military-decision-support-systems/.

234 Adrián Agenjo, "Lavender Unveiled: The Oblivion of Human Dignity in Israel's War Policy on Gaza," *Opinio Juris*, April 12, 2024, https://opiniojuris.org/2024/04/12/lavender-unveiled-the-oblivion-of-human-dignity-in-israels-war-policy-on-gaza/; Amanda Sharkey, "Autonomous Weapons Systems, Killer Robots and Human Dignity," *Ethics and Information Technology* 21 (2019): 75–87, https://doi.org/10.1007/s10676-018-9494-0.

235 Brad Boyd, "There Are Some Things We Shouldn't Do…" *Killer Robot Cocktail Party*, February 19, 2024, https://killerrobotcocktailparty.substack.com/p/there-are-some-things-we-shouldnt.

236 Tramazzo, "Is AI Nominating Targets…Bad?"

5 Conclusions and Pathways for the Debate

Based on our overview of developments and discussions surrounding AI DSS, we conclude with outlining 1) a set of questions to push the debate further, and 2) recommendations to address some of the main challenges associated with AI DSS, particularly those stemming from human-machine interaction in the military domain.

5.1 Questions for stakeholders involved in the debate on AI in the military domain

To further reflect upon balancing the potential opportunities and challenges associated with AI DSS, it is imperative for involved stakeholders to continue discussing and eventually address the following broad guiding questions:

- How does the employment of AI DSS relate to targeting and rules of engagement practices across militaries, and what kind of challenges does it raise for reasonable and appropriate intelligence analysis that informs targeting? What do different actors understand by 'reasonable and appropriate'?
- To what extent do militaries using AI DSS entail a willingness to accept particular error rates associated with such systems, and what are the potential implications of such errors for human-machine interaction, and subsequently for military decisions that have real-life consequences for both combatants and civilians, infrastructure, and other objects?
- What forms of distributed agency between humans and machines produced by situations of human-machine interaction are acceptable in various military and security contexts?
- If considering the potential use of AI DSS, how can militaries retain a human-centric perspective to ensure that the exercise of human agency and effective human judgment is maintained in these decision-making processes? Which tasks in military decision-making should always be performed by humans and never delegated to AI systems?
- What measures—technical, legal, operational, strategic, or other—are being taken and should be taken to guarantee the exercise of human agency in use-of-force decisions in the context of using AI DSS?

5.2 Recommendations

Ensuring context-appropriate human involvement and retaining human agency

A first step towards mitigating the challenges discussed in section 4 involves **ensuring and strengthening sustained human oversight, involvement, and the exercise of agency throughout the entire lifecycle of AI DSS**, from pre-design, to design, testing, through to deployment, and post-use evaluation.[237] While cross-checking intelligence is part of military practice even without DSS, in the case of a network integrating various systems, human operators should have sufficient opportunity to consider AI-based outputs together with other data sources.[238] Especially in contexts of high speed and scale, human operators should follow protocols that allow for them to exercise **1) critical assessments of systems' outputs and 2) assessments of a decision's legal, strategic, and humanitarian impacts**.

The debate on the concerns of using AI DSS is often based on the type of system and the specific tasks it is used for within the targeting process

Considering current military trends, it would be challenging, or perhaps unrealistic, to impose general limitations on the speed or pace of targeting decisions. However, increasing the speed of decision-making is not always strategically beneficial and can involve severe legal and humanitarian risks. **Limitations on the speed and pace of use-of-force decision-making must in be in place in particular contexts of use**, especially in urban, populated areas. In any case, users should be provided with **clear and practical guidelines** on using AI DSS (whether one type of system, or a combination of systems) and consider situations where the 'right' algorithmic output could be interpreted in a way that leads to actions that are unsafe, not strategically beneficial, unethical, or unlawful.[239]

Developers and users of AI DSS should conduct **rigorous testing and regular audits** via robust communication channels to assess the quality of human involvement and agency in human-machine interaction. Testing should take into consideration that some technical uncertainties associated with AI- and machine learning-based DSS, including data bias or brittleness, may not be solvable. Such testing needs to be continuous, as AI DSS will likely require constant maintenance and updates.

Developers and users should also be aware of the limitations of technical solutions which might not take everything into consideration, depending on the context of use. Military personnel should be trained on typical limitations of both humans and machines and particular problems arising from human-machine interaction in various contexts.[240] Comprehensive training programmes and exercises should focus on **how the social, political, institutional, and technical aspects interact in different contexts of use**, and with what potential implications. Targeting doctrines may need to be adapted to reflect challenges associated with these patterns of interaction.

237 IEEE SA Research Group on Issues of AI and Autonomy in Defence Systems, *A Framework for Human Decision Making Through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications* (New York: IEEE SA, 2024).

238 Hinds, "A (Pre)Cautionary Note About Artificial Intelligence in Military Decision Making."

239 Holland Michel, *Decisions, Decisions, Decisions.*

240 John Christianson, Di Cooke, and Courtney Stiles Herdt, "Miscalibration of Trust in Human Machine Teaming," *War on the Rocks*, March 8, 2023, https://warontherocks.com/2023/03/miscalibration-of-trust-in-human-machine-teaming/.

Adopting a multistakeholder approach to sustain and strengthen the human role in decision-making on the use of force

The issue of AI DSS is currently not part of regulatory debates at the UN, which focus on the issue of autonomous weapon systems.[241] Opportunities and challenges associated with AI DSS should be part of the broader global conversation on military applications of AI, with a view on **establishing regulations on human–machine interaction in use-of-force decision-making and warfare**. These debates should focus on **setting standards for the human role in military decision-making**, especially concerning use-of-force decisions and in problematic, highly dynamic contexts such as populated, urban environments with high risks of affecting civilians.

Such discussions about human–machine interaction should also take place in a space that brings together diverse stakeholders beyond state representatives, including academics across social sciences and technical disciplines, as well as representatives from civil society and international organizations.[242] An inclusive approach, such as the one adopted by the Responsible AI in the Military Domain (REAIM) Summits, can help ensure a balance between national security and humanitarian concerns.[243] Moreover, any top-down processes towards governing AI technologies in the military domain should be accompanied by a **bottom-up, standard-setting process in the form of operational standards**. Such standards could advance the need to maintain the exercise of human agency in use-of-force decisions.[244]

241 Both the UN Convention on Certain Conventional Weapons and the General Assembly debates focus on AI and autonomous technologies in weapon systems.

242 Lisa Titus and Ariel Conn, "The CELL Approach: What We Can Learm from the Way a Working Group on Issues of AI and Autonomy in Defense Systems Works," *UN Office for Disarmament Affairs Responsible AI Blog*, https://disarmament.unoda.org/responsible-innovation-ai/blog/.

243 Bode and Nadibaidze, "Human-machine Interaction in the Military Domain."

244 The AutoNorms Project, "Global Governance of AI in the Military Domain," September 28, 2023, https://www.autonorms.eu/global-governance-of-ai-in-the-military-domain/.

About the authors

Dr Anna Nadibaidze is a researcher for the European Research Council funded AutoNorms and AutoPractices projects based at the Center for War Studies, University of Southern Denmark. She holds a PhD in Political Science from the University of Southern Denmark. Her research explores, among other issues, AI technologies in international relations and security, as well as governance and arms control of AI in the military domain. Her work has been published in journals such as *Contemporary Security Policy, Ethics and Information Technology*, and *Journal of International Relations and Development.*

Dr Ingvild Bode is Professor of International Relations at the University of Southern Denmark and Director of the Center for War Studies. Her research examines processes of normative change, especially with regard to the use of force and AI technologies in the military domain. Her work has been published in various international journals such as *European Journal of International Relations, Ethics and Information Technology, Review of International Studies*, and *Cooperation and Conflict*. She is the Principal Investigator of three externally funded research projects: (1) *AutoNorms: Weaponised Artificial Intelligence, Norms, and Order (08/2020-07/2026)* and (2) *AutoPractices: Practices to Sustain and Strengthen Human Agency in the Military Domain (06/2024-12/2025)* both funded by the European Research Council, as well as (3) *HuMach: Human-Machine Interaction in Military Applications of AI (08/2024-07/2028)* funded by the Independent Research Fund Denmark. Ingvild serves as the co-chair of the IEEE Research Group on AI and Autonomy for Defence Systems and as an expert member on the Global Commission on Responsible AI in the Military Domain.

Dr Qiaochu Zhang is a researcher for the European Research Council funded AutoNorms project based at the Center for War Studies, University of Southern Denmark. She holds a PhD in Politics from the University of Manchester. Her research examines China's approach to two areas of global governance: artificial intelligence and human protection, with a particular focus on China's influence on the potential transformations of international norms and orders. Her work has been published in *International Affairs*, among others.

CENTER FOR
WAR
STUDIES

SDU

AutoNorms