Lena Trabucco & Esben Salling Larsen

# ARTIFICIAL INTELLIGENCE IN COMMAND AND CONTROL

DJØF PUBLISHING
IN COOPERATION WITH THE
CENTRE FOR MILITARY STUDIES

# Artificial Intelligence in Command and Control

Lena Trabucco &
Esben Salling Larsen

# Artificial Intelligence in Command and Control

Djøf Publishing
In cooperation with the
Centre for Military Studies
2025

*Lena Trabucco &*
*Esben Salling Larsen*
Artificial Intelligence in
Command and Control

Acquisition and Procurement



*This publication is peer reviewed according to the standards set by the Danish Ministry of Higher Education and Science.*

Cover: Kelly Chigozie Kjelsø Arazu

Print: Ecograf, Brabrand

Printed in Denmark 2025

ISBN 978-87-574-6622-5

Djøf Publishing
Gothersgade 137
1123 København K

Telefon: 39 13 55 00
e-mail: forlag@djoefforlag.dk
www. djoefforlag.dk

# Editor's preface

The publications of this series present new research on defence and security policy of relevance to Danish and international decision-makers. This series is a continuation of the studies previously published as CMS Reports. It is a central dimension of the research-based services that the Centre for Military Studies provides for the Danish Ministry of Defence and the political parties behind the Danish defence agreement. The Centre for Military Studies and its partners are subject to the University of Copenhagen's guidelines for research-based services, including academic freedom and the arm's length principle. As they are the result of independent research, the studies do not express the views of the Danish Government, the Danish Armed Forces, or other authorities. Our studies aim to provide new knowledge that is both academically sound and practically actionable. All studies in the series have undergone external peer review. And all studies conclude with recommendations to Danish decision-makers. It is our hope that these publications will both inform and strengthen Danish and international policy formulation as well as the democratic debate on defence and security policy, in particular in Denmark.

The present publication is a result of the additional grant specifically aimed at research in the international legal challenges of the Danish Defence, which the parties to the Danish Defence Agreement have awarded to the Centre for Military Studies. The international legal research is conducted in collaboration with the Faculty of Law, University of Copenhagen, and the Royal Danish Defence College. Read more at: https://jura.ku.dk/icourts/research/intermil/

The Centre for Military Studies is a research centre at the Department of Political Science, University of Copenhagen. The centre conducts research into security and defence policy as well as military strategy. Read more about the centre, its activities, and other publications at: https://cms.polsci.ku.dk/english/

Copenhagen, August 2025
*Katja Lindskov Jacobsen*

# Table of Contents

# List of Figures

**Figures**

# List of Abbreviations

**ACT:** Allied Command Transformation
**AI:** Artificial Intelligence
**AI4DEF:** Artificial Intelligence for Defence
**AI-DSS:** Artificial Intelligence—Driven Decision-Support System
**AIP:** Artificial Intelligence Platform
**ALTAI:** Assessment List for Trustworthy Artificial Intelligence
**ANTICIPE:** Augmented Real-Time Instrument for Critical Information Processing and Evaluation
**AWS:** Autonomous Weapon Systems
**C2:** Command and Control
**CJADC2:** Combined Joint All Domain Command and Control
**DIANA:** Defense Innovation Accelerator for the North Atlantic
**DoD:** Department of Defense (USA)
**EDIDP:** European Defence Industrial Development Programme
**EU:** European Union
**FELIX:** Front End Learning Information Execution
**FRIA:** Fundamental Rights Impact Assessment
**ICRAC:** International Committee for Robot Arms Control
**ICTY:** International Criminal Tribunal for the Former Yugoslavia
**IDF:** Israeli Defense Forces
**IHL:** International humanitarian law
**ISR:** Intelligence, Surveillance, and Reconnaissance
**JADC2:** Joint All-Domain Command and Control
**JADO:** Joint All-Domain Operations
**LLM:** Large Language Models
**LSMO:** Large-Scale Mobilization Operations
**MHC:** Meaningful Human Control
**NATO:** North Atlantic Treaty Organization
**RAI:** Responsible AI
**UAS:** Uncrewed Aircraft System

**USAF:** US Air Force
**UK:** United Kingdom
**US/USA:** United States of America

# Abstract and Recommendations

This report critically examines the integration of Artificial Intelligence-driven decision-support systems (AI-DSS) within military command and control (C2) architectures, focusing on Denmark's defense apparatus. Employing a mixed-methods methodology—encompassing doctrinal analysis, seven semi-structured expert interviews with Danish and US military and industry stakeholders, and detailed case studies—this report offers a starting point for investigating both the operational opportunities and challenges of embedding AI within strategic and operational decision cycles in Denmark.

We use illustrative examples and case studies from ongoing military operations—specifically, Russia's invasion of Ukraine and the conflict in Gaza—to examine the integration of AI-DSS into modern decision-making processes. In Ukraine, AI-driven platforms analyze extensive sensor and signal data to produce real-time targeting suggestions and logistical predictions, whereas in Gaza, machine learning algorithms enhance dynamic targeting by combining multi-source imagery with open-source intelligence. These instances highlight a transition from standalone, weapon-focused AI applications to comprehensive systems that aid in planning, targeting, and operational force deployment at all command levels.

The report identifies key operational benefits and risks relevant to Danish defense policy officials. These include faster integration of diverse intelligence sources, ongoing improvement through software-defined platforms, and enhanced situational awareness through real-time data integration. On the other hand, dependence on proprietary "black box" models and commercial cloud systems presents serious concerns about model transparency, data management, resilience, and the risk of automation bias. These technical and cognitive risks are intensified by threats from adversarial data poisoning and the possibility of human oversight becoming overwhelmed by the sheer volume of data.

Additionally, this report explores pressing legal concerns regarding AI-DSS. This includes the applicability of Article 36 weapon reviews to AI-DSS, targeting paradigms under international humanitarian law (IHL), and the "reasonable commander" standard. This section also presents case studies of Israel's "Gospel" and "Lavender" systems to illustrate these findings through real-world examples and elucidate legal uncertainties.

From operational and legal perspectives, AI-DSS are already deeply integrated into C2 tools and are transforming operational decision-making. This report offers a useful starting point for Danish defense officials to scope and evaluate the future of AI-DSS in the Danish Armed Forces.

## Recommendations

1. Denmark will benefit from increased AI adoption in national C2 processes, streamlining information processing and improving the quality of command decision-making.
2. Denmark should recognize AI as more than just a technology and instead view it as a vital competence. This perspective could involve incorporating AI into command exercises, training, and offering educational opportunities for specialists and officers to develop AI competencies for future iterations and advancements in AI development.
3. When implementing new AI command systems, the Danish Armed Forces should evaluate AI according to the EU ALTAI standards, as applied in the AI4DEF projects.
4. Denmark should concentrate on utilizing open-source data, NATO systems (e.g., FELIX), and commercially available models tailored to specific military purposes, sometimes in collaboration with industry. Additionally, this collaboration should ensure that the systems managing daily operations possess the classification needed to utilize AI systems throughout the organization, including territorial aspects.
5. Denmark should initiate an inquiry into whether the current Defense law regulating the use of AI-DSS and the systems' access to civilian data requires amendments to include access to civilian data and services under the provisions of § 17 of the current Defense law.

6. Danish commanders should be provided with sufficient information about AI-DSS training and testing experience together with system risk to fulfil the responsible commander standard.
7. Given the specific and contextual nature of AI decision support, Denmark should seek greater cooperation with NATO allies within the regional area of operation to promote the use of AI-DSS in commands at the joint operational level and the higher tactical level, particularly within the Nordic Defence framework.

# Resumé og anbefalinger

Rapporten undersøger integrationen af kunstig intelligens i militære beslutningsstøttesystemer (AI-DSS), der anvendes i militær kommando- og kontrol (C2), med fokus på en mulig integration i det danske forsvar. Rapporten anvender en blanding af metoder; herunder doktrinær analyse, syv semistrukturerede ekspertinterviews med danske og amerikanske militære og industrielle aktører samt detaljerede casestudier. Rapporten undersøger både de operationelle muligheder og udfordringer ved at integrere AI i militære beslutningsprocesser på såvel det militærstrategiske som det operative niveau i Danmark.

Rapporten anvender illustrative eksempler og casestudier fra igangværende militære operationer — specifikt Ruslands invasion af Ukraine og konflikten i Gaza — til at analysere integrationen af AI-beslutningsstøttesystemer i moderne militære beslutningsprocesser. I Ukraine analyserer AI-drevne platforme omfattende sensor- og signaldata for at generere realtids-forslag til måludpegning og logistiske forudsigelser, mens maskinlæringsalgoritmer i Gaza forbedrer dynamisk måludpegning ved at kombinere billedmateriale fra flere kilder med open-source efterretninger. Disse eksempler fremhæver en overgang fra enkeltstående, våbenfokuserede AI-applikationer til omfattende systemer, der støtter planlægning, måludpegning og operationel styrkeudrulning på alle kommandoniveauer.

Rapporten identificerer centrale operative fordele og risici, som er relevante for danske forsvarspolitiske beslutningstagere. Fordelene omfatter hurtigere integration af forskellige efterretningskilder, løbende forbedringer via softwaredefinerede platforme og øget situationsforståelse gennem realtidsdata.

Omvendt medfører afhængighed af kommercielt udviklede "black-box"-modeller og kommercielle cloud-systemer alvorlige bekymringer vedrørende modellernes gennemsigtighed, datastyring, robusthed/resiliens og risikoen for automatiseringsbias. Disse tekniske og kog-

nitive risici forstærkes af trusler som f.eks. datamanipulation fra fjendtlige aktører og faren for, at menneskelig kontrol svækkes af mængden af data.

Derudover undersøger rapporten centrale juridiske spørgsmål relateret til kunstig intelligens i militær beslutningsstøtte. Dette omfatter anvendelsen af våbenanmeldelser efter artikel 36 i Genevekonventionernes tillægsprotokol I, måludpegning i henhold til den humanitære folkeret og standarden for den »fornuftige kommandør«. Afsnittet inkluderer også casestudier af Israels "Gospel" og "Lavender"-systemer for at illustrere disse forhold og belyse juridiske uklarheder.

Fra både et operationelt og juridisk perspektiv er kunstig intelligens allerede dybt integreret i nye kommando- og kontrolværktøjer. Det vil transformere beslutningstagning i militære operationer. Rapporten giver et udgangspunkt for at vurdere og forme fremtiden for brugen af kunstig intelligens i militære beslutningsstøttesystemer i Forsvaret.

## Anbefalinger

1. Danmark vil kunne drage fordel af øget anvendelse af kunstig intelligens i nationale kommando- og kontrolprocesser i form af en mere effektiv behandling af informationer og højere kvalitet i de beslutninger, der træffes i udøvelse af kommando.
2. Danmark bør betragte kunstig intelligens som mere end blot en teknologi og i stedet se det som en vital kompetence. Dette kunne indebære at indarbejde kunstig intelligens i udøvelsen af kommando, i uddannelse og løbende at tilbyde læringsmuligheder for specialister og officerer til at udvikle kompetencer indenfor kunstig intelligens i takt med den fremtidige udvikling.
3. Ved implementering af nye kommandosystemer med kunstig intelligens bør Forsvaret evaluere dette i henhold til EU's ALTAI-standarder, som anvendt i AI4DEF-projekterne.
4. Danmark bør fokusere på at anvende open-source-data, NATO-systemer (som FELIX) og kommercielt tilgængelige modeller tilpasset militære formål og gøre dette i samarbejde med industrien. Det bør sikres, at systemerne, der håndterer de løbende operationer, har den nødvendige klassifikation til at anvende systemerne på tværs af organisationen – også i en ren national sammenhæng.

5. Danmark bør igangsætte en undersøgelse af, om den nuværende forsvarslovgivning, der regulerer brugen af kunstig intelligens i beslutningsstøttesystemer, skal ændres; herunder særligt med hensyn til at sikre adgang til civile data og tjenester i krig og ekstraordinære situationer jf. §17 i den gældende forsvarslov.
6. Chefer og officerer i det danske forsvar bør gives tilstrækkelig viden om kunstig intelligens i beslutningsstøttesystemer, herunder trænings- og testforløb samt risikoprofil, for at kunne opfylde kravet om at agere som "fornuftig kommandør".
7. Givet at anvendelsen af kunstig intelligens i militær beslutningsstøttens vil have karakter af at være kontekstspecifik, bør Danmark fremme samarbejdet med NATO-allierede i det regionale nærområde for at styrke brugen af AI i militære beslutningsstøttesystemer på det fælles operative og de højere taktiske niveauer – især inden for rammerne af det nordiske forsvarskoncept.

## ACKNOWLEDGEMENTS

*The authors thank the Centre for Military Studies for their support, guidance, and feedback on multiple versions of this report. They also wish to thank all who participated in interviews or conversations about this fast-paced and important field.*

# 1

# Introduction

Artificial Intelligence (AI) is already integral to modern conflict. The ongoing Russia-Ukraine and Israel-Hamas conflicts both demonstrate how AI is already shaping military operations and decision-making in distinct ways. In Ukraine, AI-driven technologies have enhanced both defensive and offensive capabilities. Ukrainian forces have leveraged AI for surveillance, using drones with computer vision to monitor Russian troop movements, detect threats in real time, and apply machine learning to targeting.[1] Additionally, the Israeli Defense Forces (IDF) have integrated advanced AI systems (e.g., "Gospel", "Lavender") into their military operations, employing AI for data analysis and even target nomination. Gospel is an AI-powered system that synthesizes vast amounts of real-time data from sources such as drones, satellites and sensors to inform military commanders in making rapid targeting decisions. Lavender is another AI-driven system used by the IDF; it is designed to help identify combatants by analyzing patterns in enemy behaviour, identifying high-priority threats and suggesting courses of action based on data analysis. Each of these systems heavily informs the IDF's strategic and operational actions.

1. See, for example, the Ukraine-made Saker Scout drone. These drones use machine learning for object recognition to identify targets and visual navigation in the event of GPS jamming. Saker Scouts can be used in a fully autonomous mode, and reports have confirmed their use in fully autonomous mode during operations in Ukraine. See David Hambling, "Ukraine's AI Drones Seek and Attack Russian Forces without Human Oversight" *Forbes*, October 17, 2023, https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/

AI has informed—or directly guided—strategic and operational decision-making in these conflicts, signalling a qualitative shift in the tools and agents responsible for real-time decision-making. Recent global conflicts illustrate that AI has evolved from a tool within the kill chain of individual weapon systems to a capability embedded in the planning and command of broader military operations.

As Denmark and its partners continue to develop and integrate emerging technological capabilities, it is vital to explore the functions, operational benefits and legal risks of integrating AI into the broader Command and Control (C2) structures. Accordingly, this report investigates the following research question: *What are the opportunities and challenges for implementing AI decision-support systems in the Danish military?*

As a concept, C2 is both straightforward and elusive, encompassing a broad range of functions, activities and responsibilities. According to the North Atlantic Treaty Organization (NATO), C2 is "[t]he authority, responsibilities and activities of military commanders in the direction and coordination of military forces as well as the implementation of orders related to the execution of operations."[2] There is a growing trend to incorporate cutting-edge AI capabilities to assist, analyze and contribute to C2 architectures, providing commanders with a technical edge and strategic advantage in decision-making. However, there are also serious concerns and risks associated with this integration, which we address below.

At its core, C2 structures represent how national and multinational military commanders plan, make and implement decisions, and monitor the consequences, as C2 frameworks directly shape the operational environment. On the one hand, AI holds significant promise and opportunities for more effective and less labour-intensive C2 arrangements; on

2. In contrast, the United States defines C2 as follows: 'Command and control' is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission." William C. Barker, "Guideline for Identifying an Information System as a National Security System," National Institute of Standards and Technology, August 2003, 13, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf

the other hand, it raises the risk that legal perspectives may be neglected or misrepresented in complex systems in which it is often difficult to understand the logic and output of machine decision-making. This report explores the benefits and risks of integrating AI into C2 structures for decision support, and details pressing legal issues associated with this emerging capability in current and future conflicts.

Much of the military AI landscape overwhelmingly focuses on the implications of lethal autonomy through autonomous weapon systems (AWS). This is understandable, as delegating life-or-death decision-making to a machine represents the highest stakes for this emerging capability and has generated significant controversy.[3] Although AI is not an inherently lethal weapon, its application in operational environment analysis and military decision-making warrants scrutiny of its role in the broader context of C2 and military planning.[4] While application of AI in C2 and military planning has been an aspiration for decades,[5] we are now witnessing the development of civilian AI applications with the potential to operationalize these tools in military command and planning.[6]

As AI decision-support systems (AI-DSS) become integrated into military staff operations, the implications extend beyond the legal questions surrounding their use within individual weapon systems. For instance, as AI-DSS becomes integrated within the broader understanding and awareness of the operating environment, it naturally implicates critical legal concepts, such as military necessity. This raises distinct operational and legal considerations, separate from the application of AI in individual weapon systems, and imposes broader implications for Denmark.

This report demonstrates that AI offers significant potential as a decision-support tool that harbours substantial operational implications. It aims to shift the conversation beyond the tactical employment of AI—

3. Lena Trabucco and Kevin Heller, "Beyond the Ban: Comparing the Ability of 'Killer Robots' and Human Soldiers to Comply with IHL," *Fletcher Forum of World Affairs* no 46 (2022), 15.
4. James Johnson, "Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age," *Defence Studies* 1, no. 23 (2022), 43-67.
5. David. E Wilkins and Roberto V. Desimone, "Applying an AI Planner to Military Operations Planning," *SRI International*, Technical Note No. 534 (1993).
6. Johnson, "OODA Loop."

such as how it is used in individual systems and units—and instead explores the risks of AI in C2 at the operational level,[7] which directs the employment of AI systems in tactical action. From this perspective, the report also addresses the legal implications of embedding AI in operational C2 platforms. However, it is important to acknowledge that this report is intended only as a starting point. The implications of AI in C2 are far-reaching; covering them all is beyond the scope of this report. Rather, we present the foundational concepts of AI and C2 together with the most pressing operational and legal considerations necessary in the shifting global security landscape. Further research is necessary to investigate these issues in greater depth.

AI-DSS presents substantial opportunities. These systems are "computerised that use AI software to display, synthesise and/or analyse data and in some cases make recommendations – even predictions – in order to aid human decision-making in war."[8] The application of AI systems can complement the strengths of human cognition by enhancing situational awareness and accelerating decision-making.[9] Decision-support systems are found both at the tactical level—in the command facilities of formations and units employed in the engagements—and at the operational level, where major operations are planned and executed. AI-DSS can support military decision-making by helping translate strategic objectives into military plans and operations. Thus, AI potentially has profound implications not only for the execution of military force but also for how decision-makers interpret and engage with the operational environment.

However, AI-DSS also presents daunting risks and challenges for wartime decision-making, as discussed in greater detail below. This is especially true for smaller militaries such as the Danish Armed Forces.

7. NATOTERM definitions (NATOTERM is a NATO online database listing all authoritative NATO definitions): Operational level: The level at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theatres or areas of operations. Tactical level: The level at which activities, battles, and engagements are planned and executed to accomplish military objectives assigned to tactical formations and unit. https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en
8. Ruben Stewart and Georgia Hinds, "Algorithms of War: The Use of Artificial Intelligence in Decision Making in Armed Conflict," *Humanitarian Law & Policy*, October 24, 2023, https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-intelligence-decision-making-armed-conflict/
9. Stewart and Hinds, "Algorithms of War."

Denmark must assess AI in C2 not only on its technical merits but also within the context of being a smaller military, where decision-making frequently occurs within alliance-based structures.

Before proceeding, it is important to clarify key definitions to avoid common conflations. In particular, distinguishing between AI, machine learning, autonomous systems, and algorithms is a necessary first step towards understanding the functions and applications of military AI.

**Figure 1: AI Definitions[10]**

| | | |
|---|---|---|
| **Artificial Intelligence:** the ability for a system to learn and perform suitable techniques to solve problems and achieve context-appropriate goals. | **Autonomous System:** a system that can independently plan and decide sequences of steps to achieve a specific goal without human intervention. | **Algorithm:** lists the precise steps to take (e.g., a person writes in a computer code). AI systems contain algorithms. |
| **Machine Learning:** a subset of AI that explores how computer agents can improve their perception (or learn), knowledge, thinking or actions based on experience or data. | **Deep Learning**: the use of large multi-layer (artificial) neural networks that compute with continuous representations, much like the hierarchically organized neurons in human brains. | **Narrow AI:** intelligent systems for a narrow and defined task. **General AI:** seeks broadly intelligent, context-aware machines. |

The remainder of this report is organized as follows. First, we outline its methodology and approach. Second, we discuss how AI-DSS can provide operational benefits and strategic advantages in future warfighting capabilities, along with the associated risks of integrating AI into C2 structures. Third, we detail concrete steps taken at the national level in both Denmark and the United States to integrate AI into C2 structures, as well as parallel developments within NATO to illustrate the breadth and momentum of AI-DSS system adoption in multilateral defense settings. Fourth, we highlight significant defense-industry developments to showcase systems currently on the market that have the potential to transform command decision-making. Fifth, we explore the legal implications of integrating AI into C2, emphasizing areas where legal uncertainty still exists surrounding AI as a decision-support tool, with a particular focus on AI decision-support in targeting decision-making.

10. Human-Centered Artificial Intelligence, "Artificial Intelligence Definitions," HAI Stanford University, https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf

Finally, we offer conclusions and policy recommendations for Danish defense stakeholders on how to ensure the appropriate and effective integration of AI into national C2 frameworks.

## 1.1. Methodology

This report employs multiple methodological techniques to assess the integration of AI into C2 structures. First, we analyzed primary legal sources and military doctrine at both national and international levels to evaluate current technological initiatives and the legal and operational challenges to integration. We also reviewed a range of secondary sources addressing future-oriented issues, including academic analyses, blog-posts, human rights reporting, and media coverage.

Second, we conducted seven interviews with relevant stakeholders. These included four interviews with Danish military officials and industry representatives, and three with United States (US) Army legal advisors. These interviews provided firsthand accounts of current efforts to implement AI in Danish and US C2 systems—to the extent information could be shared—and identified key national priorities. The insights gained from these interviews informed our analysis of Denmark and the US as both bilateral partners and NATO allies.

Third, our legal analysis applied doctrinal legal methodology and relied on primary legal sources to assess current and emerging legal challenges related to AI integration in military decision-making.

# 2

# Operational Benefits

Incorporating AI into military command alters how we need to understand the range of its applications more broadly. Simple AI has long been utilized at the tactical level in weapon systems. For example, it has been used for pre-emption—alerting the system operator to more dangerous threats than they are currently engaging, or predicting and reacting to a threat faster than a human operator possibly can. An iconic example of this is the downing of a British Tornado fast jet in the Iraq War in 2003, when the US Patriot missile air defense system algorithms mistook the maneuvering of a British aircraft for a missile launch against the installations the missile system was tasked to protect.[11] However, AI innovation has rapidly developed in the commercial and civilian sectors, moving away from simple automation and toward more complex machine learning, which offers numerous operational benefits for military planners.

One operational benefit is making decisions faster and with greater situational awareness. The amount of data available for military operations has grown enormously. As such, we are on the brink of deploying AI far more advanced than previous simple military applications of AI and automation in tactical military weapon systems.[12] These dual developments offer a major advantage in utilizing decision-support systems capable of processing complex situations faster and better understanding

11. *The Guardian*, "'Glaring Failures' Caused US to Kill RAF Crew," UK News, October 31, 2006.
12. For more on AI in weapon systems, see Lena Trabucco, "*The Procurement of Autonomous Weapon Systems: Implications for International Humanitarian Law*," CMS Report (2023), https://cms.polsci.ku.dk/english/publications/international-humanitarian-law-and-lethal-autonomous-weapon-systems/

the operating environment in which the military is employed. Military decision support could also benefit from having more AI-qualified recommendations for the employment of tactical systems and units, as well as recommendations for the overall campaign plan and targeting.

A second operational benefit is AI's application at the strategic, operational and tactical levels to effectively translate strategic goals into tactical action. The United States, for example, has developed concepts such as Joint All-Domain Operations (JADO) and Multi-Domain Operations, which envision a far more integrated use of military assets across domains to enable the rapid and coordinated employment of effects against adversaries.[13] These military concepts include the idea of a Joint All-Domain Command and Control system—a more comprehensive integration of effects across domains and units. AI and integrated cloud environments are critical components of JADO, enabling effective communications and interoperable systems for joint operations.[14] The goal is for cutting-edge technologies to allow the US joint force to gain and sustain a decisive advantage across all domains, including cyberspace.[15]

Many operational benefits stem from these developments and the adoption of cutting-edge concepts. Military frameworks such as Net-Centric Warfare, introduced in the late 1990s and early 2000s,[16,17] included the notion of a "Combat Cloud,"[18] which was a shared military Internet of Things where units could continuously access and exchange information. This connectivity enabled more comprehensive, real-time situational awareness by integrating data from various unit sensors and situational pictures. Another operational benefit was enhanced target-

13. United States Department of Defense, *Summary of the Joint All-Domain Command and Control Strategy*, March 2022, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF
14. US DoD, *Summary*.
15. US DoD, *Summary*.
16. Clay Wilson, "Network Centric Operations: Background and Oversight Issues for Congress," *Congressional Research Service,* Report R32411 (March 2007), https://sgp.fas.org/crs/natsec/RL32411.pdf
17. David S. Alberts, Richard E. Hayes, and John Stenbit, *Power to the Edge: Command, Control in the Information Age* (Vol. 259) (CCRP publication series, 2003).
18. David Deptula, "Combat Cloud Is the New Face of Long-Range Strike," *Armed Forces Journal* September 18, 2013, http://armedforcesjournal.com/deptula-combat-cloud-is-new-face-of-long-range-strike/

ing: forces could leverage data collected by nearby allied units to refine and improve targeting decisions in dynamic environments.

Today, two developments are central to understanding Joint All-Domain Command and Control and the combat cloud, which offer clear operational benefits: software-defined defense and data-centric infrastructure.[19] Software-defined defense (or software-driven capability) means that software determines the function and performance of military systems. This evolution is reshaping and redefining military capacity, as software can be continuously updated and improved. Military hardware—the platforms—remains essential, but the software-hardware relationship is evolving in terms of both effectiveness and efficiency. Although hardware is critical for various reasons, including enabling software capabilities, it is often static and cannot match software in terms of learning, adaptability or precision. It thus plays a fundamentally different role.

From the outset, data-centric infrastructure is designed to store, manage and process data optimized for the many applications that accompany data-driven defense. This infrastructure provides computing and networking services to a range of applications and requires a mature multi-domain data management system. In military contexts, data-centric infrastructure supports the collection, analysis and dissemination of information critical to operations.[20] One clear benefit of this approach is that it "makes data the common element for systems to act on and consume, while also producing data that other systems can use such as uncrewed aircraft system (UAS) payloads generating ever-increasing amounts of intelligence, surveillance, and reconnaissance (ISR) data."[21] These systems are often modular, allowing components to be added, re-

19. Simona R. Soare, Pavneet Singh, and Meia Nouwens, *Software-Defined Defence: Algorithms at War* (The International Institute for Strategic Studies (IISS), February 2023); see also Nand Mulchandani and Jack Shanahan, *Software Defined Warfare: Architecting the DoD's Transition to the Digital Age*, Center for Strategic & International Studies (2022), https://www.csis.org/analysis/software-defined-warfare-architecting-dods-transition-digital-age
20. Department of Defense, *Data Strategy* (2020). DoD Data Strategy (defense.gov)
21. Andre Odermatt, *MOSA Systems: The Benefits of Deploying a Datacentric Architecture,* Military Embedded Systems, https://militaryembedded.com/unmanned/payloads/mosa-systems-the-benefits-of-deploying-a-datacentric-architecture

moved or replaced throughout their lifecycle, thereby fostering greater innovation and providing a strategic edge in competition.[22]

Military innovation often builds on civilian advances.[23] This relationship between the civilian and military sectors offers numerous benefits but also presents certain drawbacks.[24] Two issues raised by software-defined defense and data-centric networks deserve particular attention. The first is the reliance on civilian suppliers, especially within data-centric networks. Rather than acquiring a specific system, a data-centric network acquires a cloud ecosystem—or fabric—driven by civilian innovation, as illustrated by the US military's Joint Warfighting Cloud Capability contract, which includes multiple contractors (Microsoft, Amazon, Oracle, and Google).[25] This reliance can introduce significant transparency and data quality concerns. Transparency is challenged by the "black box" nature of AI decision-making, the complexity of system logic, and the opaque foundations upon which AI-DSS recommendations may be based. These factors can raise legal and ethical questions about employing systems developed by civilian technology firms. Data quality presents an additional challenge. Military applications of AI-DSS often rely on classified data to generate recommendations or outputs, leading to concerns about how models are trained and tested. It remains uncertain whether—and to what extent—civilian contractors can access and use classified data to train and test models to perform optimally in dynamic operational environments.[26]

Relatedly, the second issue concerns the potential use of civilian data in military operations, a trend that has grown substantially. For example,

22. Odermatt, *MOSA Systems*.
23. Soare et al., *Software-Defined Defence*.
24. Trabucco, "Autonomous Weapon Systems"; Risa Brooks, "Technology and Future War Will Test US Civil-Military Relations" *War on the Rocks* (2018) https://warontherocks.com/2018/11/technology-and-future-war-will-test-u-s-civil-military-relations/
25. Department of Defense, "Department of Defense Announces Joint Warfighting Cloud Capability Procurement." https://www.defense. gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/
26. Generally, models are trained on synthetic data that creates a simulated environment similar to that in which it would be expected to operate without compromising or making classified data vulnerable. However, there are natural concerns to this approach, including whether performance in the simulated environment and synthetic data is sufficient for verifying and validating expected performance in the actual operational environment with classified and real-world data.

open-source intelligence leverages advanced civilian datasets as parametric inputs to derive military patterns of life in the joint operational area. This capability presents significant challenges for military practitioners who seek to deploy it responsibly, but they also understand that using these systems responsibly involves numerous issues and vulnerabilities introduced by AI systems. Military applications of civilian data and AI technologies raise serious ethical and legal concerns, including algorithmic bias, data ownership, and accountability.[27] They also prompt questions about who bears responsibility for AI-generated recommendations—a topic explored in greater detail below.

This section has demonstrated how AI offers numerous operational benefits for military planners and practitioners. It increases the speed of decision-making, potentially providing an operational edge and strategic advantage. It also enables more comprehensive analysis and broader data integration, enhancing situational awareness and delivering a more accurate operational picture. Additionally, AI models significantly improve joint force interoperability and communications. However, these capabilities also introduce limitations and new vulnerabilities. For example, challenges persist in adopting and integrating systems from the commercial technology sector, along with ongoing concerns about data quality.

## 2.1. Current National, Allied and Industry Capabilities and Developments

There are notable differences in the readiness of states to adopt AI into existing military decision-making structures. Even within some of the most advanced nations in AI development—such as the United States and the United Kingdom (UK)—experts warn that outreach to civilian commercial partners for procurement risks producing technologies that lack "mission-oriented functions."[28] In other words, AI solutions are typically statistics-driven (e.g., precision) rather than what may trans-

27. For more on AI bias and accountability issues, see Trabucco, "Autonomous Weapon Systems."
28. Courtney Crosby, "Operationalizing Artificial Intelligence for Algorithmic Warfare," *Military Review*, July-August (2020), 43; Jesse Ellman, Lisa Samp, and Gabriel Coll, *Assessing*

late to a military objection.[29] The rest of this section presents ongoing initiatives to integrate AI into C2 structures within NATO, the European Union (EU), the US and Denmark. It also examines two critical developments in the defense industry with significant C2 implications, surveys a range of emerging AI systems that impact C2, and highlights a portfolio of concrete C2 applications.

### 2.1.1. NATO

NATO has taken significant steps toward AI integration, focusing on the creation of multilateral frameworks for "Responsible AI" (RAI) development and deployment, while also fostering civil-military relationships to support responsible development and the swift integration of AI into allied military capabilities. This section outlines some of the most notable developments across NATO as a whole, along with concrete initiatives for integrating AI into NATO command and control structures.

One of the most notable developments is the release of NATO's AI strategy in 2021,[30] which was among the first of its kind to outline a vision for the Alliance that acknowledges the significance of AI in future operations while also providing concrete steps for implementing AI principles in NATO's AI development and deployment. It is important to acknowledge, however, that NATO's influence in this area may be limited, as much of the AI development and decision-making authority resides with national governments. Nevertheless, recent years have demonstrated that NATO plays a role in shaping the governance of AI within the national security domain.[31]

---

*the Third Offset Strategy* (Washington, DC: Center for Strategic and International Studies, March 2017), 6–8.

29. Crosby, "Operationalizing Artificial Intelligence," 43; *Advancing the Science and Acceptance of Autonomy for Future Defense Systems: Hearing Before the Subcommittee on Emerging Threats and Capabilities of the Comm. on Armed Services,* 114th Cong. 1 (2015), https://www.hsdl.org/?view&did=793840; U.S. Army Capabilities Integration Center, *Robotic and Autonomous Systems Strategy* (March 2017), https://mronline.org/wp-content/uploads/2018/02/RAS_Strategy.pdf; Defense Science Board, *Report of the Defense Science Board Summer Study on Autonomy*; Executive Office of the President, Preparing for the Future of Artificial Intelligence October (2016), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf
30. See the NATO summary of the AI strategy for more information. https://www.nato.int/cps/en/natohq/official_texts_187617.htm
31. See Lena Trabucco and Zoe Stanley Lockman, "NATO's Role in Responsible AI Governance in Military Affairs," in *Oxford Handbook on AI Governance* (Oxford University Press,

There are two significant takeaways from the NATO AI strategy. The first is the development of the NATO Principles of Responsible Use of AI in Defense:

A. **Lawfulness:** AI applications will be developed and used in accordance with national and international law, including international humanitarian law and human rights law, as applicable.
B. **Responsibility and Accountability:** AI applications will be developed and used with appropriate levels of judgment and care; clear human responsibility must be maintained to ensure accountability.
C. **Explainability and Traceability:** AI applications will be designed to be understandable and transparent, including through the use of review methodologies, sources, and procedures. This includes verification, assessment and validation mechanisms at either the NATO and/or national level.
D. **Reliability:** AI applications will have explicit, well-defined use cases. The safety, security, and robustness of such capabilities will be subject to testing and assurance within those cases throughout their entire life cycle, including through established NATO and/or national certification procedures.
E. **Governability:** AI applications will be developed and used according to their intended functions and will enable appropriate human-machine interaction, the ability to detect and avoid unintended consequences, and the capacity to take corrective actions (e.g., disengagement or deactivation) when systems exhibit unintended behavior.
F. **Bias Mitigation:** Proactive steps will be taken to minimize unintended bias in both the development and use of AI applications as well as in the data sets used to train them.[32]

The AI strategy acknowledges that the individual allies and NATO have committed to ensuring that AI applications (including C2 capabilities)

2022), 1015-42.

32. Summary of the NATO Artificial Intelligence Strategy, NATO, October 2022, https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

that have been developed and deployed comply with the principles above at all stages of an AI system's lifecycle.

The second significant takeaway is the development of the Defense Innovation Accelerator for the North Atlantic (DIANA), which aims to establish closer links between NATO and industry innovation across a suite of emerging technologies, including AI. The AI accelerator labs are located in Germany, Norway, France, Portugal, Spain, Slovenia, Greece, Turkey, Bulgaria, Romania, Hungary, Slovakia, Poland, Lithuania, Latvia, Estonia and the United States. In fact, Denmark is one of two countries without an AI accelerator; this is because Denmark hosts the quantum technologies accelerator—another critical technology with defense applications.[33]

NATO has also taken steps to incorporate AI into future C2 structures and coalition decision-making. It is important to note that NATO's C2 structures differ in significant ways from those in the national contexts discussed in Denmark and the US. There is a strong emphasis on interoperability within NATO to ensure that multilateral partners can effectively and efficiently integrate systems and data-driven decision-making into NATO command structures. This section discusses two examples of NATO initiatives aimed at achieving this objective.

The first is a NATO project entitled "Human Considerations in Artificial Intelligence for Command and Control: Augmented Real-Time Instrument for Critical Information Processing and Evaluation" (ANTICIPE),[34] which focuses on utilizing AI-enabled technology to support the development, monitoring, and assessment of a commander's critical information requirements, facilitating much faster decision-making.[35] While much about this system has yet to be publicly released, General

33. See https://www.diana.nato.int/test-centres.html for more information.
34. NATO Allied Command Transformation, "Joint Force Development Experimentation & Wargaming Branch Fact Sheet – Human Considerations in Artificial Intelligence for Command and Control: Augmented Near Real-Time Instrument for Critical Information Processing and Evaluation (ANTICIPE)," https://www.act.nato.int/wp-content/uploads/2023/05/2023_Fact_Sheet_EiE_STJU23_ANTICIPE.pdf
35. Critical information requirements refer to a process in joint military operations that helps commanders identify and prioritize essential information for operational decision-making. For more on these requirements, see Christopher R. Bolton and Matthew R. Prescott, "Commander's Critical Information Requirements: Crucial for Decisionmaking and Joint Synchronization," *Joint Force Quarterly* 113 (2024), https://digitalcommons.ndu.edu/joint-force-quarterly/vol113/iss1/15

Philippe Lavigne, Supreme Allied Commander Transformation, stated, "It is not the machine, it's the human in the loop who will decide...[b]ut he will have the opportunity to go faster, to get proposals faster than ever."[36] The ANTICIPE system is currently under the NATO Science & Technology Organization and was developed by Thales, a French defense company, to employ machine learning and war-gaming tools to determine how best to assist NATO commanders in complex operational decision-making. The system is currently undergoing experimentation.

A second and very different project that NATO is exploring relates to how AI can assist military staff procedures in less safety-critical contexts while holding significant implications for the C2 environment. This initiative, called AI Front End Learning Information Execution (AI FELIX), employs machine learning tools to automate previously manual or resource-intensive processes. AI FELIX automates the extraction of metadata and the distribution of tracking information across NATO. Accordingly, AI FELIX,

> *demonstrated the feasibility of applying Artificial Intelligence in the NATO SECRET Wide Area Network. By developing an operational Graphical User Interface, users are able to link AI FELIX with NATO's information and knowledge management tools, such as the Enterprise Document Management System, Tasker Tracker Plus, and the NATO Information Portal. The Graphical User Interface enables dynamic learning, a process that allows the Artificial Intelligence to improve its predictions by using feedback and responses from users. By creating Web Apps, AI FELIX can be distributed to the rest of the Alliance.*[37]

AI FELIX has already revolutionized numerous areas and streamlined NATO deliverables. In one example,

> *AI FELIX reads incoming correspondence, including hundreds of incoming correspondence that arrive at the headquarters every day. It then recommends how that correspondence should be distributed internally,*

36. NATO STO release on ANTICIPE: https://www.youtube.com/watch?v=A2ZAHrT3UwM
37. See background information from NATO Allied Command Transformation, https://www.act.nato.int/our-work/innovation/

*uploads the document to the appropriate Enterprise Document Management System folders, and predicts if there is a task to be completed by the Command as a result of the correspondence.*

NATO Allied Command Transformation (ACT) notes that AI FELIX "has consistently delivered highly accurate results with an average processing time of 27 seconds per document compared to the 5-10 minutes required by a person."[38] This tool can reduce the time necessary for command staff to analyze information and help distribute it to appropriate stakeholders, thereby streamlining C2 decision-making and assisting traditional staff procedures. However, it is not in itself an AI application that produces analytical work for the staff.

In addition to the systems mentioned above, the NATO Allied Command Operations introduced an interim AI-DSS. On March 25, 2025, NATO's Communications and Information Agency (NCIA) and Palantir finalized the acquisition of the Maven Smart System NATO (MSS NATO) for Allied Command Operations (ACO).[39] The acquisition of MSS NATO is intended to advance the adoption of AI, modelling, and simulation tools across the Alliance and provide an immediate capability to NATO operations.

These are just three examples of what are almost certainly many initiatives across the Alliance to streamline and assist decision-making, both in the C2 context and other domains. From both a practical application standpoint and through its governance initiatives, NATO's efforts can set the stage for national governments to better incorporate AI into military decision-making practices, particularly for less technically capable governments.

### 2.1.2. European Union

The EU is actively integrating AI into its strategies with the aim of enhancing European operational capabilities while ensuring ethical standards. It has launched several initiatives to bolster AI applications

38. NATO Allied Command Transformation, "Artificial Intelligence Front End Learning Information Execution (AI FELIX)," https://www.act.nato.int/wp-content/uploads/2023/05/2019_ai-felix.pdf
39. NATO Allied Command Operation, "NATO acquires AI-enabled Warfighting System", April 14 2025, https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system-.

in defense. A notable example is the Artificial Intelligence for Defence (AI4DEF) project, which aims to use AI technologies to improve military situational awareness, decision-making and planning. This project is funded under the European Defence Industrial Development Programme (EDIDP) and involves a consortium of 21 partners from 10 European countries, including industry and institutions.

The TERMA Group from Denmark leads the AI4DEF consortium, focusing on integrating AI to enhance defense systems, with Aalborg University contributing a structured approach to identifying and selecting suitable AI models. The project demonstrated the utility of AI in improving situational awareness and decision support in military operations—examples include object identification in video streams, adaptive mission rerouting, and summarization of military intelligence reports—while also addressing well-known challenges such as data scarcity and the handling of sensitive, classified information.[40]

The AI4DEF was aimed at demonstrating the potential in particular military fields, but the process in itself—where industry and militaries were cooperating across normal commercial and national boundaries—could also point to how the European application of AI in the military may be improved in future. The ability to access know-how across European companies and partners was an asset unto itself.[41] Even though the AI4DEF program was aimed at demonstrating the feasibility of integrating AI into military systems, the cross military/commercial cooperation and pooling of the competencies of European companies might point to a future model for leveraging AI in military applications in the European setting. The rapid development of AI models also needs to address military decision-support systems' ability to operate in a hybrid operational environment. This may require a more constant interaction between the military and the commercial sector in what can be described as various forms of inter-organizational interactions—in the same way that the military has a cooperative approach to the commercial sector in areas such as logistics.[42]

40. Interview with TERMA expert.
41. Ibid.
42. Joakim Berndtsson, Anne Roelsgaard Obling, and Åse Gilje Østensen, "Business-Military Relations and Collaborative Total Defence in Scandinavia," in *Total Defence Forces in the Twenty-First Century* (McGill-Queen's University Press, 2023), 397-420.

The AI4DEF consortiums were obliged to use the ALTAI tool, which was developed to ensure that AI systems align with the EU's ethical guidelines. It recommends that users conduct a Fundamental Rights Impact Assessment (FRIA) before deploying AI systems, ensuring adherence to the EU's Charter of Fundamental Rights. It is thereby an approach that helps identify and mitigate potential risks associated with AI applications.[43] The operationalization of ALTAI in the AI4DEF gave the involved partners an opportunity to gain competencies in the practical applications of ethical standards within the field of AI.[44] There is thus an established practice that can be drawn upon in future projects and the development and update of future AI-supported decision systems.

The EU AI Act prohibits AI practices that pose unacceptable risks to fundamental rights. These include subliminal manipulation and exploitation of vulnerabilities, social scoring by public authorities and predictive policing based on profiling, unauthorized facial recognition and emotion recognition in workplaces and schools, and biometric categorization to infer sensitive traits (e.g., race, political views).[45] These guidelines ensure that AI aligns with European values and ethical standards.[46] The AI Act primarily applies to civilian AI applications, and military and defense-related AI systems are generally excluded from its restrictions. However, if AI technologies developed for civilian use are repurposed for military applications, they may still be subject to regulations. This raises issues as the military works to leverage the advances in civilian AI technologies. Furthermore, hybrid threats and a rivalry/competition between Russia and European states that transcends a peacetime/wartime dichotomy challenge the idea in the EU AI Act that the military use of AI can be seen as something distinct from civilian use.

43. TERMA, "AI4DEF continues work on ethics: AI for Defence" June 3, 2024, https://ai4def.com/ai4def-continues-work-on-ethics/
44. Interview with TERMA expert.
45. European Union, Policy and Legislation, "Commission publishes the Guidelines on prohibited Artificial Intelligence (AI) practices, as defined by the AI Act." *Shaping Europe's digital future*, 4 February 2025, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act
46. European Union, "Guidelines on prohibited AI."

### 2.1.3. United States

The US has been an active player on the global stage, advocating for technological supremacy and greater AI integration into military activities. In several ways, it is ahead of its peers in taking concrete steps to integrate AI-enabled systems into the Department of Defense (DoD). For example, the US is the only country to go beyond simply creating a defense AI strategy, having also implemented a DoD Directive for the responsible development, integration and deployment of autonomous weapon systems.[47] Similarly, the DoD has made significant strides to integrate AI models and systems into decision-making processes and C2 architectures.

The Americans argue that embedding AI across C2 infrastructures will enable commanders to make decisions at machine speed using real-time data sources, enhancing their C2 posture and creating strategic advantages against adversaries.[48] Numerous concrete steps have already been taken to realize this initiative across the DoD and at the individual service levels. In early 2021, for instance, the Pentagon established the AI and Data Acceleration initiative, where the DoD's operational data and AI teams of technical experts would travel to the military's 11 combatant commands to help them better understand their data and create AI tools to streamline decision-making. Deputy Secretary of Defense Kathleen Hicks acknowledged that

> *All of this and more is helping realize Combined Joint All Domain Command and Control [CJADC2]. These systems are separate from other efforts focused on amassing hardware for weapons development or other warfighting capabilities. To be clear, CJADC2 isn't a platform or single system we're buying. It's a whole set of concepts, technologies, policies, and talent that are advancing a core US warfighting function—the ability to command and control forces.*[49]

47. US Department of Defense, "Directive 3000.09: Autonomy in Weapon Systems", January 2023, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.
48. Wes Haga and Courtney Crosby, "AI's Power to Transform Command and Control," *National Defense*, November 13, 2020, https://www.nationaldefensemagazine.org/articles/2020/11/13/ais-power-to-transform-command-and-control
49. Jaspreet Gill, "DoD Releases New AI Adoption Strategy Building on Industry Advancements," *Breaking Defense*, November 2, 2023, https://breakingdefense.com/2023/11/dod-releases-new-ai-adoption-strategy-building-on-industry-advancements/

There are also significant initiatives at the service level. The US Air Force (USAF), US Navy, and US Army are all at various stages of incorporating AI into their respective C2 processes. For example, the USAF announced a strategic overhaul to incorporate AI into three key areas of Air Force C2: mission-tailored AI for C2 optimization, federated composable autonomy, and AI toolbox development.[50] The USAF stated, "AI holds great potential in transforming DAF capabilities across strategic, operational, and tactical levels by enabling decision makers to effectively assess the battlespace, rapidly explore, create, and select the best plan, and direct and monitor forces at pace and scale in a distributed setting."[51] A particular priority—and ongoing challenge—for the USAF is incorporating generative AI—specifically, Large Language Models (LLMs)—into military applications. The operational and legal challenges posed by LLMs will be addressed below, but it is worth noting the direct engagement of the US DoD with the commercial industry developing LLMs to leverage the benefits from generative AI.[52]

Additionally, the US Army announced an initiative to incorporate AI into large-scale mobilization operations (LSMO) as early as 2024.[53] The Army outlined efforts to run simulations exploring millions of scenarios as part of everyday operations to support faster and more informed decision-making.[54]

50. Department of Air Force Press Release, *Artificial Intelligence and Next Generation Distributed Command and Control*, February 29, 2024, https://sam.gov/opp/d8eb1d7f980d4c02b080d87747297ee6/view
51. Ibid.
52. It is also worth noting the evolution from industry in the US on supplying LLMs to the US DoD. For example, when OpenAI launched ChatGPT, there was an explicit prohibition on supplying such capabilities for military purposes. Of course, the military could use the publicly available version of ChatGPT, but the output was too unreliable for military purposes. Over the next year, OpenAI removed the military prohibition and opened their services to the DoD to signal that LLMs will have a place in strategic, operational and tactical decision-making. Additionally, see the discussion regarding Palantir's development of a military LLM and the supplementary information in the appendix for examples of how to incorporate LLMs into military planning and decision-making.
53. The announcement came from US First Army in December 2023. First Army, "First Army Taps Artificial Intelligence to Enhance Command and Control," https://www.first.army.mil/News/ArticleView/Article/3613646/first-army-taps-artificial-intelligence-to-enhance-command-and-control/
54. Ibid.

> *With AI, we have the ability to pre-calculate solutions. We estimate what is going to happen if you make this decision, and we can go ahead and run it and calculate all those different decisions and have the best three or four recommended to the commander. The commander still makes the decisions, but we can get there a lot faster if we have it pre-calculated and ready to run when something happens.*[55]

As a critical ally and national security partner for Denmark, it is worth noting how the US has embraced AI as an essential tool for future C2 operations at both the DoD- and service-level planning. Understanding developments in the United States can help ensure greater C2 interoperability, strengthen robust and effective communications, and offer Denmark a source of relevant "lessons learned," where appropriate.

### 2.1.4. Denmark

NATO and Denmark view themselves as being in ongoing competition with Russia in the Baltic Sea region, where conventional threats require deterrence and defense, and where hybrid threats are also significant.[56] This implies that the command and control of armed forces must be understood in relation to conventional warfighting tasks and must also include countering hybrid threats—particularly in light of Denmark's role as a staging area for allied forces entering the Baltic Sea region.[57] These dynamics have implications for what AI can offer Danish C2 and how AI is incorporated into these structures.

The incorporation of AI into Danish C2 must therefore be capable of supporting both the current state of competition and any future crisis scenarios. In such situations, Denmark should be able to detect and counter hybrid threats using military means while also operating effectively in a state of armed conflict. Within the NATO collective defense framework, Denmark must maintain the necessary command and control to enable the forward movement of allied forces and to support operations from Danish air stations against both hybrid and conventional

55. Ibid.
56. Esben S. Larsen and Rasmus Dahlberg, *Hjemmefronten: Nationale opgaver frem mod 2035*, (DJØF Publishing, 2024).
57. Alexander H. Tetzlaff, "Værtsnationsstøtte" in Esben S. Larsen and Rasmus Dahlberg (eds), *Hjemmefronten: Nationale opgaver frem mod 2035*, (DJØF Publishing, 2024).

military threats. Additionally, Denmark must function as a battlespace owner in one or more military domains, ensuring that its C2 systems operate in full integration with NATO.[58] This requirement regarding integration with the NATO command structure also applies to the North Atlantic and the Arctic, where the Arctic Command may, to a lesser extent, serve as a battle space owner due to the expansive operational area. Nevertheless, it must still be capable of managing hybrid threats and potentially the convergence of hybrid and conventional military threats during periods of heightened tension.

The incorporation of AI into Danish command and control is largely about the ability to establish a baseline pattern-of-life picture in the operational area during peacetime; particularly concerning critical infrastructure, which the Danish Defence Agreement identifies as significant to Denmark's role as a staging area for allied forces.[59] A contemporary pattern-of-life image refers to an understanding of the daily activities occurring within the operational environment—both civilian and military—so that the military can detect significant changes that might indicate an increased threat level (whether conventional or hybrid). This capability is essential for protecting civilian activities in times of war.

AI will also have significant potential to coordinate and allocate units in response to hybrid threats. This requires data-sharing with civil authorities, including those in other parts of the Kingdom of Denmark (i.e., Greenland and the Faroe Islands). It also implies that AI may need to be employed differently across various aspects of Danish command and control. Introduced in the previous defense agreement,[60] domain commands were established within the Danish military services, and these will potentially need to function as battlespace owners within the NATO framework. This means that Danish command and control will simultaneously include elements that operate in an alliance-like context, and others that function as a pure national command authority.

The Danish use of AI decision-support systems remains in its nascent stages. The Danish Defence has signed a long-term contract for C2

58. Interview with Danish officer in the Air Command.
59. A.M. With, "Hybride maritime trusler", in Esben S. Larsen and Rasmus Dahlberg (eds) *Hjemmefronten: Nationale opgaver frem mod 2035*, (DJØF Publishing, 2024).
60. Forsvarsministeriet, "Aftale på forsvarsområdet 2018-2023", January 2018, https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-forsvarsforlig-2018-2023-2018.pdf

systems with Systematic, a Danish company, whose SitaWare software is already in widespread use across the Danish armed forces.[61] An AI capability is currently being developed for Sitaware by the company.[62] The Danish Army has been working on an AI decision-support capability, initially exploring Palantir technology but now collaborating with Systematic. The Danish Armed Forces are also closely monitoring developments in partner and allied militaries, where Palantir has supported US forces and Ukraine with AI-driven intelligence in combat missions.[63] The Danish Army project focuses primarily on enabling faster decision-making at the brigade and battalion levels, particularly in issuing orders and instructions to subordinate units.[64] In that sense, the Danish approach focuses more on the staffing process than on intelligence consolidation. Private companies have been granted access to plans and orders from Danish military exercises to help develop decision-support systems that can generate this material rapidly.[65] Systematic is currently involved in developing a new decision-support system aimed at implementing existing army doctrine—but at a much faster pace. Danish defense authorities are not only concentrating on systems development but are also seeking to build AI competencies through education.[66] When military officers use AI-DSS to gain a comprehensive understanding of the operational environment, they must be aware of both the opportunities and potential pitfalls of such systems. Given the rapid pace of AI model development, the education and training of officers should receive attention alongside the development of new systems and the AI applications within them.

As noted previously, military-commercial interaction is likely to occur in a hybrid operating environment and where an employment of the

61. Forsvarsministeriets Materiel- og Indkøbsstyrelse, "Ny 20-årig rammeaftale med Systematic om operative it-systemer til hele forsvaret", February 2023, https://www.fmi.dk/da/nyheder/2023/ny-20-arig-rammeaftale-med-systematic-om-operative-it-systemer-til-hele-forsvaret/
62. Huw Williams, "*SitaWare Gains AI-Powered Intelligence, Decision Support Tools*," January 11, 2022, https://www.janes.com/osint-insights/defence-news/defence/sitaware-gains-ai-powered-intelligence-decision-support-tools
63. Anthony King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," *Journal of Global Security Studies* 9, no. 2 (2024).
64. Interview with Danish Army Officer.
65. Ibid.
66. Ibid.

Danish Military is not confined solely to war but extends into deterrence and competition. Danish law does not currently provide for governance over AI in military-commercial relations or secure the necessary AI resources within a total defense framework. Section 17 of the Danish Defense Act[67] provides the framework for military-commercial relations in other areas, but it is outdated regarding access to resources and oversight in the field of AI.

It should be noted that the development of AI in Danish military decision-making has a parallel in the Danish police, where Palantir technology has been employed in systems used by law enforcement.[68] There is thus a precedent and relevant experience that can be utilized in the governance of Danish military AI decision-support systems.

### 2.1.5. Industry Developments

The capabilities referred to as "AI systems" and "decision-support tools" are designed and developed by commercial partners in the civilian defense industry or by emerging technology firms and start-ups at the forefront of AI innovation. Tech innovation is a global industry, with most products tailored for civilian purposes and applications. The nature of AI as a dual-use technology means that many of these systems and tools are not necessarily designed with military functions as their primary purpose, unlike traditional pathways for military technology development. Nevertheless, the military is a "fast follower" of the tech industry, seeking to harness cutting-edge capabilities and functions to gain a strategic and tactical edge in complex decision-making and warfighting.

It would be impossible to comprehensively assess all industry developments of tools that can aid commanders in C2 decision-making—the pace of innovation is too rapid to capture fully for our purposes. However, we will discuss two systems in particular that demonstrate the direct utility and application of AI-DSS and how AI can aid or even transform decision-making in complex operational environments.

67. Forsvarsministeriet, "Bekendtgørelse af lov om forsvarets formål, opgaver og organisation m.v.", 2017.
68. The introduction of Palantir was enabled by legislation addressing the issues raised by the surveillance system. See, Folketinget, "Forslag til lov om ændring af lov om politiets virksomhed", 2017. Available at https://www.ft.dk/samling/20161/lovforslag/l171/index.htm

Systematic, a long-time provider of military C2 solutions, now offers AI decision support in conjunction with their Sitaware C2 command software.[69] Initially, its focus was on automated functions in presenting the operational picture to the operator (e.g., automatically assigning designations to targets and units). It is now evolving to include AI-assisted detection of anomalies in the surveillance picture. This AI is being developed into a decision-support tool, both aiding the decision-making process and facilitating a comprehensive understanding of the operating environment.

Another notable development is Palantir's recent launch of its Artificial Intelligence Platform (AIP) for Defense. This initiative reflects the broader trend in the technology sector toward generative AI—models capable of producing images, videos and text based on their training data. Generative AI, particularly the watershed release of OpenAI's release of ChatGPT, is widely seen as a turning point in AI research and a major advancement in the practical utility of AI across various applications. In the defense domain, generative AI offers significant promise—but also serious concerns. While this report does not explore those concerns in depth, we will examine one defense-specific generative AI system in particular.

Palantir's system, called "AIP for Defense," is notable for its application of AI at the tactical edge and LLMs tailored specifically for military operations. AIP for Defense functions as an AI-DSS with a range of capabilities, including support for targeting operations. The system was launched in the summer of 2023; however, many details regarding its architecture and performance remain unavailable. Nevertheless, Figure 2 in the appendix presents a fictional scenario that illustrates the system's capabilities and demonstrates how an AI-DSS might function across different levels of the chain of command.

AIP has several notable features. First, it provides a platform for real-time communication between commanders, subordinates and the system itself, similar to other LLMs, such as OpenAI's ChatGPT. Second, the system can instantaneously generate operational plans and multiple courses of action for operators to review, with these options sent directly to the commander for approval. Third, as discussed below, the system

69. Artificial Intelligence (systematic.com). Interview with Danish Army Officer.

can generate targeting options for the operator and commander to authorize. No information is publicly available regarding the data sources, legal frameworks or other operational considerations that inform the system's decision-making protocols for this feature. Nevertheless, it represents a significant breakthrough for AI-DSS in military operations.

While this brief overview of notable industry developments is far from exhaustive, it is useful to highlight how these capabilities can be employed in real-world scenarios to provide concrete examples of AI in C2 decision-making. The next chapter examines key considerations when incorporating AI into C2 systems together with the operational benefits that militaries may gain from this emerging capability.

# 3

# AI in Command and Control—Legal Implications

This chapter examines the most relevant legal implications of AI-DSS. The first part reviews legal evaluations of military AI, focusing on decision-making frameworks to assess the applicability of Article 36 weapons reviews to AI-DSS. It also explores other regulatory avenues of regulation, particularly in acquisition and procurement, which may serve as mechanisms for AI assurance. The second part addresses the legal implications of using AI-DSS in targeting processes. This discussion is distinct from the broader and ongoing debate on autonomous weapons and instead focuses on the relationship between commanders and AI-DSS; an interaction that may play a critical role in target identification and selection.

## 3.1. AI Decision-Support Systems and Article 36 Reviews

Article 36 of Additional Protocol I of the Geneva Conventions (commonly referred to as "Article 36 reviews") requires state parties, including Denmark, to assess new means and methods of warfare to ensure their compliance with international legal obligations.

Article 36 requires,

> *In the study, development, acquisition, or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all*

> *circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.*[70]

Article 36 reviews have garnered considerable scholarly attention in the context of AWS, where they are viewed as a critical component of responsible development and deployment.[71] However, it remains unclear whether AI-DSS are required—or ought—to undergo an Article 36 review.

Some scholars advocate for including AI-DSS in the Article 36 review process.[72] As Klaudia Klonowska argues, "[e]ven if AI systems are not embedded into a weapon and do not autonomously 'pull the trigger,' there is considerable concern that the algorithmic recommendations in a chain of machine-machine and machine-human interactions lead to the engagement of targets."[73] Klonowska proposes four criteria to determine whether AI-DSS should be subject to Article 36 reviews. First, she evaluates whether AI-DSS can challenge a state's compliance with obligations under IHL. She identifies three characteristics of the current state of AI that could undermine a state's ability to comply with IHL: legal interpretation, battlefield complexity, and technical limitations.[74] Based on these three factors, she concludes that AI-DSS could feasibly challenge a state's capacity to meet its IHL obligations.

The second criterion considers whether the AI-DSS is integral to military decision-making. Klonowska warns of how AI-DSS risks leading to over-reliance on system outputs—a phenomenon known as automation bias. There is some empirical evidence supporting this concern. For ex-

70. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 36 (adopted 8 June 1977, entered into force 7 December 1978). [Hereinafter Additional Protocol I].
71. See Damian Copeland, Rain Liivoja and Lauren Sanders, "The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems," *Journal of Conflict & Security Law* 28, no. 2 (2022); Tim McFarland and Zena Assaad, "Legal Reviews of *in situ* Learning in Autonomous Weapons," *Ethics and Information Technology* 25, no. 9 (2022); Ryan Poitras "Article 36 Weapons Reviews & Autonomous Weapon Systems: Supporting an International Review Standard," *American University International Legal Review* 34, no. 2 (2018).
72. See Klaudia Klonowska, "Article 36: Review of AI Decision-Support Systems and Other Emerging Technologies of War," *Asser Institute Research Paper Series* (2021).
73. Klonowska, "AI Decision-Support Systems," 3.
74. These limitations include AI biased data, learning curves, and AI's ability to classify objects.

ample, a simulation study involving pilots in cockpit simulators found that pilots often trusted faulty, non-intuitive system recommendations over their own judgment.[75] She contends that AI-DSS can significantly impact human decision-making processes and, for this reason, should be subjected to legal review.[76]

The third criterion considers whether AI-DSS provides actionable intelligence for commander decision-making. Klonowska distinguishes between "algorithms that simply present information and those that provide *actionable intelligence*"[77] [emphasis in original]. In the latter case, AI-DSS equipped with machine learning or deep neural networks can identify moving objects (such as vehicles), track their direction of movement, identify individuals, and perform other functions. Such systems may highlight specific data points or prioritize certain features autonomously, potentially altering—rather than assisting—commander decision-making.[78]

Finally, the fourth criterion evaluates whether an AI-DSS is *intended* and *capable* of producing direct or indirect effects on the battlefield—particularly harm, damage, or injury.[79] Klonowska notes that the intended use of the system—specifically, its contribution to hostilities through offensive capabilities—is central to determining the applicability of Article 36 reviews. AI-DSS operates through various constellations of interaction, including human-to-machine and machine-to-machine communication, and functions across multiple stages of the kill chain.[80]

75. Linda J, Skitka, Kathleen L,Mosier,and Mark Burdick , 'Does Automation Bias Decision-Making?' *International Journal of Human-Computer Studies 51, no.* 5 (1999). ). To be sure, the capabilities of AI have dramatically improved since this study, and there has been plenty of research where instances where pilots ignored AI recommendations and human judgement led to adverse outcomes.
76. Klonowska, "AI Decision-Support Systems," 24.
77. Klonowska, "AI Decision-Support Systems," 24.
78. Klonowska, "AI Decision-Support Systems," 25. Deeks et al. make a similar argument: "machine learning calculations could consequently play a critical role in life and death decisions for whole countries...the role of algorithms in the underlying calculations could lead states to unwittingly make war-related decisions almost entirely based on machine calculations and recommendations." Ashley Deeks, Noam Lubell and Daragh Murray, "Machine Learning, Artificial Intelligence, and the Use of Force by States," *Journal of National Security Law & Policy* (2019), 1-26.
79. Klonowska, "AI Decision-Support Systems," 16.
80. According to Arthur Holland Michel, "the lead-up to a strike may involve dozens or hundreds of separate algorithms, each with a different job, passing findings not just to human overseers to also from machine-to-machine." Arthur Holland Michel, "The Killer Algorithms Nobody's

Algorithms play a critical, iterative role in processes that lead to the use of force and "definitely will affect the control or limit the decision of others in the [kill] chain."[81]

There is no global consensus on whether AI-DSS falls within the scope of Article 36 review processes. However, Klonowska overlooks the fact that the already complex and rigorous acquisition and procurement procedures for any new system—including AI-DSS—can address many of these concerns.[82] Certainly, if an AI-DSS does not undergo a formal weapons review, it may not be subject to the same level of scrutiny regarding compliance with IHL considerations as it would under an Article 36 review. Nevertheless, given that AI-DSS likely incorporates machine learning, LLMs, and/or deep-learning techniques, such systems would undergo extensive testing, evaluation and validation to ensure reliable performance within their intended operational context.

Some states have modified their often cumbersome and slow acquisition process to better align with the rapid pace of AI innovation.[83] These changes stem from defense officials collaborating with non-traditional partners—particularly technology companies developing dual-use technologies—and from frustration with bureaucratic red tape that has hindered the acquisition of cutting-edge capabilities. Although the acquisition process still requires further reform to support the effective adoption of AI-DSS, much of it remains inaccessible to the public. Nonetheless, revised acquisition and procurement practices offer an opportunity to address many of Klonowska's concerns. Such revisions could include a form of legal review specifically tailored to non-weaponized applications of AI.

Talking About," *Foreign Policy*, January 20, 2020, https://foreignpolicy.com/2020/01/20/ai-autonomous-weapons-artificial-intelligence-the-killer-algorithms-nobodys-talking-about/

81. Merel 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).
82. For more on AWS and acquisition and procurement, see Trabucco, "Autonomous Weapon Systems."
83. See Trabucco, "Autonomous Weapon Systems," for a detailed assessment of acquisition changes in the US and UK to account for AI-specific modifications.

## 3.2. Targeting and AI Decision-Support Systems

As the previous section outlined, technology plays a critical role in targeting decision-making, often informing and complementing human judgment and established decision-making protocols. Accordingly, within the targeting context, it is essential to consider what AI-DSS introduces that is novel to the targeting process.

To assess the legal implications of AI-DSS in targeting, it is important to distinguish between two forms of targeting—deliberate targeting and dynamic targeting—which involve different rules of engagement and may incorporate AI through varying procedures and protocols. Deliberate targeting involves preplanned and preapproved targets that are already known within the operational environment. In contrast, dynamic targeting addresses unanticipated targets, previously unidentified targets, or "targets that were detected, located or selected in insufficient time to be included in the deliberate process."[84] Dynamic targeting is more responsive in real-time than deliberate targeting and often requires decision-making based on incomplete or unverified information and insufficient time to gather more or validate existing information than is typically the case in deliberate targeting. Despite these differences, both forms of targeting follow the same procedural steps and require adherence to the same rules and principles of targeting law.[85]

The most significant distinction between the two forms of targeting is time. Deliberate targeting refers to pre-planned targets or situations where there is sufficient time to assess and transmit a targeting package. In contrast, dynamic targeting involves targets not identified in advance but that meet specific criteria aligned with mission objectives. It is also used when plans are adjusted in response to evolving conditions or newly available information. A core assumption of IHL is that commanders carry out targeting protocols in good faith, based on the information available to them at the time. AI-DSS may offer them access to an unprecedented volume of information; potentially an overwhelming amount, as discussed below. Critically, however, AI-DSS accelerates the

84. Merel A. C. Ekelhof, *The Distributed Conduct of War: Reframing Debates on Autonomous Weapons, Human Control and Legal Compliance in Targeting* (PhD thesis, Vrije Universiteit Amsterdam, 2019), 52.

85. NATO, AJP-3.9 Allied Joint Doctrine for Joint Targeting (2016), p. 1-3.

information flow, presenting both opportunities and challenges for applying the "reasonable commander" standard.

### 3.2.1. Reasonable Commander Standard

The standard of reasonableness permeates all aspects of targeting and IHL. Some experts regard reasonableness as the "touchstone" of the rules governing armed conflict.[86] The lawfulness of targeting requires combatants to conduct operations in accordance with the principles of distinction, proportionality and precaution. The principle of distinction obliges parties to a conflict to differentiate between military objectives and civilian objects, as well as between combatants and civilians.[87] The principle of proportionality prohibits attacks in which the expected civilian harm would be excessive in relation to the anticipated military advantage.[88] The principle of precaution requires all feasible measures to be taken to minimize harm to civilians during military operations.[89] Embedded within each of these principles, "reasonableness remains the touchstone for determining the appropriate application of specific targeting rules and for assessing the lawfulness of action after the fact."[90]

International law assumes that "decisions are based on reasonable expectations rather than results. In other words, honest mistakes often occur on the battlefield due to a 'fog of war' or when it turns out that reality does not match expectations."[91] This concept dates back to the Nuremberg Tribunal's decision in the case of General Lothar Rendulic, which held that his destructive actions were not criminal, as they were based on his judgment and the information available to him at that time.

The "reasonable commander" standard is inherently difficult to define with precision, as it is context-dependent. However, it is useful to clarify the notion of reasonableness in relation to each of the core prin-

86. Laurie Blank, "New Technologies and the Interplay between Certainty and Reasonableness," in *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, eds. Christopher M. Ford and Winston S. Williams (Oxford University Press, 2019).
87. Additional Protocol I, art. 48.
88. Additional Protocol I, arts. 51(5)(b), 57(2)(a)(iii), and 57(2)(b).
89. Additional Protocol I, art. 57(1).
90. Blank, "New Technologies," 321.
91. Michael N. Schmitt, Charles H. B. Garraway, and Yoram Dinstein, *The Manual on the Law of Non-International Armed Conflict—With Commentary* 23 (International Institute of Humanitarian Law, 2006); quoted in Blank (2019), 321.

ciples of IHL before analyzing how AI-DSS may complicate current interpretations of this standard.

As previously discussed, the principle of distinction requires parties to a conflict to differentiate between objects and individuals that constitute legitimate targets (e.g., combatants, military objectives, civilians directly participating in hostilities) and those that are protected from attack (e.g., civilians, civilian objects, *hors de combat* combatants, medical personnel). Making such determinations is often difficult, and errors do occur. However, IHL requires that attackers make these determinations objectively and reasonably at the time of action. For instance, a *hors de combat* combatant—whether due to sickness, injury, surrender or capture—may not lawfully be targeted under IHL.[92] The determination of whether someone is *hors de combat* must be based on the attacker's reasonable belief *at the time*.[93]

The principle of proportionality is traditionally where the notion of reasonableness is attributed. It requires "that a commander assess, at the time of the attack, the expected likely civilian casualties and the anticipated military advantage gained from the attack and then determine, based on good faith judgment, whether the expected civilian casualties will be excessive so as to preclude the attack."[94] Both international jurisprudence[95] and military manuals[96] recognize the critical role of the "responsible commander" in making proportionality assessments. In the *Galić* case, the International Criminal Tribunal for the Former Yugoslavia (ICTY) held that "[i]n determining whether an attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable

92. Additional Protocol I, art. 41.
93. Blank, "New Technologies," 322; see Geoffrey S. Corn, Laurie R. Blank, Chris Jenks, and Eric Talbot Jensen, Belligerent Targeting and the Invalidity of a Least Harmful Means Rule, *International Law Studies* 89 (2013), 536, 587.
94. Blank, "New Technologies," 323; Additional Protocol I, arts. 51(5)(b), 57(2)(a)(iii), and 57(2)(b).
95. Prosecutor v. Galić, Case No. IT-98-29-T, Judgment, (International Criminal Tribunal for the Former Yugoslavia Dec. 5, 2003) at para. 58
96. For example, Office of the Judge Advocate General, National Defence of Canada, *The Law of Armed Conflict at the Operational and Tactical Levels* (1992) sec. 5 para. 27 ("Consideration must be paid to the honest judgement of responsible commanders, based on the information reasonable available to them at the time").

use of the information available to him or her, could have expected excessive civilian casualties to result from the attack."[97]

Finally, the principle of precautions requires both reasonableness and feasibility. Article 57 of Additional Protocol I requires those who plan or decide upon an attack to "do everything feasible" and "take all feasible precautions."[98] However, what is deemed feasible depends on the specific conditions faced by commanders or soldiers in the operational environment. Accordingly, the International Committee of the Red Cross (ICRC) Commentary recognizes that precautions and feasibility assessments will "be a matter of common sense and good faith."[99]

Can a commander meet the standard of reasonableness when relying on AI-DSS? Would there be sufficient grounds to deem a commander "unreasonable" for decisions informed by AI-DSS data or recommendations? If inadvertent outcomes or grave breaches result from following AI-DSS recommendations, does this render the commander's actions unreasonable? Does this create an accountability gap?

Experts have been grappling with these questions to varying degrees, although the debate has been more developed in the context of AWS than AI-DSS.[100] The key distinction—and one that is critical to acknowledge—is that with AI-DSS, it is still the commander, often supported by an entire targeting board (sometimes called a strike cell), who ultimately evaluates the information and authorizes the attack. Legal considerations, especially those related to proportionality and precautions, are still reviewed by human legal advisors. The recommendations produced by an AI-DSS constitute one tool among many that may assist or guide commanders in their decision-making. Nonetheless, the actions taken by commanders in response to AI-DSS data and the degree of reliance placed on that data provide critical insights of relevance to the questions posed above.

On the one hand, it is reasonable to conclude that AI-DSS is not fundamentally new. Technology is already deeply integrated into target-

97. Prosecutor v. Galić, at para. 58; see also Ian Henderson and Kate Reece, "Proportionality under International Humanitarian Law: The 'Reasonable Military Commander' Standard and Reverberating Effects," *Vanderbilt Journal of Transnational Law* 51 (2018), 835-55.
98. Additional Protocol 1 art. 57(ii)
99. Additional Protocol I, Commentary at 682; Blank (2019), 324.
100. See for example Blank, "New Technologies;" Deeks et al., "Machine Learning."

ing decision-making processes, and since AI-DSS is not autonomous in function, commanders remain the ultimate decision-makers. One might argue that AI-DSS simply provides information derived from data analysis, much like human analysts do. On the other hand, certain aspects of AI-DSS introduce new challenges. AI-DSS not only processes data but also frames and presents its interpretation of a military problem and its possible solutions—effectively shaping what is considered a military necessity. A significant concern is the inability to trace the system's outputs back through the specific analytical process it followed. This black box phenomenon in AI systems creates two key issues: (1) the inability to understand how a particular conclusion or recommendation was reached; and (2) the inability to confirm that the system performed as intended.

Ultimately, the deployment of AI-DSS gives rise to three anticipated outcomes with legal implications. The impact of AI—specifically AI-DSS—on legal standards and interpretations is not yet well understood, partly due to the relative novelty of the use of such systems (especially for targeting generation). While considerable scholarly attention has been given to the reasonableness standard in the AWS context, much less has been devoted to decision-support systems and how commanders incorporate AI analysis and data into their decisions.

One anticipated outcome is a growing demand for certainty in targeting decisions. As AI technology becomes more advanced and accurate, expectations concerning precision increase. This shift has tangible battlefield consequences. One of the key advantages of integrating AI-DSS is its capacity to overcome the cognitive limitations of human decision-making under crisis conditions.[101] Humans are notoriously susceptible to make mistakes, biases and other forms of error, particularly when operating under stress. By contrast, AI systems are not subject to emotional responses or physiological limitations, such as fatigue, cognitive overload or the need for (e.g., bathroom) breaks. With this shift in the conditions under which decisions are made comes the expectation that "while autonomous weapon systems cannot be required to be perfect, they will in practice be held to standards that are significantly higher

101. Trabucco and Heller, "Beyond the Ban;" Steward and Hinds, "Algorithms of War."

than those posed for humans."[102] This expectation applies just as much to AI decision-support systems as it does to autonomous weapon systems.

Utilizing advanced AI-DSS systems may push targeting decision-making towards greater certainty compared to decisions made without such support. This shift could result in overly cautious commanders, potentially leading to slower processing times for target validation and redundant efforts by legal advisors and other key analysts. Conversely, it may also result in overreliance on AI-DSS, introducing high risk of automation bias; that is, undue trust in the information and recommendations produced by the AI. Each of these outcomes has operational implications and introduces new risks into the operational environment.

A second outcome is the increased risk of adversarial attacks. Adversaries or other malicious actors could exploit AI-DSS to manipulate data outputs, particularly target recommendations. There is a significant risk embedded in decision-making protocols within systems that adversaries could feasibly manipulate, potentially resulting in false target recommendations against friendly forces or civilian-populated areas. While validation and verification are already required for IHL compliance, they also serve as essential risk mitigation measures for protecting national or allied forces.

A third outcome involves the volume of data AI-DSS can produce. The sheer quantity of target recommendations could easily overwhelm human analysts, operators or commanders. This issue is especially acute in dynamic targeting contexts, where time is often a decisive factor in life-or-death decisions. States must therefore implement protocols for data management and establish procedures to mitigate the risk of overloading analysts with information.

One final consideration is whether commanders have valid reason to question the outputs of an AI-DSS. If the recommendations—or any system-generated outputs—consistently produce errors or prove unreliable, the commander has a duty to disregard that information. Even in scenarios where strategic-level directives mandate the use of specific

102. Christoph Heyns, "Increasingly Autonomous Weapon Systems: Accountability and Responsibility," in *Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects* (International Committee for the Red Cross, 2014), 45; Carrie McDougall, "Autonomous Weapon Systems and Accountability: Putting the Cart Before the Horse," *Melbourne Journal of International Law* 20 (2019).

systems, if the data quality is poor, the AI-DSS cannot be responsibly deployed in an operational setting. Because many AI-DSS platforms represent cutting-edge technology with the potential to significantly influence military planning and command—especially in tactical targeting—there may be a natural inclination to over-rely on such systems or to present them as advanced capabilities with deterrent value. Nevertheless, if reasonable doubt arises regarding the reliability of these systems, a responsible commander must refrain from using the AI-DSS and should cease its use as soon as that doubt becomes apparent.

### 3.2.2. Case Study: "Gospel" and Military Decision-Making

Media reports have revealed how the Israeli Defense Forces (IDF) uses AI, specifically, an AI-DSS system called "the Gospel", which has been integrated into ongoing IDF targeting procedures in the Israeli-Hamas conflict since the attack on October 7, 2023. Critics of the system have used media outlets to label Gospel a "data factory" or "mass assassination" machine.[103] Regardless of media portrayals, Gospel serves as a concrete example of the type of AI-DSS this report addresses. Consequently, it is important to examine it more closely and apply the legal concerns outlined above to this specific case study.

The IDF's use of AI for targeting purposes includes three AI systems that work together: Alchemist, Fire Factory and Gospel.[104] The first two systems broadly analyze and classify large amounts of data. Gospel is the third system, which evaluates the Alchemist and Fire Factory data, along with other classified and non-classified data sources (e.g., social media).[105] The Gospel system then produces a targeting recommendation for consideration and authorization by a team of targeting analysts, which includes a legal adviser, intelligence officer, operational officer, an

103. 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; Yuval Abraham, "A Mass Assassination Factory: Inside Israel's Calculated Bombing of Gaza," *+972 Magazine*, November 20, 2023, https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

104. 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

105. Brumfiel, "Israel Using AI System."

engineer from the Israeli Air Force (for air attacks) and a munitions expert (collectively called the "targeting room").[106] The type of package delivered by Gospel is the same output a team of human targeting analysts would produce (and which would undergo the same targeting-room consideration).

The novelty of the Gospel system is found in its ability to provide target recommendations significantly faster than a team of human analysts is able to do. Gospel can generate 200 targets in 10 days, whereas it would take approximately 25-30 analysts 200 days to produce the same number.[107] Gospel can recommend stationary targets (e.g., buildings, other military objects), while other systems, notably "Lavender," focus on individuals. According to Israeli protocol, if the target is a stationary military object, it must be approved by a high-ranking military officer.[108] However, if the target is an individual, approval must come from the Chief of Staff or, if unavailable, the Vice Chief of Staff.[109]

Concerns have also been raised about overwhelming human analysts—or, in the IDF's case, the targeting room—with a massive volume of information and target recommendations. It is reasonable to imagine analysts and operators being overwhelmed by the pace and volume of data, leading to diminished scrutiny in target verification. This type of overload may result in automation bias, where analysts or operators over-trust a system that has, for example, been accurate 90% of the time. Such overreliance could lead to the authorization of unverified targets, increasing the risk of inadvertently targeting civilians.

Can an IDF commander escape culpability by claiming that civilian deaths resulted from a Gospel system recommendation? Ultimately, no. While there may be legitimate concerns regarding the nature of target recommendations or the quality of data used, the targets are clearly authorized at multiple levels within the chain of command. The IDF is legally obligated to ensure that AI-DSS-generated targets are verified and lawful, that the attack is necessary and proportionate, and that all feasible precautions are taken to protect civilian populations.

106. Brumfiel, "Israel Using AI System."
107. Brumfiel, "Israel Using AI System."
108. Which officer that is could depend on a number of factors (e.g., which service, the timeline for the target).
109. Brumfiel, "Israel Using AI System."

The Gospel represents a real-world case that grapples with these issues in real time. This case study demonstrates how states—including Denmark—that are preparing to adopt AI-DSS must establish procedures to anticipate and mitigate such challenges. Denmark, in particular, should consider mechanisms to manage the potentially overwhelming volume of data produced by such systems so that it can be processed and acted upon reasonably and responsibly.

### 3.2.3. Case Study: "Lavender" and Meaningful Human Control

Another consideration is how AI-DSS interacts with human decision-makers and the inherent risks of using AI in the targeting process. There are obvious risks associated with delegating such high-stakes decisions. AI-DSS may contain errors in the code chain, potentially leading to inaccurate outputs; the system could also malfunction without human awareness; or it may reach incorrect conclusions regarding the legitimacy of a particular target. However, the key difference between an AI-DSS and an autonomous AI system is that an AI-DSS cannot take any specific action; it only generates information. In other words, humans must take positive action based on this information.

This raises important questions about human interaction and control. In the debate over autonomous weapons, these systems function as the ultimate gatekeeper for targeting decision-making protocols due to their autonomous nature, prompting many experts to advocate for a form of "meaningful human control" over such weapon capabilities. However, within the AI-DSS framework, human judgment remains integral to the targeting process, as it necessitates positive action and authorization from human agents. To better understand this within the context of human control, it is useful to examine some proposals for meaningful human control (MHC).

The term first appeared in a 2013 report by Article 36, a British NGO.[110] In this report, Article 36 proposed three elements that satisfy the MHC of an autonomous weapon:

110. Article 36, *"Killer Robots: UK Government Policy on Autonomous Weapons"* (Apr. 2013) https://article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf

1. Information—A human operator, and others responsible for attack planning, must have adequate contextual information about the target area of an attack, information on why any specific object has been suggested as a target, information on mission objectives, and information on the immediate and longer-term effects that will result from an attack in that context.
2. Action—Initiating the attack should require a positive action by a human operator.
3. Accountability—Those responsible for assessing the information and executing an attack must be accountable for its outcomes.

Other expert groups have proposed criteria similar to those outlined by Article 36. For example, the International Committee for Robot Arms Control (ICRAC) proposed minimum conditions necessary for MHC, including:

1. A human commander (or operator) must have full contextual and situational awareness of the target area and be able to perceive and react to any change or unanticipated situations that may have arisen since planning the attack.
2. There must be active cognitive participation in the attack and sufficient time for deliberation on the nature of the target, its significance in terms of the necessity and appropriateness of the attack, and likely incidental and possible accidental effects of the attack.
3. There must be a means for the rapid suspension or abortion of the attack.[111]

111. Frank Sauer, "ICRAC Statement on Technical Issues to the 2014 UN CCW Expert Meeting", International Commision for Robot Arms Control, May 14, 2014.
Other groups have put forward other similar criteria. For example, Michael Horowitz and Paul Scharre proposed:
    1. "Human operators are making informed, conscious decisions about the use of weapons;
    2. Human operators have sufficient information to ensure the lawfulness of the action they are taking, given what they know about the target, the weapon, and the context for action;
    3. The weapon is designed and tested, and human operators are properly trained, to ensure effective control over the use of the weapon."

Let us examine the IDF system Lavender against these criteria. Under the proposed criteria, the first element requires human operators—or Lavender's human targeting analysts—to have full situational and contextual awareness. Targeting analysts will undoubtedly maintain operational situational awareness, as their ability to perceive operational context has not changed. There is an inherent risk in using a system like Lavender for target nomination, however, because there may be minimal transparency regarding how the system arrived at a particular conclusion for a specific target. This lack of transparency could diminish the sense of awareness, since the analyst is relying on the system's assessment. This context differs from merely relying on data from technical sources (e.g., drones, sensors, or other forms of data), because a human would still have performed the assessment or analysis; in the case of Lavender, that step is delegated to the AI-DSS. This introduces a new risk but does not necessarily compromise the situational awareness element entirely.

The second element requires positive human action. This remains evident in Lavender's use case, as the output necessitates authorization and action from human analysts and appropriate commanders. How this element operates in practice may vary by context and national culture. However, early reporting on Lavender indicates that "human personnel often served only as a 'rubber stamp' for the machine's decisions," adding that they would typically allocate only about "20 seconds" to each target before authorizing a bombing—simply to ensure that the Lavender-marked target is male.[112] The "positive human action" element likely aims to compel militaries to preserve human judgment within the targeting chain, ensuring that targets—especially human ones—are vetted and validated by humans against an IHL backdrop. Reports indicating that Lavender output received only "20 seconds" of validation are unlikely to meet the intent of this criterion.

The third element differs between proposals. The first proposal requires maintaining accountability for those responsible for planning and carrying out the attack. It is unlikely that analysts or commanders could avoid criminal accountability simply because they employed an AI-DSS. As the second criterion is still present with an AI-DSS—that is, human

112. 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/

action and target validation are still required under IHL—any failure to follow protocol could result in liability. Whether any particular military body follows that protocol in practice is a separate issue, but it does not negate the possibility of individual criminal responsibility simply because an AI-DSS was employed in a particular operation.

The third criterion in the second proposal requires appropriate time and means for the suspension or abortion of an attack. Since Lavender is not an autonomous system (i.e., it involves human supervision), this element is not applicable to the AI-DSS case. Here, humans are still responsible for carrying out the attack and are therefore able to abort it if necessary, such as due to changing circumstances on the ground.

# 4

# Conclusion

AI already informs or directly guides strategic and operational decision-making in modern conflicts through new weapons capabilities and AI decision-support systems (AI-DSS). This development signals a qualitative shift in the tools and agents responsible for real-time strategic and operational decision-making. As Denmark and its partners continue to develop and integrate emerging technological capabilities, it is vital to explore the capabilities, operational benefits, and legal risks of integrating AI into the broader Command and Control (C2) structures. This report is a stepping stone towards filling that gap.

Significant benefits arise from AI-DSS. These systems are "computerised systems that use AI software to display, synthesise, and/or analyse data and, in some cases, make recommendations—even predictions—to aid human decision-making in war."[113] AI systems can enhance the strengths of human decision-making and cognition through improved situational awareness and expedited processes. Furthermore, AI-DSS can contribute to tactical military decisions fulfilling military objectives and translating strategic goals into military plans and operations. Therefore, AI has the potential for profound implications not only for the application of military force but also for how military decision-makers perceive the environment in which they operate.

AI-DSS also poses great risks and challenges for wartime decision-making. For example, military innovation builds on civilian advances, which can introduce significant concerns regarding transparency and data quality. Additionally, this could raise legal and ethical consider-

113. Stewart and Hinds, "Algorithms of War."

ations for utilizing systems built by civilian technology firms, including the quality of training and data-testing. There may be concerns about how the models are trained and whether—or to what extent—civilian contractors can train models on classified data to ensure that the model performs as expected in dynamic operational environments.

Important multinational and national initiatives also signal the ongoing integration of AI-DSS into essential C2 structures. For example, NATO released an AI strategy in 2021 that included principles for responsible AI development and launched DIANA to establish stronger connections between NATO and industry innovation across a range of critical technologies, including AI. NATO also has tangible AI and C2 developments, notably the ANTICIPE project, which focuses on utilizing AI-enabled technologies to help develop, monitor and assess a commander's critical information requirements, facilitating much faster decision-making. The United States has taken significant steps to incorporate AI through an AI and Data Acceleration initiative, where the DoD's operational data and AI teams of technical experts visit the military's 11 combatant commands to aid them in better understanding their data and creating AI tools to streamline decision-making across Joint All-Domain Command and Control.

Denmark is facing a different strategic landscape compared to NATO and other partners, including the United States, but has nonetheless begun taking essential steps toward AI integration into Danish C2. There are important lessons for Denmark. We argue that incorporating AI into Danish C2 must support ongoing competitive situations and crises in the Baltic region. In this context, Denmark should be able to detect and counter hybrid threats with military means and respond effectively during a state of war. In the framework of NATO's collective defense, Denmark must have the necessary C2 to ensure the advancement of allied forces and operations from Danish air stations against both hybrid and military threats. Furthermore, Denmark must be able to function as a battlespace owner in one or more military domains, and Danish C2 must be integrated with NATO.

This report has discussed key legal considerations regarding AI in C2. It has covered the potential for Article 36 legal reviews of AI-DSS, as well as alternative regulatory avenues when such reviews are absent—particularly focusing on acquisition and procurement as pathways for AI assurance. Furthermore, it has addressed the potential for human

control and the legal responsibility associated with AI-DSS in targeting decision-making. Additionally, it has presented concrete case studies on Israel's use of AI-DSS.

We have already witnessed the integration of AI-DSS into modern warfare. As this report indicates, however, Danish decision-makers will grapple with a broad range of implications—both potential benefits and novel risks—in the years ahead. Clearly, AI-DSS will be essential to a contemporary and interoperable Danish Defense Force as Denmark and its partners confront modern security threats. While further consideration is necessary to appreciate and evaluate the impact of AI-DSS fully, this report offers a critical first step.

## 4.1. Recommendations

1. Denmark will benefit from increased AI adoption in national C2 processes, streamlining information processing and improving the quality of command decision-making.
2. Denmark should recognize AI as more than just a technological tool and instead view it as a vital strategic competence. This perspective could involve incorporating AI into command exercises and training, as well as offering educational opportunities for specialists and officers to develop AI competencies in anticipation of future iterations and advancements in AI development.
3. When implementing new AI command systems, the Danish Armed Forces should evaluate the AI according to the EU ALTAI standards as applied in the AI4DEF projects.
4. Denmark should concentrate on utilizing open-source data, NATO systems (e.g., FELIX) and commercially available models tailored to specific military purposes, sometimes in collaboration with industry. This collaboration should also ensure that the systems managing daily operations have the classification levels required to utilize AI systems throughout the organization, including territorial aspects.
5. Denmark should initiate an inquiry into whether the current Defense law regulating the use of AI decision-support systems and their access to civilian data requires amendment to include access to civilian data and services (under the provisions of § 17 of the current Defense law).

6. Danish commanders should be provided with sufficient information about AI-DSS training, testing experience and system risk to fulfil the responsible commander standard.
7. Given the specific and contextual nature of AI decision support, Denmark should seek greater cooperation with NATO allies within the regional area of operation to promote AI-DSS use in commands at the joint operational level and the higher tactical level, particularly within the framework of the Nordic Defence Concept.

# Appendix

**Figure 2: AIP for Defense Demonstration—Palantir.com**

| COA 1 - Target with Air Asset | |
|---|---|
| Time required: | 18 min |
| Asset: | HAWK11 (F-16) |
| Armament: | 4x AGM-114 |
| Distance to Target: | 40.3 km |
| Fuel Level: | 935 kg (89%) |
| Personnel Req. | 8 |

| COA 2 - Target with Long Range Artillery | |
|---|---|
| Time required: | 7 min |
| Asset: | Knight 114 (HIMARS) |
| Armament: | 4x ER GMLRS |
| Distance to Target: | 53.5 km |
| Vehicle status: | READY |
| Personnel Req. | 4 |

| COA 3 - Target with Tactical Team | |
|---|---|
| Time required: | 2 hrs 15 min |
| Team: | Team Omega |
| Armament: | 6 Javelin Missile |
| Distance to Target: | 39.5 km |
| Team Status: | ON MISSION, READY |
| Personnel Req. | 9 |

# Bibliography


Abraham, Yuval. "A Mass Assassination Factory: Inside Israel's Calculated Bombing of Gaza." *+972 Magazine*, November 20, 2023. https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

Abraham, Yuval. "'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/

*Advancing the Science and Acceptance of Autonomy for Future Defense Systems: Hearing Before the Subcommittee on Emerging Threats and Capabilities of the Comm. on Armed Services*, 114th Cong. 1 (2015). https://www.hsdl.org/?view&did=793840

Alberts, David S., Richard E. Hayes, and John Stenbit. *Power to the Edge: Command, Control in the Information Age* (Vol. 259). CCRP Publication Series, 2003.

Article 36. *"Killer Robots: UK Government Policy on Autonomous Weapons"* (April 2013). https://article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf

Barker, William C. "Guideline for Identifying an Information System as a National Security System." National Institute of Standards and Technology, August 2003, 13. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf

Berndtsson, Joakim, Anne Roelsgaard Obling, and Åse Gilje Østensen. "Business-Military Relations and Collaborative Total Defence in Scandinavia." In *Total Defence Forces in the Twenty-First Century*. McGill-Queen's University Press, 2023.

Blank, Laurie. "New Technologies and the Interplay between Certainty and Reasonableness". In *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*, edited by Christopher M. Ford and Winston S. Williams. Oxford University Press, 2019.

Bolton, Christopher R., and Matthew R. Prescott. "Commander's Critical Information Requirements: Crucial for Decisionmaking and Joint Synchronization." *Joint Force Quarterly* 113 (2024). https://digitalcommons.ndu.edu/joint-force-quarterly/vol113/iss1/15

Brooks, Risa. "Technology and Future War Will Test US Civil-Military Relations." *War on the Rocks* (2018). https://warontherocks.com/2018/11/technology-and-future-war-will-test-u-s-civil-military-relations/

Brumfiel, Geoff. "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

Copeland, Damian, Rain Liivoja, and Lauren Sanders. "The Utility of Weapons Reviews in Addressing Concerns Raised by Autonomous Weapon Systems." *Journal of Conflict & Security Law* 28, no. 2 (2022).

Corn, Geoffrey S., Laurie R. Blank, Chris Jenks, and Eric Talbot Jensen. Belligerent Targeting and the Invalidity of a Least Harmful Means Rule, *International Law Studies* (2013) 89: 536, 587.

Crosby, Courtney. "Operationalizing Artificial Intelligence for Algorithmic Warfare." *Military Review*, July-August (2020), 43.

Davies, Harry, 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.

Deeks, Ashley, Noam Lubell, and Daragh Murray. "Machine Learning, Artificial Intelligence, and the Use of Force by States." *Journal of National Security Law & Policy* 10 (2019), 1-26.

Defence Innovation Accelerator for the North Atlantic. "Test Centres." https://www.diana.nato.int/test-centres.html

Defense Science Board. *Report of the Defense Science Board Summer Study on Autonomy*; Executive Office of the President, Preparing for the Future of Artificial Intelligence October (2016). https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

Department of Air Force Press Release. *"Artificial Intelligence and Next Generation Distributed Command and Control."* February 29, 2024. https://sam.gov/opp/d8eb1d7f980d4c02b080d87747297ee6/view

Department of Defense. "Department of Defense Announces Joint Warfighting Cloud Capability Procurement." https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/

Department of Defense (2020) Data Strategy. DOD Data Strategy (defense.gov).

Deptula, David. "Combat Cloud Is the New Face of Long-Range Strike." *Armed Forces Journal,* September 18, 2013. http://armedforcesjournal.com/deptula-combat-cloud-is-new-face-of-long-range-strike/

Ekelhof, Merel. "Lifting the Fog of Targeting: 'Autonomous Weapons' and Human Control through the Lens of Military Targeting." *Naval War College Review* 71, no. 3 (2018).

Ekelhof, Merel A. C. *The Distributed Conduct of War: Reframing Debates on Autonomous Weapons, Human Control and Legal Compliance in Targeting* (PhD Thesis - Research and graduation internal, Vrije Universiteit Amsterdam, 2019).

Ellman, Jesse, Lisa Samp, and Gabriel Coll, *Assessing the Third Offset Strategy*. Center for Strategic and International Studies, March 2017), 6–8.

European Union, Policy and Legislation. "Commission Publishes the Guidelines on Prohibited Artificial Intelligence (AI) Practices, as Defined by the AI Act." *Shaping Europe's Digital Future*. February 4, 2025. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

First Army. "First Army Taps Artificial Intelligence to Enhance Command and Control." https://www.first.army.mil/News/ArticleView/Article/3613646/first-army-taps-artificial-intelligence-to-enhance-command-and-control/

Folketinget. "Forslag til lov om ændring af lov om politiets virksomhed", L 171, 2017.

Forsvaret. "Aftale om Forsvaret 2018-2023. https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-forsvarsforlig-2018-2023-2018.pdf

Forsvaret. "Ny 20-årig rammeaftale med Systematic om operative it-systemer til hele forsvaret. https://www.fmi.dk/da/nyheder/2023/ny-20-arig-rammeaftale-med-systematic-om-operative-it-systemer-til-hele-forsvaret/

Forsvarsministeriet (2018) Aftale på Forsvarsområdet 2018-2023. FMN 28. january 2018.

Forsvarsministeriet. "Bekendtgørelse af lov om forsvarets formål, opgaver og organisation m.v." LBK nr 582. Maj 2017.

Forsvarsministeriets Materiel- og Indkøbsstyrelse (2023) Ny 20-årig rammeaftale med Systematic om operative it-systemer til hele forsvaret. FMI 21. February 2023

Gill, Jaspreet. "DoD Releases New AI Adoption Strategy Building on Industry Advancements." *Breaking Defense*, November 2, 2023. https://breakingdefense.com/2023/11/dod-releases-new-ai-adoption-strategy-building-on-industry-advancements/?utm_content=buffer6e382&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer

Haga, Wes, and Courtney Crosby. "AI's Power to Transform Command and Control." *National Defense* Magazine (2020). https://www.nationaldefensemagazine.org/articles/2020/11/13/ais-power-to-transform-command-and-control

Hambling, David. "Ukraine's AI Drones Seek and Attack Russian Forces without Human Oversight." *Forbes*, October 17, 2023. https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/

Henderson, Ian, and Kate Reece. "Proportionality under International Humanitarian Law: The 'Reasonable Military Commander' Standard and Reverberating Effects." *Vanderbilt Journal of Transnational Law* 51 (2018): 835-55.

Heyns, Christoph. "Increasingly Autonomous Weapon Systems: Accountability and Responsibility." In *Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects*. International Committee for the Red Cross, 2014, 45.

Human-Centered Artificial Intelligence. "Artificial Intelligence Definitions," HAI Stanford University https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf

Johnson, James. "Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age." *Defence Studies 1* no 23 (2022): 43-67.

Joint Publication 1-02; United States Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf

King, Anthony. "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence." *Journal of Global Security Studies* 9, no. 2 (2024).

Klonowska, Klaudia. "Article 36: Review of AI Decision-Support Systems and Other Emerging Technologies of War." *Asser Institute Research Paper Series* (2021).

Larsen, Esben S., and Rasmus Dahlberg. *Hjemmefronten, nationale operationer frem mod 2035*. DJØF Publishing, 2024.

McDougall, Carrie. "Autonomous Weapon Systems and Accountability: Putting the Cart before the Horse." *Melbourne Journal of International Law* 20 (2019).

McFarland, Tim, and Zena Assaad, "Legal Reviews of *in situ* Learning in Autonomous Weapons." *Ethics and Information Technology* 25, no. 9 (2022).

Michel, Arthur Holland. "The Killer Algorithms Nobody's Talking About." *Foreign Policy* January 20, 2020. https://foreignpolicy.com/2020/01/20/ai-autonomous-weapons-artificial-intelligence-the-killer-algorithms-nobodys-talking-about/

Mulchandani, Nand, and Jack Shanahan. *Software Defined Warfare: Architecting the DoD's Transition to the Digital Age*, CSIS (2022). https://www.csis.org/analysis/software-defined-warfare-architecting-dods-transition-digital-age

NATO. AJP-3.9 Allied Joint Doctrine for Joint Targeting (2016).

NATO Allied Command Operation. "NATO acquires AI-enabled Warfighting System". SHAPE.

NATO Allied Command Transformation. "Joint Force Development Experimentation & Wargaming Branch Fact Sheet – Human Considerations in Artificial Intelligence for Command and Control: Augmented Near Real-Time In-

strument for Critical Information Processing and Evaluation (ANTICIPE)." https://www.act.nato.int/wp-content/uploads/2023/05/2023_Fact_Sheet_EiE_STJU23_ANTICIPE.pdf

NATO Allied Command Transformation. "Artificial Intelligence Front End Learning Information Execution (AI FELIX)." https://www.act.nato.int/wp-content/uploads/2023/05/2019_ai-felix.pdf

NATO Allied Command Transformation. "Innovation." https://www.act.nato.int/our-work/innovation/

NATO STO release on ANTICIPE: https://www.youtube.com/watch?v=A2ZAHrT3UwM

NATOTERM. "The Official NATO Terminology Database." https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en

Odermatt, Andre. *MOSA Systems: The Benefits of Deploying a Datacentric Architecture.* https://militaryembedded.com/unmanned/payloads/mosa-systems-the-benefits-of-deploying-a-datacentric-architecture

Office of the Judge Advocate General. National Defence of Canada. *The Law of Armed Conflict at the Operational and Tactical Levels* (1992) sec. 5 para. 27.

Poitras, Ryan. "Article 36 Weapons Reviews & Autonomous Weapon Systems:

Prosecutor v. Galić, Case No. IT-98-29-T, Judgment (International Criminal Tribunal for the former Yugoslavia Dec. 5, 2003) at para. 58.

Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). art. 36 (adopted 8 June 1977, entered into force 7 December 1978).

Sauer, Frank. *ICRAC Statement on Technical Issues to the 2014 UN CCW Expert Meeting.* ICRAC Int'l Comm. for Robot Arms Control (May 14, 2014). https://www.icrac.net/icrac-statement-on-technical-issues-to-the-2014-un-ccw-expert-meeting/

Schmitt, Michael N., Charles H. B. Garraway, and Yoram Dinstein. *The Manual on the Law of Non-International Armed Conflict with Commentary* 23 (2006).

Skitka, Linda J, Kathleen L. Mosier, and Mark Burdick , 'Does Automation Bias Decision-Making?' *International Journal of Human-Computer Studies* 51, no. 5 (1999).

Soare, Simona R., Pavneet Singh, and Meia Nouwens. *Software-Defined Defence: Algorithms at War*. The International Institute for Strategic Studies (IISS) (February 2023).

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

*Summary of the NATO Artificial Intelligence Strategy*. October 2022. https://www.nato.int/cps/en/natohq/official_texts_187617.htm

Supporting an International Review Standard." *American University International Legal Review* 34, no. 2 (2018).

TERMA. "AI4DEF continues work on ethics: AI for Defence." June 3, 2024. https://ai4def.com/ai4def-continues-work-on-ethics/

Tetzlaff, Alexander H. Værtsnationsstøtte. In *Hjemmefronten, nationale operationer frem mod 2025*, edited by Esben S. Larsen and Rasmus Dahlberg. DJØF Publishing, 2004.

*The Guardian*, "'Glaring Failures' Caused US to Kill RAF Crew," UK News, October 31, 2006. https://www.theguardian.com/uk/2006/oct/31/military.iraq

Trabucco, Lena. "*The Procurement of Autonomous Weapon Systems: Implications for International Humanitarian Law*." CMS Report (2023). https://cms.polsci.ku.dk/english/publications/international-humanitarian-law-and-lethal-autonomous-weapon-systems/

Trabucco, Lena and Kevin Heller. "Beyond the Ban: Comparing the Ability of 'Killer Robots' and Human Soldiers to Comply with IHL." *46 Fletcher Forum of World Affairs* no.46 15 (2022).

Trabucco, Lena, and Zoe Stanley Lockman. "NATO's Role in Responsible AI Governance in Military Affairs." In *Oxford Handbook on AI Governance.* Oxford University Press, 2022.

United States Department of Defense. Summary of the Joint All-Domain Command and Control Strategy. March 2022. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF

US Army Capabilities Integration Center. *Robotic and Autonomous Systems Strategy* (March 2017). https://mronline.org/wp-content/uploads/2018/02/RAS_Strategy.pdf

US Department of Defense Directive. 3000.09. "Autonomy in Weapon Systems." January 25, 2023. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf

Wilkins, David. E., and Roberto V. Desimone. "Applying an AI Planner to Military Operations Planning." *SRI International*, Technical Note No. 534 (1993).

Williams, Huw. "SitaWare Gains AI-Powered Intelligence, Decision Support Tools." *Janes*, January 11, 2022. https://www.janes.com/osint-insights/defence-news/defence/sitaware-gains-ai-powered-intelligence-decision-support-tools

Wilson, Clay. "Network Centric Operations: Background and Oversight Issues for Congress." *Congressional Research Service* Report R32411 (March 2007). https://sgp.fas.org/crs/natsec/RL32411.pdf

With, A.M. "Hybride maritime trusler." In *Hjemmefronten, nationale operationer frem mod 2025*, Esben S. Larsen and Rasmus Dahlberg (eds). DJØF Publishing, 2024.

## ABOUT THE AUTHORS

Lena Trabucco is a Nonresidential Research Fellow at the Stockton Center for International Law at the US Naval War College and a Research Fellow at the Center for Technology, Law, and Security at American University Washington College of Law

Esben Salling Larsen is a Military Analyst at the Royal Danish Defence College.