Jeppe T. Jacobsen

MILITÆR AI

Amerikanske erfaringer, danske muligheder

DJØF FORLAG
I SAMARBEJDE MED
CENTER FOR MILITÆRE STUDIER

Militær AI

Amerikanske erfaringer, danske muligheder

Jeppe T. Jacobsen

Militær AI

Amerikanske erfaringer, danske muligheder

Djøf forlag
i samarbejde med
Center for Militære Studier
2025

Jeppe T. Jacobsen
Militær AI
– Amerikanske erfaringer, danske muligheder

Publikationen er fagfællebedømt

Omslag: Kelly Chigozie K. Arazu

Print: Ecograf

Printed in Denmark 2025

ISBN 978-87-574-6465-8

Djøf Forlag
Gothersgade 137
1123 København K

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

Redaktørens forord

Denne udgivelsesrække indeholder ny forskning om forsvars- og sikkerhedspolitiske emner, som er relevante for især danske beslutningstagere og den danske offentlighed.

Udgivelsesrækken viderefører de studier, der hidtil har været udgivet som CMS-rapporter. Den udgør dermed en væsentlig del af Center for Militære Studiers forskningsbaserede myndighedsbetjening for Forsvarsministeriet og de politiske partier bag forsvarsforliget. Center for Militære Studier er omfattet af Københavns Universitets retningslinjer for forskningsbaseret myndighedsbetjening, herunder forskningsfrihed og armslængdeprincippet. Analyserne er udført uafhængigt og er ikke udtryk for holdninger hos den danske regering, det danske forsvar eller andre myndigheder.

Rapporterne fokuserer på at tilvejebringe akademisk holdbar og anvendelsesorienteret viden. Udgivelsesrækkens analyser har gennemgået ekstern fagfællebedømmelse, og alle analyser afsluttes med anbefalinger til danske beslutningstagere. Det er mit håb, at vi med disse udgivelser både kan informere og styrke dansk politikformulering såvel som den demokratiske debat om forsvars- og sikkerhedspolitik i Danmark.

Center for Militære Studier er et forskningscenter på Institut for Statskundskab, Københavns Universitet. På centret forskes der i sikkerheds- og forsvarspolitik samt militær strategi. Læs mere om centret, dets aktiviteter og andre udgivelser på: https://cms.polsci.ku.dk/.

København, marts 2025
Katja Lindskov Jacobsen

Indholdsfortegnelse

Oversigt over figurer og tabeller

Figurer

Tabel

Resumé og anbefalinger

I NATO's multidomænevision anses kunstig intelligens (AI) for at være løsningen på de analyse- og beslutningsudfordringer, der følger af den enorme mængde data, som indsamles og deles. Rapporten undersøger, hvordan militære organisationer kan gøre sig klar til en kampplads, hvor AI er med hele vejen – fra drift til beslutningsstøtte og ultimativt til engagement af mål. Rapporten ser på den praktiske anvendelse af AI, som har fundet sted i regi af det amerikanske forsvar og amerikanske forsvarsvirksomheder. Den lader herefter disse erfaringer fungere som bagtæppe for en praksisnær og handlingsanvisende diskussion af det danske forsvars muligheder for integration af AI. Rapporten afdækker indledningsvist tre kategorier og syv gængse udfordringer for integration af militær AI. Eksempler fra USA viser, hvordan strategisk prioritering kombineret med en eksperimentel tilgang ude i enhederne samt en balancering mellem ansvarlig AI og anerkendelse af behovet for risikovillighed har fremmet evnen til at håndtere og overvinde de dominerende udfordringer ved militær AI. Det danske forsvar har accepteret en virkelighed, hvor AI er en uundgåelig del af den militære organisation og operation, men er kun sporadisk og langsomt ved at tilpasse sig. Der mangler ikke blot specialiseret viden og oversættelseskompetencer i organisationen, men også en klar strategisk retning, et opgør med tunge indkøbsprocedurer og en systematisk udnyttelse af de særlige styrkepositioner, som især danske softwarevirksomheder og den danske forskningsverden har tilegnet sig på det militære AI-område. Rapporten kommer med seks anbefalinger, der berører strategiudvikling, eksperimentering, uddannelse, offentlig-privat samarbejde, Ukrainestøtten og international positionering. De anbefalede indsatser kan hjælpe Forsvaret med at få gavn af militær AI og derved følge med den teknologiske udvikling, de alliancemæssige forventninger og det ændrede trusselsbillede.

Anbefaling 1 – Strategi: Det er afgørende, at Forsvarsministeriet i den kommende militære AI-strategi a) eksplicit afdækker de danske krav til ansvarlig militær AI og b) fastholder det strategiske fokus med en ambitiøs implementeringsplan, der indeholder:

i. En governancestruktur med fokus på vidensdeling og tilsyn
ii. Opbygning af et test-, evaluerings-, verificerings- og valideringsregime (TEVV) med realtidsmonitorering og løbende brugerfeedback
iii. En strømlinet proces for implementering af AI-produkter gennem hele indkøbs- og implementeringsforløbet med fokus på håndtering af risici
iv. Opdyrkning af et ansvarligt AI-økosystem i industrien og forskningsverdenen.

Anbefaling 2 – Eksperimenter: Uafhængigt af det igangværende strategiarbejde bør Forsvarsministeriet tilskynde underliggende myndigheder til at igangsætte konkrete projekter (eksperimenter) med AI-løsninger i den praktiske opgaveløsning, især i forbindelse med optimeringen af driftsfunktionerne, og gerne i samarbejde med virksomheder og vidensinstitutioner. Det kræver dog samtidig:

i. At der afsættes en pulje, som de underliggende myndigheder kan søge til igangsættelsen af sådanne projekter – gerne i samarbejde med industrien og forskningsverdenen
ii. Igangsættelsen af en systematisk afdækning af muligheder for undtagelser til eller opdatering af eksisterende udbuds-, indkøbs-, kontrakt- og klassificeringsprocedurer
iii. Etableringen af en proces for systematisk erfaringsindhentning fra de igangsatte projekter, der kan inspirere de videre strategiudviklingsprocesser.

Anbefaling 3 – Uddannelse: Forsvarskommandoen (FKO) bør oprette AI-officersfunktioner hos de underliggende myndigheder og sikre tilstrækkelig uddannelse og kapacitetsopbygning på tværs af organisationen, eventuelt gennem innovative uddannelsessamarbejder mellem Forsvarsakademiet og det eksisterende teknologiske vidensmiljø i Danmark.

Anbefaling 4 – Samarbejde: Givet tilbageholdenheden i forbindelse med at tilføje ekstra administrative årsværk, tage politiske risici og gentænke armslængdeprincippet bør Forsvarsministeriet, FKO og Forsvarsministeriets Materiel- og Indkøbsstyrelse (FMI) etablere nye partnerskabsmodeller med industrien og forskningsverdenen, der er forankret uden for Forsvarsministeriets koncern, og samtidig sikre, at:

i. Sikkerhedsgodkendelse af forskere og medarbejdere i virksomheder aktivt prioriteres
ii. Kontraktrammer, der balancerer muligheden for kommercialisering af AI-modeller med Forsvarets behov for at eje AI-algoritmerne, der er udviklet på baggrund af egne data, afklares
iii. De nye partnerskabsmodeller tilføres tilstrækkelige økonomiske midler.

Anbefaling 5 – Ukrainestøtten: Forsvarsministeriet bør dedikere en separat indsats i regi af Ukrainestøtten til AI-udvikling og innovation, der får i opdrag at koble danske AI-virksomheder, danske AI-forskere og Forsvaret med de tilsvarende ukrainske aktører med henblik på konkret, operativ problemløsning på slagmarken samt hjemtagning og videreudvikling af AI-løsningerne, så de lever op til NATO's krav til ansvarlig AI.

Anbefaling 6 – Internationalt: Forsvarsministeriet og FKO bør prioritere en dansk indsats for udvikling af internationale standarder for et robust test-, evaluerings-, verificerings- og valideringsregime i tæt samarbejde med danske virksomheder og vidensinstitutioner og eventuelt i regi af NORDEFCO eller PESCO. Det ville understøtte det danske udenrigs- og sikkerhedspolitiske selvbillede som en ansvarlig småstat – også inden for militær AI.

Abstract and Recommendations

In NATO's multi-domain vision, artificial intelligence (AI) is seen as the solution to the analysis and decision-making challenges arising from the enormous amount of data that is collected and shared. The report examines how military organisations can prepare for a battlefield where AI is present all the way – from administration to decision support and ultimately to target engagement. This is done by looking at the practical application of AI that has taken place under the auspices of the US Defense and American defence companies. The report then uses these experiences as a backdrop for a practical and actionable discussion of the Danish Defence's opportunities for integrating AI. The report initially identifies three categories and seven common challenges for integrating military AI. Examples from the US show how strategic prioritisation combined with an experimental approach in units, as well as a balance between responsible AI and recognising the need for risk-taking, has promoted the ability to handle and overcome the dominant challenges of military AI. The Danish Defence has accepted a reality where AI is an inevitable part of the military organisation and operations, but it is only sporadically and slowly adapting. Not only does the organisation lack specialised knowledge and technology translation skills, but there is also a need for clear strategic direction, a re-evaluation of the cumbersome acquisition procedures, and a systematic exploitation of the special positions of strength that notably Danish software companies and the research community have acquired in the area of military AI. The report offers six recommendations that touch on strategy development, experimentation, education, public-private cooperation, support for Ukraine, and international positioning. The recommended efforts can help the Danish Defence benefit from military AI and thereby keep up with technological developments, alliance expectations, and the changing threat landscape.

Recommendation 1 – Strategy: It is crucial that the Ministry of Defence in the upcoming military AI strategy a) explicitly identifies the Danish requirements for responsible military AI and b) maintains the strategic focus with an ambitious implementation plan that includes:

IV. A governance structure with focus on knowledge-sharing and oversight
V. Building a test, evaluation, verification, and validation (TEVV) regime with real-time monitoring and ongoing user feedback
VI. A streamlined process for implementing AI products throughout the entire procurement and implementation process with focus on managing risks
VII. Cultivating a responsible AI ecosystem in industry and the research community.

Recommendation 2 – Experiments: Independently of the ongoing development of an AI strategy, the Ministry of Defence should encourage subordinate authorities to initiate concrete AI projects (experiments) that solve practical issues, especially regarding the optimisation of operational functions, preferably in collaboration with companies and knowledge institutions. However, this also requires:

I. That a pool is set aside for subordinate authorities to apply for funding to initiate such projects – preferably in collaboration with industry and the research community
II. The Ministry to initiate a systematic identification of the possibilities for exceptions to, or updates of, existing procurement, contract, and classification procedures
III. The establishment of a process for systematically gathering experience from the initiated projects that can inspire further strategy development processes.

Recommendation 3 – Education: The Defence Command should establish AI officer functions within the underlying authorities and ensure sufficient education and capacity building across the organisation, possibly through innovative educational collaboration between the Royal Danish Defence College and the existing technological knowledge environment in Denmark.

Recommendation 4 – Collaboration: Given the reluctance to provide additional administrative resources, take political risks, and rethink acquisition rules, the Ministry of Defence, the Defence Command, and the Danish Ministry of Defence Acquisition and Logistics Organisation should establish new partnership models with industry and the research community anchored outside the Ministry of Defence and, at the same time, ensure that:

I. Security clearances of researchers and employees in companies are actively prioritised
II. Contract frameworks that balance the possibility of commercialisation of AI models with the Danish Defence's need to own the AI algorithms developed from its own data are clarified
III. The new partnership models are given sufficient financial resources.

Recommendation 5 – The Ukraine Support: The Ministry of Defence should dedicate a separate initiative under the auspices of the Ukraine Support for AI development and innovation tasked with linking Danish AI companies, Danish AI researchers, and the Danish Armed Forces with Ukrainian AI companies, AI-research community, and military with a view to solving specific operational problems on the battlefield as well as to further development of AI solutions in a Danish context to meet NATO requirements for responsible AI.

Recommendation 6 – Internationally: The Ministry of Defence and the Defence Command should prioritise a Danish effort to develop international standards for a robust testing, evaluation, verification, and validation regime in close cooperation with Danish companies and knowledge institutions – possibly under the auspices of NORDEFCO or PESCO. This would support the Danish foreign and security policy self-image of acting as a responsible small state – also within military AI.

TAK

Stor tak til den anonyme bedømmer for det grundige og konstruktive arbejde. Også tak til de CMS-medarbejdere, der tog sig tid til at kommentere, samt ikke mindst til min hårde kerne af AI-sparringspartnere Iben Yde, Andreas I. Graae, Rune Pilgaard Nielsen og Daniel Møller Ølgaard for ikke bare at støtte og kritisere gennem hele processen, men frem for alt for de utallige diskussioner om alle de mange svære spørgsmål, der knytter sig til militær anvendelse af AI. En helt speciel tak til Morten Kromann – rapporten er dedikeret til dig.

1

Indledning

En russisk kampvogn springer i luften i det østlige Ukraine. Forud for affyringen af det amerikanskproducerede Javelin-missil har der været en lang beslutningskæde med inddragelse af AI hele vejen. Det er automatiserede, AI-understøttede analyser af alle tilgængelige datakilder, der sender en advarsel til den ukrainske militæroperatør om en sandsynlig samling af fjendtlige styrker i området. Det er en assisterende AI-chatbot, der foreslår at få en MQ-9 Reaper-drone i nærheden til at indsamle ekstra videomateriale for at verificere truslen. Det er chatbotten, der opstiller tre handlingsmuligheder, som lægges til grund for en militær beslutningstagers beslutning om at deployere et hold, der skal neutralisere kampvognen med et Javelin-missil. Det er en automatiseret, AI-baseret terrænanalysemodel, baseret på geospatial data og viden om det deployerede holds sammensætning, der foreslår en optimal rute mod målet. Det er AI, der bruges til at identificere og validere fjendens kommunikationsnoder og parre disse med tilgængelige jamming-kapabiliteter. Og endelig er det AI-chatbotten, der opsummerer operationsplanen og sender den til godkendelse. Kort sagt: AI er en uundværlig og uundgåelig del af moderne krigsførelse.

Det er i hvert fald det, som en af verdens førende softwarevirksomheder, Palantir Technologies, forsøger at sælge i virksomhedens demonstrationsvideo for dets Artificial Intelligence Platform (AIP) for Defense, hvori ovenstående fiktive scenarie præsenteres.[1] Budskabet flugter med CEO Alex Karps udtalelser om, at Palantir Technologies er ansvarlig

1. Palantir, 'Palantir AIP – Defense and Military', YouTube, 25. april 2023, https://www.youtube.com/watch?v=XEM5qz__HOU.

for størstedelen af den måludpegning, der finder sted i Ukraine.[2] Og det taler ind i NATO's strategiske multidomænevision, hvor AI er helt afgørende for at få analyseret de enorme mængder af data, som et voksende netværk af sensorer på tværs af de militære værn indsamler og deler. Uden AI, ingen informationsdominans og beslutningsoverlegenhed på kampladsen.[3]

Danmark abonnerer også på NATO's multidomænevision, bedst illustreret ved daværende forsvarschef Flemming Lentfer, der i 2021 udtalte, at han så et behov for "servere før kampfly".[4] Men skal multidomænevisionen omsættes til faktisk integration af militær AI, kræver det, at Forsvaret har organisationen på plads. AI-systemer er nemlig ikke som andre systemer, der blot kan indkøbes, implementeres og indsættes i drift. De er i konstant udvikling og kræver derfor konstant test og evaluering. Hvad enten Forsvaret vælger at købe de nyeste AI-systemer fra udlandet eller udvikle dem selv, eventuelt i samarbejde med danske virksomheder, kommer militær AI kun til at virke, hvis Forsvaret er en datadrevet organisation. Det betyder, som denne rapport argumenterer for, at Forsvaret skal have bedre styr på sin data, løbende skal tage stilling til efterlevelsen af krav og standarder for ansvarlig brug af AI og skal opbygge tillid til og viden om den operative anvendelse af AI.[5] Ingen af delene er i tilstrækkelig grad tilfældet i dag.

Selvom AI kan lyde som den simple og naturlige løsning på udfordringerne med at håndtere den store mængde data, der indsamles, er det langtfra ligetil at gøre organisationen klar til militær AI. Mens størstedelen af den offentlige opmærksomhed, når det gælder militær AI, er rettet mod enten dræberrobotapokalypser eller teknooptimistiske utopier, har forskellige fagdiscipliner fra politik, jura og organisationsstudier til tekniske og militæroperative discipliner hver især påpeget en lang række praktiske udfordringer forbundet med udvikling, implementering og

2. Jeffrey Dastin, 'Ukraine Is Using Palantir's Software for "targeting," CEO Says', *Reuters*, 2. februar 2023, https://www.reuters.com/technology/ukraine-is-using-palantirs-software-targeting-ceo-says-2023-02-02/.
3. Iben Yde, 'Introduktion', i *Smart Krig: Militær Anvendelse Af Kunstig Intelligens*, red. Iben Yde et al. (Djøf Forlag, 2021), 6.
4. Andreas I. Graae, 'Servers Before Tanks? Defence AI in Denmark', i *The Very Long Game – 25 Case Studies on the Global State of Defence AI*, red. Heiko Borchert et al. (Springer, 2024), 177-178.
5. I denne rapport refererer AI primært til maskinlæring. Se næste afsnit.

drift af AI-systemer.[6] Der mangler dog et samlet overblik over disse udfordringer og – ikke mindst – et indblik i, hvordan hver af disse udfordringer i øjeblikket håndteres og overvindes. For militær AI er allerede i brug på kampladsen.

Ukraines AI-understøttede Saker Scout-droner har efter sigende helt autonomt identificeret og destrueret russiske kampvogne i et jammet operationsmiljø.[7] Mens sådanne historier stadig er omgærdet med megen spekulation, har det amerikanske forsvar delt en del information om dets brug af AI, når det skal identificere potentielle militære mål i Mellemøsten og Østukraine ud fra store mængder af indsamlet data.[8] Det amerikanske flyvevåben har samtidig detaljeret beskrevet, at det har udviklet og er i gang med at implementere ubemandede, bevæbnede kampfly, der ved hjælp af AI kan følge og støtte et bemandet kampfly.[9] Og det amerikanske forsvar har bekræftet, at man gør brug af AI-modeller, når man skal identificere og udbedre sårbarheder i organisationens it-systemer, eller når man søger at optimere interne logistikkæder og vedligeholdelsesprocedurer.[10] Samtidig har flere amerikanske AI-virksomheder gjort deres softwaremodeller tilgængelige for det ukrainske forsvar, der fx har udnyttet disse til at identificere russiske soldater som mål for enten kinetiske angreb eller informationsoperationer.[11]

6. Peter Svenmarck et al., 'Possibilities and Challenges for Artificial Intelligence in Military Applications' (NATO Big Data and Artificial Intelligence for Military Decision Making – Specialists' Meeting, Bordeaux, 2018), 1-15; Jon R. Lindsay, 'War Is from Mars, AI Is from Venus: Rediscovering the Institutional Context of Military Automation', *Texas National Security Review* 7, nr. 1 (2023): 30-47.
7. David Hambling, 'Ukraine's AI Drones Seek And Attack Russian Forces Without Human Oversight', *Forbes*, 17. oktober, 2023, https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/; Stacie L. Pettyjohn, 'Drones are Transforming the Battlefield in Ukraine But in an Evolutionary Fashion', *War on the Rocks*, 5. marts 2024, https://warontherocks.com/2024/03/drones-are-transforming-the-battlefield-in-ukraine-but-in-an-evolutionary-fashion/.
8. Anthony King, 'Digital Targeting: Artificial Intelligence, Data, and Military Intelligence', *Journal of Global Security Studies* 9, nr. 2 (2024): 1-16.
9. Andreas I. Graae og Hans Peter H. Michelsen, 'F-35, Skyborgs og den kommende sværm: Kunstig intelligens i våbensystemer', i *Smart krig: Militær anvendelse af kunstig intelligens*, red. Iben Yde, et al. (Djøf Forlag, 2021).
10. Kelley M. Sayler, *Artificial Intelligence and National Security*, Congressional Research Service Report (Congressional Research Service, 2020), 11.
11. Vera Bergengruen, 'How Tech Giants Turned Ukraine Into an AI War Lab', *TIME,* 8. februar 2024, https://time.com/6691662/ai-ukraine-war-palantir/.

Denne rapport beskæftiger sig med den praktiske anvendelse af militær AI og den organisatoriske tilpasning, der har muliggjort denne anvendelse. Mere præcist svarer rapporten på, *hvordan militær AI har fundet anvendelse i det amerikanske forsvar og hos de amerikanske virksomheder, der har stillet AI-modeller til rådighed på kamppladsen i Ukraine, herunder ikke mindst hvordan disse aktører har håndteret de gængse udfordringer, der ofte tilskrives militær AI*. Rapporten forsøger at trække generelle læringspunkter ud fra de amerikanske erfaringer med henblik på, hvor det er muligt at lade dem fungere som inspiration, når andre landes forsvar – herunder specifikt det danske forsvar – skal forsøge at følge med den teknologiske udvikling, de alliancemæssige forventninger og det ændrede trusselsbillede.

Det amerikanske forsvar, den amerikanske forsvarsindustri og amerikansk kommerciel softwareudvikling er unikke, hvad angår både omfang, økonomisk kapacitet og sociokulturel forankring. Alene i perioden august 2022 til august 2023 afsatte det amerikanske forsvarsministerium (DoD) 557 millioner dollars til AI-relaterede kontrakter.[12] Og sammenholdt med, at DoD ved indkøb af AI-systemer har formået at omgå de generelt tunge udbudsprocedurer, har det resulteret i, at USA naturligt nok er længst fremme i udviklingen og implementeringen af militær AI. Den brede vifte af AI-projekter og den relative åbenhed med hensyn til disse betyder, at USA trods sin unikke position udgør en brugbar illustration af de mange forskellige måder, hvormed AI kan bidrage i militære organisationer, samt ikke mindst af de nødvendige afvejninger, som må adresseres af ethvert land, der ønsker at implementere militær AI.

Selvfølgelig er de forsvarspolitiske, forsvarsøkonomiske og forsvarsorganisatoriske forskelle mellem USA og Danmark enorme. USA er en strategisk *first mover* drevet af en frygt for at sakke bagud i det geostrategiske og militære teknologikapløb, mens Danmark historisk har været en *second* eller *third mover*, primært drevet af at sikre NATO-alliancen og relationen til USA med en minimal økonomisk investering.[13] Siden Ruslands invasion af Ukraine i 2022 har Danmark imidlertid åbnet op

12. Will Henshall, 'The U.S. Military's Investments Into Artificial Intelligence Are Skyrocketing', *TIME*, 3. marts 2024, https://time.com/6961317/ai-artificial-intelligence-us-military-spending/.
13. Jeppe T. Jacobsen og Katrine Nørgaard, 'Reading Security Imaginaries as Fantasies – Loss, Desire, and Enjoyment in the Military Quest for Explainable AI', *Millennium: Journal of*

for en større økonomisk revitalisering af Forsvaret, ligesom Forsvaret har knyttet behovet for en strategisk omorganisering til NATO's krav om alliancemæssig interoperabilitet i et fremtidigt multidomænemiljø og den dertilhørende nødvendige orientering mod en datadrevet militær organisation.[14] Skal disse strategiske tilkendegivelser omsættes, så Danmark lever op til NATO's AI-strategi, som man politisk allerede har forpligtet sig til at implementere, kan Danmark med fordel forsøge at identificere de relevante læringspunkter fra de amerikanske operative og organisatoriske erfaringer – selvfølgelig tilpasset de unikke forhold og begrænsninger, der gør sig gældende for Danmark.

På den måde er rapporten et forsøg på med praksisnære og handlingsanvisende anbefalinger at understøtte den allerede vedtagne forsvarspolitiske vision om at få indarbejdet AI i Forsvarets organisation og derved kunne bidrage til et interoperabelt multidomænemiljø i NATO-regi. Rapporten tager derfor ikke et kritisk-teoretisk udgangspunkt med henblik på at afdække de bredere problematikker omkring militær-industrielle komplekser, magt- og sociopolitiske implikationer eller de underliggende myter og fantasier, der knytter sig til udviklingen og promovering af militær AI.[15] Det betyder langtfra, at sådanne perspektiver ikke er vigtige for de bredere politiske drøftelser af, hvilken rolle militær AI kan og bør spille i fremtiden. Det er de bestemt. Men det er en anden og sideløbende diskussion end rapportens ambition om at afdække det organisatoriske og strategiske mulighedsrum, der lige nu eksisterer for at udmønte den nuværende politiske vision om at få AI integreret i det danske forsvar.

International Studies 52, nr. 2 (2024): 408-433; Peter Viggo Jakobsen og Steen Rynning, 'Denmark: Happy to fight, will travel', *International Affairs* 95, nr. 4 (2019): 877-895.

14. Andreas I. Graae, 'Servers Before Tanks?', 177-178.
15. For en sådan afdækning, se Jacobsen og Nørgaard, 'Reading Security Imaginaries as Fantasies'; Erik Reichborn-Kjennerud, 'Krig i en verden av fremmed intelligens', i *Digitalisering og internasjonal politikk*, red. Håkon Bergsjø og Karsten Friis (Scandinavian University Press, 2022), 192-212; Raluca Csernatoni og Bruno Oliveira Martins, 'Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination', *Geopolitics* 29, nr. 3 (2024): 849-872; Ingvild Bode og Hendrik Huelss, 'Constructing expertise: the front- and back-door regulation of AI's military applications in the European Union', *Journal of European Public Policy* 30, nr. 7 (2023): 1230-1254; Lucy Suchman, 'Imaginaries of omniscience: Automating intelligence in the US Department of Defense', *Social Studies of Science* 53, nr. 5 (2022): 761-786.

Metodisk bygger rapporten på den ene side på den eksisterende litteratur, der – på tværs af relevante fagdiscipliner – har identificeret de mest gængse anvendelsesformer og praktiske udfordringer i forbindelse med implementeringen af militær AI. På den anden side bygger rapporten på en række amerikanske casestudier, heriblandt "Skyborg", Clearview AI, "Project Maven", "Project Voltron" og C3 AI. Casene er udvalgt på grund af deres respektive evne til at illustrere, hvordan de gængse udfordringer kan overvindes. Og de er udvalgt, fordi de alle har været genstand for en bredere dækning i medierne og forskningsverdenen, hvorfor rapportens empiriske grundlag ikke blot er DoD's eller virksomhedernes anbefalinger. Rapporten belyser dog kun i mindre grad de fejlskud og mindre succesfulde AI-projekter, som DoD har søsat. Det betyder ikke, at vigtige læringspunkter ikke ekstrapoleres fra fejlskud. Tværtimod. De mange fejlskud har været centrale for de succesfulde AI-eksempler, som rapporten præsenterer. Og når rapporten vender sig mod en *second mover* som Danmark, er det antagelsen, at læringspunkterne fra den mere succesfulde amerikanske udvikling, implementering og anvendelse af AI kan hjælpe Danmark med at undgå de begynderfejl, som en *first mover* nødvendigvis oplever. Overførslen af amerikanske læringspunkter til danske muligheder vil dog i rapportens diskussion være tilpasset det faktum, at den danske økonomiske og organisatoriske kapacitet er lille, samt at den kulturelle kontekst for så vidt angår villigheden til at innovere og relationen til den private sektor er fundamentalt forskellig fra den amerikanske.

Rapporten er delt op i tre kapitler. Første kapitel identificerer på baggrund af den eksisterende litteratur først de gængse udfordringer i forbindelse med udvikling og implementering af militær AI og derefter de mest almindelige anvendelsesformer. Sidstnævnte inddeles i tre kategorier – AI som henholdsvis våbensystemer, beslutningsstøtte og drift – ud fra hvilke udfordringerne vægtes og vurderes. I det andet kapitel analyserer rapporten de amerikanske cases. I kapitlet struktureres analysen gennem de tre kategorier med henblik på at afdække, hvordan udfordringerne i praksis er blevet imødegået. Kapitlet afsluttes med at uddrage to modsatrettede dynamikker, som ethvert forsvar, der søger at implementere AI, bør søge at balancere: 1) langsigtet strategiudvikling versus kortsigtede projekteksperimenter og 2) risikovillighed versus ansvarlighed. Med udgangspunkt i det danske forsvars nuværende strategiske pejlemærker og organisation diskuterer rapporten i tredje kapitel disse læringspunkter

med henblik på at identificere områder, der med fordel kan prioriteres, hvis Danmark vil leve op til NATO's krav og forventninger med hensyn til militær AI. Rapporten afsluttes med en konklusion og anbefalinger.

2

Militær AI: Afgrænsning og inddeling

Det første kapitel er inddelt i to. Først defineres og introduceres AI og de centrale begreber og diskussioner, der ofte knytter sig til fænomenet. Herefter oplistes syv centrale udfordringer, som bør adresseres, hvis et land ønsker at udvikle og implementere militær AI. Det sidste afsnit vender sig mod den militære anvendelse af AI og introducerer tre kategorier, hvorigennem militær AI og dens udfordringer kan forstås og analyseres. Afsnittet illustrerer vigtigheden af en mere nuanceret forståelse af militær AI. Når det danske forsvar skal vælge strategisk retning og prioritere sine indsatser, er det vigtigt at have sig for øje, hvor man hurtigere, nemmere og mere uproblematisk kan gøre erfaringer med AI, og hvor grundigere og mere langsigtede afklaringer er nødvendige, før initiativer sættes i søen.

2.1. Definitioner

'AI' defineres i denne rapport som den digitale eller kunstige reproduktion af kognitive egenskaber, der tidligere var forbeholdt mennesker.[16] Sagt på en anden måde er AI computersystemer, der er i stand til at udføre opgaver, som normalt anses for at kræve menneskelig intelligens

16. Anders Theis Bollmann og Katja Lindskov Jacobsen, 'Militær dataoversættelse og digital transformation: Erfaringer fra Ukraine og fokuspunkter for det danske forsvar', CMS Rapport (Djøf Forlag, 2023), 34.

at løse. Ofte inddeles AI i '*generel AI*' – den endnu ikke opnåede fulde reproduktion af menneskelig kognition – og '*smal AI*', som beskæftiger sig med en mere snæver opgaveløsning, der normalt kun kræver én form for intelligens. Sidstnævnte, oftest i form af *maskinlæring*, er genstand for alle de AI-modeller, der anvendes i dag, og vil derfor udgøre rapportens omdrejningspunkt.[17] Det betyder også, at den primære opmærksomhed gennem hele rapporten vil være på automatiseringen af (analysen af og læringen fra) data- og informationsprocesser. I tillæg til de tre typer af maskinlæring, som er nævnt i boksen nedenfor, har maskinlæring flere anvendelsesformer, fx *computer vision* til mønster- og ansigtsgenkendelse og *generativ AI* til tekst-, billed-, og videogenerering. Åbningsscenen i rapportens introduktion illustrerer brugen af *computer vision* i forbindelse med identifikationen af en fjendtlig enhed og generativ AI i forbindelse med udarbejdelsen af handlingsmuligheder og en operationsplan.

Både den militære og den civile anvendelse af AI er muliggjort af en markant stigning i mængden af data, af den generelle regnekraft samt af brugen af *cloud computing* og nye, kraftfulde mobile netværk.[18] Men selvom disse udviklinger har skabt enormt mange muligheder for anvendelse af maskinlæring til problemløsning, er der stadig mange udfordringer og begrænsninger forbundet med teknologien – nogle generelle og andre med særlig betydning for den militære organisation (og operation).

Maskinlæring

'Maskinlæring' (*machine learning*) handler om at få en computer til at lære på baggrund af data. 'Læring' betyder her, at der ud fra datainput og ved hjælp af algoritmer og statistiske metoder laves forudsigelser og på det grundlag eventuelt tages beslutninger. Maskinlæring opdeles ofte i tre typer:

17. Nogle AI-eksperter ser neurale netværk som noget fundamentalt anderledes end maskinlæring, hovedsageligt på grund af det mindre behov for menneskelig indblanding. Da denne rapport imidlertid introducerer maskinlæring som et paraplybegreb for de algoritmer og modeller, der lærer at lave forudsigelser ud fra data, vil dybe neurale netværk blive kategoriseret som en type maskinlæring.
18. Jens Ulrik Hansen, 'En Introduktion til kunstig intelligens og maskinlæring', i *Smart Krig: Militær anvendelse af kunstig intelligens*, red. Iben Yde et al. (Djøf Forlag, 2021), 14.

Ved *superviseret læring* er modellen trænet på klassificeret data, fx billeder, hvorpå man har markeret en kampvogn. Superviseret læring bruges ofte til at forudsige priser, eller hvad et billede forestiller.

Ved *ikkesuperviseret læring* finder modellen mønstre i data uden forudgående information om, hvad der ønskes klassificeret eller forudsagt. Ikkesuperviseret læring bruges ofte til at gruppere kunder, levere anbefalinger eller identificere afvigende adfærd.

Ved *reinforcement-læring* lærer modellen at tage beslutninger efter forsøg-og-fejl-metoden, hvor der modtages feedback fra omgivelserne i form at belønning eller straf. Reinforcement-læring bruges ofte til spil.

Maskinlæring er også tæt knyttet til begrebet 'neurale netværk', som er inspireret af neuronforbindelser i den menneskelige hjerne. Neurale netværk er en kompleks og datatung teknik, der oftest anvendes til superviserede læringsproblemer (men kan dog også bruges til ikkesuperviseret læring og reinforcement-læring), og som har vist sig succesfuld til især billed- og sprogbehandling.

2.2. Generelle udfordringer

1) Dataudfordringen. Den nok mest grundlæggende udfordring for maskinlæring generelt er *data* og nærmere bestemt data af den rette type, kvalitet og mængde. Som nævnt ovenfor er data i konteksten af maskinlæring hele grundlaget for at kunne skabe en algoritme, der kan lave forudsigelser. Det er kort sagt data, der producerer algoritmen, *ikke* programmørens "hvis X, så Y"-regler. Således er en forudsætning for udviklingen af en AI-model ikke blot, at man formår at formulere et praktisk problem på en måde, som en AI-algoritme kan løse. En forudsætning er også, at man kan skaffe den rette data til at træne – det vil sige udvikle – den algoritme eller model, man ønsker.[19] Det kræver fx, at man har adgang til en stor mængde billeder, som ligner de billeder, man i fremtiden forventer at skulle have identificeret. Det nytter ikke noget at træne AI-algoritmer på højresolutionsbilleder af kampvogne i en ørken i Mellemøsten, hvis algoritmerne skal bruges til at identificere

19. Hansen, 37.

kampvogne ud fra dårlige mobilkamerafotos i en østukrainsk skov. Vanskeligheder ved at producere relevant data i en militær kontekst betyder, at modeller og algoritmer ofte trænes på syntetisk data fra simulationer og øvelsesscenarier, hvilket kræver ekstra opmærksomhed på og tid til at adressere de forskelle, der uundgåeligt eksisterer, når algoritmerne møder den virkelige verden. Og selv hvis store, virkelighedsnære datamængder er tilgængelige – som det især er tilfældet for store techvirksomheder – kan historisk data ofte indeholde, hvad man i dag ville identificere som uhensigtsmæssige bias, hvilket en AI-algoritme, uden indgriben, blot vil reproducere. Derfor er sikring af en tilstrækkelig høj datakvalitet, hvor data efter systematisk indsamling – gerne på tværs af organisationen – skal klargøres, renses (herunder ofte annoteres af mennesker) samt løbende testes før, under og efter, at algoritmen møder virkeligheden, den nok mest omfattende proces i udviklingen af AI-modeller.[20] Det gælder både i den civile verden og i en militær kontekst.

I en militær kontekst vedrører dataudfordringen også i særlig grad spørgsmålet om dataejerskab. Militære AI-algoritmer trænes oftest på klassificeret data, og de ændres (og bør evalueres), når de sættes i anvendelse i politisk og operativt sensitive miljøer, fx i en konfliktsituation. Det stiller store krav til dataopbevaringen og datasikkerheden i den militære organisation, enten når den overdrager data til en cloud administreret af store teknologivirksomheder, eller når den giver AI-virksomheder adgang til en statslig cloud, så de kan udvikle (og drifte) AI-algoritmer på baggrund af relevant data. Det er dog stadig ofte forbundet med en del juridisk uklarhed, hvem der ejer data i clouden og kan få adgang til den: staten; virksomheden; staten, hvori datacentret er placeret; eller staten, hvorfra virksomheden stammer.[21]

Selv med en høj datakvalitet og -kontrol er en AI-model stadig afhængig af mennesker til at beslutte, hvad der skal forudsiges, hvorfor, og hvad forudsigelsen skal bruges til.[22] I den militære organisation kan

20. Husanjot Chahal, Ryan Fedasiuk og Carrick Flynn, 'Messier than Oil: Assessing Data Advantage in Military AI', CSET Issue Brief (Center for Security and Emerging Technology, 2020), 5-6.
21. Jeppe T. Jacobsen og Tobias Liebetrau, 'Big tech at war: The infrastructural politics of public-private relations', *European Journal of International Relations* (under udgivelse).
22. Avi Goldfarb og Jon R. Lindsay, 'Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War', *International Security* 46, nr. 3 (2022): 22.

sådanne beslutninger spænde bredt – fra dagligdagens drift og administration til beslutninger om liv og død på kampladsen. Alvoren af de yderste konsekvenser ved den militære profession gør, at militære beslutningstagere i højere grad ønsker at forstå AI-modellernes forudsigelser, før de selv beslutter eller lader AI-modellen beslutte, hvad der skal ske.[23] Men forklarbarhed er i udgangspunktet vanskelig for AI-modeller. Især neurale netværk har ofte karakter af *sorte bokse*, hvor man putter data ind i den ene ende, og får data ud i den anden uden at vide, hvad der skete indimellem. Den direkte sammenhæng mellem algoritmens nøjagtighed og graden af uforklarbarhed medfører flere udfordringer for militær anvendelse af AI.

2) Forklarbarhed som folkeretsudfordring. I folkeretlig forstand er sorte bokse ikke eksplicit ulovlige, så længe AI-systemet bedst muligt sikrer efterlevelsen af de relevante regler.[24] Dog peger folkeretsjurister på et indirekte krav om, at brugerne forstår et (AI-baseret) våbensystems muligheder og begrænsninger, herunder fx i forbindelse med udøvelsen af menneskelig kontrol ved udpegning og engagering af mål samt i forbindelse med lovpligtige våbenscreeninger.[25] Det folkeretlige behov for inddragelse af menneskelig kontrol og dømmekraft skyldes ikke blot, at AI-modeller endnu ikke er tilstrækkelig sofistikerede til at foretage de påkrævede kontekstspecifikke distinktions- og proportionalitetsvurderinger. Det skyldes også, at *ansvarsplaceringen*, når uheld sker, vanskeliggøres med uforklarbare AI-modeller.[26] Det folkeretlige svar på disse udfordringer er flere. Det kræver først og fremmest et øget test- og evalueringsregime, så AI-modellernes pålidelighed overstiger konventionelle

23. U.S. DoD, 'Summary of the 2018 Department of Defense Artificial Intelligence Strategy – Harnessing AI to Advance Our Security and Prosperity' (U.S. Department of Defense, 2018); Alejandro Barredo Arrieta et al., 'Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI', *Information Fusion* 58 (2020): 84; Arthur Holland Michel, 'The Black Box, Unlocked: Predictability and Understandability in Military AI', Report (United Nations Institute for Disarmament Research, 2020).
24. Iben Yde, 'Sorte bokse, kontroltab og ansvarsflugt: Folkeretten og militær anvendelse af kunstig intelligens.' i *Smart krig: Militær anvendelse af kunstig intelligens*, red. Iben Yde et al. (Djøf Forlag, 2021), 183.
25. Vincent Boulanin et al., 'Limits of Autonomy in Weapon Systems – Identifying Practical Elements of Human Control', SIPRI-ICRC Report (Stockholm International Peace Research Institute, 2020).
26. Rebecca Crootof, 'War Torts: Accountability for Autonomous Weapons', *University of Pennsylvania Law Review* 164, nr. 6 (2016): 1347-1402.

våbensystemers.[27] Men det kræver også nye standarder for AI-modellernes forklarbarhed, øget uddannelse og teknisk forståelse hos brugerne samt ikke mindst et behov for en politisk afklaring af, hvor høj grad af forståelse der kræves, før det er acceptabelt at anvende AI-baserede våbensystemer.[28]

3) Forklarbarhed som en operativ tillidsudfordring. Fra et militæroperativt perspektiv knytter AI-modellernes manglende forklarbarhed sig til en anden udfordring, nemlig til de militære beslutningstageres *tillid* til de teknologier, der tages i anvendelse, og derfor grundlæggende til spørgsmålet om, hvorvidt et AI-baseret system overhovedet vil blive brugt. Tillid til våben- eller beslutningsstøttesystemer opbygges oftest ved den succesfulde brug af disse systemer over tid. Med andre ord skal de testes – ikke bare i simulationer men også gerne i faktiske konfliktsituationer. Men føler militære beslutningstagere, at den specifikke konfliktsituation, de står i, ikke ligner tidligere situationer, kan disse beslutningstagere med rette stille sig skeptiske over for de anbefalinger, som en AI-model kommer med.[29] AI-modeller har som nævnt vanskeligt ved at tilskrive betydning til data, der ikke ligner den data, de er trænet på baggrund af. Så selvom en AI-model leverer "objektive", sobre vurderinger, betyder det ikke, at selv den teknisk veluddannede beslutningstager er villig til at tage AI-modellens anbefalinger for pålydende – eller anerkende og overvinde egne tidligere erfaringer, personlige overbevisninger og bias, kognitive og fysiske begrænsninger eller gruppepres.[30] Skal militære AI-systemer for alvor finde anvendelse, må disse menneskelige dynamikker overvindes. Det kræver som minimum, at beslutningstageren har mulighed for at få begrundet AI-modellens anbefalinger; det vil sige, at modellen bliver bedre til at forklare sig.

27. Lena Trabucco, 'International Humanitarian Law and Lethal Autonomous Weapons Systems – Legal Considerations for Acquisition and Procurement', CMS Rapport (Djøf Forlag, 2023): 53-56.
28. Yde, 'Sorte Bokse, kontroltab og ansvarsflugt'.
29. Benjamin M. Jensen, Christopher Whyte, og Scott Cuomo, 'Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence', *International Studies Review* 22, nr., 3 (2020): 532.
30. Jeppe T. Jacobsen og Tobias Liebetrau, 'Kunstig intelligens, militærstrategi og international konkurrence', i *Smart krig: Militær anvendelse af kunstig intelligens*, red. Iben Yde et al. (Djøf Forlag, 2021), 134.

4) Den etiske udfordring. En øget mulighed for interaktion og menneskelig involvering med en mere forklarbar AI-model sænker dog uundgåeligt beslutningshastigheden sammenlignet med fuldt autonome systemer. Og da netop beslutningshastighed de sidste fyrre år har været hjørnestenen i de vestlige landes forsøg på at opnå og opretholde militær overlegenhed,[31] kan forklarbarhed og den menneskelige dømmekraft i praksis blive tilsidesat til fordel for hastighed – især hvis presset og risikovilligheden forøges. Det kan med andre ord være svært for en beslutningstager i skarpe, højspændte situationer at afvige fra de anbefalinger, som et AI-baseret beslutningsstøttesystem kommer med. Skræk-eksempler er her det israelske AI-måludpegningssystem Lavender, hvor den militære beslutningstager kun fik tyve sekunder til at verificere mål, før en bombning blev autoriseret – med mange civile dræbte i Gaza til følge.[32] Manglende tid og forståelse for systemernes logik kan føre til, at den ønskede meningsfulde menneskelige kontrol med AI-modellerne ender med at blive meningsløs.[33] Neil Renic tager skridtet videre og peger på, at AI-modeller skaber en falsk tillid, der ultimativt kultiverer en ufølsomhed over for volden og dennes tragiske effekter og dermed sandsynligvis vil føre til mere vold.[34] Denne grundlæggende *etiske udfordring* for militær anvendelse af AI i våben- og beslutningsstøttesystemer – forklarbare eller ej – er således kort sagt, at teknificeringen risikerer både at dehumanisere de mennesker, der rammes, og underminere den moralske dømmekraft hos de mennesker, der faciliterer den autonome vold.[35]

31. Jeppe T. Jacobsen og Tobias Liebetrau, 'Artificial Intelligence and Military Superiority – How the "Cyber-AI Offensive-Defensive Arms Race" Affects the US Vision of the Fully Integrated Battlefield', i *Artificial Intelligence and International Conflict in Cyberspace*, red. Fabio Cristiano et al. (Routledge, 2023), 135-156.
32. Ishaan Tharoor, 'Israel offers a glimpse into the terrifying world of military AI', *The Washington Post,* 5. april 2024, https://www.washingtonpost.com/world/2024/04/05/israel-idf-lavender-ai-militarytarget/.
33. Ingvild Bode og Tom Watts, 'Meaning-Less Human Control – Lessons from Air Defence Systems on Meaningful Human Control for the Debate on AWS', Drone Wars (Center for War Studies, SDU, 2021); Elke Schwarz, 'Autonomous Weapons Systems, Artificial Intelligence, and the Problem of Meaningful Human Control', *The Philosophical Journal of Conflict and Violence* 5, nr. 1 (2021): 53-72.
34. Neil Renic, 'Tragic Reflection, Political Wisdom, and the Future of Algorithmic War', *Australian Journal of International Affairs* 78, nr. 2 (2024): 247-256.
35. Neil Renic og Elke Schwarz, 'Crimes of Dispassion: Autonomous Weapons and the Moral Challenge of Systematic Killing', *Ethics & International Affairs* 37, nr. 3 (2023): 321-343.

5) Uddannelses- og vidensudfordringen. Både retligt, operativt og etisk er et centralt svar på udfordringerne for den militære anvendelse af AI, at de rette mennesker *uddannes* bedre. Det er også konklusionen for Bollmann og Jacobsen, der introducerer begrebet 'militær dataoversættelse' netop for at understrege nødvendigheden af at opbygge en bedre fællesforståelse civile og militære, tekniske og ikke-tekniske aktører imellem – både internt i den militære organisation og i relationen til den private sektor.[36] Selvom specifikt uddannede militære dataoversættere med viden om både teknologien og den militære operation er essentielle for at kunne overvinde de vidensudfordringer, som nye datadrevne teknologier såsom AI introducerer på kampladsen, kan dette ikke stå alene. Da det i sidste ende altid er operatøren, der skal have forståelse for, hvordan systemet vil agere i en konkret situation i et kontekstspecifikt operationsmiljø, er et generelt videns- og kompetenceløft på tværs af alle stillingskategorier i de militære organisationer nødvendig – hvad enten det drejer sig om at skulle lede, udvikle, integrere, facilitere eller bruge militær AI.[37] Udfordringen, der følger heraf, er dog et behov for en øget trænings- og uddannelsesmængde. For at undgå en degeneration af de oprindelige soldaterfærdigheder, må soldater gennemgå træning, der sikrer, at de mestrer kampen *både* assisteret af komplekse AI-systemer og konventionelt, for det tilfælde at de datadrevne systemer forstyrres som følge af jamming eller cyberangreb.[38]

6) Indkøbs- og driftsudfordringen. Øget uddannelsesbehov er dog ikke den eneste organisatoriske udfordring, som militær AI medfører. De fleste militære organisationer har indkøbsprocedurer for konventionelt materiel, der er kendetegnet ved at være langsigtede og underlagt et omfattende sæt af regler og krav. Det går sjældent godt i spænd med de hurtigt udviklende AI-modeller, som drives fremad af den private sektor.[39] For mindre startup-virksomheder kan det fx være vanskeligt at allokere ressourcer til at leve op til krav om håndtering af klassifice-

36. Bollmann og Jacobsen, 'Militær dataoversættelse og digital transformation'.
37. U.S. DoD Joint AI Center, *DoD AI Education Strategy – Cultivating an AI Ready Force to Accelerate Adoption* (U.S. Department of Defense, 2020).
38. Sarah Grand-Clément, 'Artificial Intelligence Beyond Weapons – Applications and Impact of AI in the Military Domain', UNIDIR Report (United Nations Institute for Disarmament Research, 2023).
39. Simona R. Soare, 'European Military AI: Why Regional Approaches Are Lagging Behind', i *The AI Wave in Defence Innovation – Assessing Military Artificial Intelligence Strategies,*

ret materiale eller gennemgå specielle statslige certificeringer forud for at kunne ansøge om kontrakter.[40] Sådanne krav kan selvfølgelig være nødvendige – også på AI-området, fx i forbindelse med opbygningen af en gennemgående datainfrastruktur. Men der er samtidig behov for at overveje mulighederne for at gentænke nogle af de eksisterende krav, så den tilgængelige data hurtigere kan udnyttes via innovative AI-løsninger. Selv hvis sådanne løsninger integreres i Forsvaret, kræver disse løbende tilpasning, i takt med at AI-systemerne udrulles i faktiske operative situationer. Et AI-system er derfor ikke bare en anskaffelse, der skal driftes på normal vis. Implementering af AI kræver en driftsorganisation, der er gearet til løbende tilpasninger af systemerne.

7) **Tilstedeværelse af en modstander**. Behovet for løbende tilpasning bliver især aktuelt med eksistensen af den sidste udfordring, der kan forhindre, at AI-systemer kan give værdi på slagmarken, nemlig tilstedeværelsen af en (ligeværdig) *modstander*. Aktører har en strategisk interesse i løbende at forsøge at manipulere modstanderens AI-modeller ved at føde læringsalgoritmerne med fejlagtig data eller forsøge aktivt at ændre i selve algoritmerne.[41] Det stiller krav til udviklerne af militære AI-modeller, driftsmedarbejderne samt de cybersikkerhedsspecialister, der løbende skal sikre sig, at udefrakommende aktører ikke har adgang til læringsalgoritmerne eller den data, som disse trænes på baggrund af.

Ovenstående udfordringer er dog ikke lige presserende for alle former for militær anvendelse af AI. Følgende afsnit præsenterer en kategorisering af militær AI, der ser nærmere på de militære funktioner, som AI-modeller faktisk understøtter, samt diskuterer betydningen af ovennævnte udfordringer.

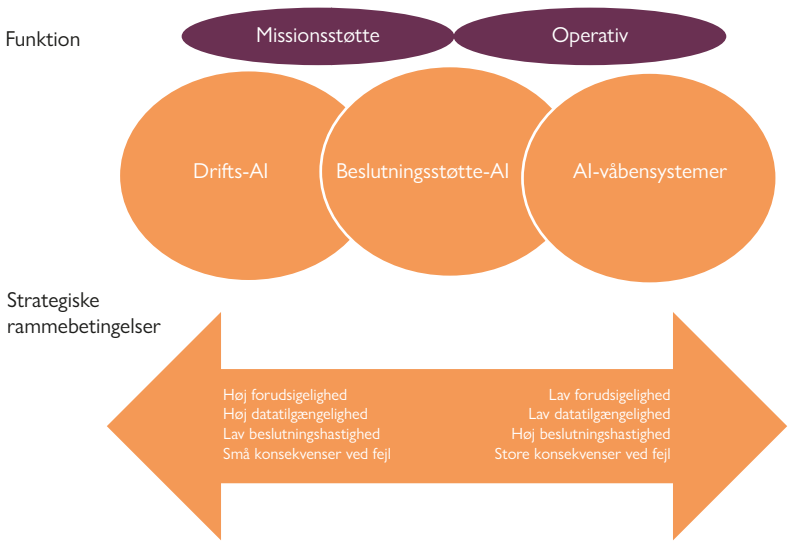
Capabilities, and Trajectories, red. Michael Raska og Richard A. Bitzinger (Routledge, 2023), 92-93.

40. Paul Scharre, *Four Battlegrounds – Power in the Age of Artificial Intelligence* (W. W. Norton & Company, 2024), 213.
41. Paul Scharre og Michael C. Horowitz, *Artificial Intelligence: What Every Policymaker Needs to Know*, The Artificial Intelligence and International Security Series (Center for New American Security, 2018), 14-15.

2.3. En kategorisering af militær AI

Den militære anvendelse af AI kan med fordel inddeles i tre overordnede kategorier, drifts-AI, beslutningsstøtte-AI og AI-våbensystemer. Kategorierne repræsenterer ikke klart afgrænsede funktioner. I stedet bør de tilgås som overlappende nedslagspunkter på et kontinuum, hvor de strategiske rammebetingelser spænder fra et miljø karakteriseret ved høj forudsigelighed og datatilgængelighed, men lav beslutningshastighed og små konsekvenser ved fejl til et miljø karakteriseret ved lav forudsigelighed og datatilgængelighed, men høj beslutningshastighed og store konsekvenser ved fejl. Figur 1 skal fungere som en forsimplet illustration af den tredelte kategorisering af AI-systemer, og hvordan disse systemer for størstedelens vedkommende placerer sig i forhold til ovennævnte kontinuum samt i forhold til distinktionen mellem missionsstøttesystemer og operative systemer. Udviklingen af AI-systemer inden for de tre kategorier er dog knyttet sammen og påvirker hinanden. Det vil sige, at nogle erfaringer med AI til én funktion ofte vil hjælpe udviklingen i en anden.

Figur 1: Illustration af den tredelte kategorisering af militær AI



Drifts-AI refererer til applikationer udviklet i et relativt kontrolleret miljø, oftest i den militære organisation, hvor data er tilgængelig, arbejdsopgaverne forudsigelige, beslutningshastigheden sjældent høj og konsekvenserne ved fejl sjældent store.[42] Sådanne opgaver inkluderer bureaukratiske funktioner som fx skemaplanlægning, rekruttering, medarbejderevaluering og budgethåndtering, men også funktioner, der skaber overblik over materielbeholdninger og vedligeholdelsesbehov, identificerer anomalier i organisationens informations- og kommunikationsnetværk samt understøtter trænings-, øvelses- og simulationsaktiviteter. Jo mere gentagende, rutineprægede og standardiserede disse driftsprocesser er, desto bedre kan en AI-model lave forudsigelser og dermed optimere funktionerne.

Da de driftsmæssige opgaver varierer, er der også stor variation i den datakvalitetsudfordring, som organisationen står over for, når den søger at få gavn af AI-modeller. Skal store mængder data i forskellige formater og fra forskellige systemer tale sammen, kræver AI-applikationerne mere arbejde at udvikle og implementere, end det er tilfældet ved mindre ambitiøse løsninger. Og det kompliceres ofte af, at organisationen sjældent har etableret en gennemgående datainfrastruktur og dataarkitektur, der systematisk indsamler og gemmer data. Datakvalitetsudfordringen vil dog alt andet lige være mere overvindelig ved drifts-AI end for AI-systemer, der også er afhængige af data, som genereres af og indsamles fra kilder uden for organisationen i et konstant foranderligt operationsmiljø.

Drifts-AI er sjældent så direkte involveret i voldshandlinger som ved autonome våbensystemer, hvorfor de folkeretlige og etiske udfordringer ikke i samme grad gør sig gældende. Selvom AI-baseret HR-, logistik-, og cybersikkerhedssystemer er vigtige for den militære kampkraft og ofte kan have indflydelse på senere voldshandlingers effektivitet, slår drifts-AI eller den beslutning, der tages på baggrund af drifts-AI-modellens forudsigelser, ikke direkte de formodede fjender ihjel. At konsekvenserne af fejl og uhensigtsmæssigheder ved brugen af drifts-AI-systemer – om end potentielt økonomisk omkostningstunge – generelt er mindre alvorlige, betyder også, at behovet for forklarbarhed ikke er så stort. Derfor har tillid også bedre vilkår. Nye teknologer vil dog altid blive mødt med

42. Danielle Tarraf et al., *The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations* (RAND Corporation, 2019), 25.

skepsis fra nogle medarbejdere, men AI-systemer, der gør trænings- og simulationsværktøjer mere realistiske, eller generative AI-modeller, der hjælper HR- eller logistikmedarbejderen med at få overblik og tage beslutninger, kan hurtigere tages i brug i et faktisk arbejdsmiljø og dermed hurtigere blive testet og forbedret. Det kræver dog stadig, at den militære organisation er villig til at lade de leverandører, der udvikler HR- og logistiksystemer, få adgang til og lov til at arbejde med den til tider sensitive medarbejder-, materiel- eller øvelsesdata, som en AI-model skal trænes på baggrund af. Eller alternativt at den militære organisation selv rekrutterer og uddanner personel, som kan udvikle drifts-AI-modeller. Med andre ord er udfordringerne med både uddannelse og indkøbsprocedurer stadig til stede ved drifts-AI. Det samme gør sig gældende for tilstedeværelsen af en modstander. Drifts-AI minder om en hvilken som helst virksomheds forsøg på at optimere processer. Men i krig er drifts-AI-modeller også mål for fjendtlige hackere, der har en strategisk interesse i at forstyrre logistikkæder, lønudbetalinger og simulationsværktøjer. Det betyder, at sårbarheden af disse systemer også er betydelig.

Den anden kategori er *beslutningsstøtte-AI.* Kategorien refererer til applikationer, som mere direkte understøtter den militære beslutningstagning i en konfliktsituation. Her vil datatilgængeligheden ofte være mere varierende, da dataindsamlingen typisk sker på slagmarken, og forudsigeligheden påvirkes af ændrede strategiske og operative mål. Beslutningsstøtte-AI knytter sig til opgaver som Intelligence, Surveillance, Reconnaissance (ISR), Target Development (TD) og Command and Control (C2). AI-udfordringerne for de forskellige typer af beslutningsstøtteopgaver er dog ikke nødvendigvis ens. Udsigten til en højere datakvalitet er fx bedre for C2-AI-modeller, da data fra venligsindede organisationer og procedurer ofte er nemmere at kontrollere og derfor producerer mere forudsigelig data.[43] Samtidig er stabsmedarbejderens arbejde med at efterspørge viden samt søge og reformatere information ofte gentagende og rutinepræget, hvilket øger muligheden for at højne datakvaliteten.

Sådanne C2-opgaver er samtidig mindre berørte af etik-, folkeretsog tillidsproblematikkerne end de beslutningsstøtte-AI-modeller, der analyserer store mængder af data fra overvågnings- og rekognoscerings-

43. Goldfarb and Lindsay, 'Prediction and Judgment', 37.

droner og foreslår mål for kinetiske angreb. Overvågningssensorer kan indsamle en eksorbitant mængde data, som en AI-baseret *computer vision*-algoritme med fordel kan hjælpe med at finde mønstre i og identificere mulige mål ud fra. Men algoritmens mere direkte forbindelse til en kinetisk voldshandling gør, at den menneskelige operatørs etiske og folkeretlige ansvar i højere grad er til debat, hvorfor operatøren – for at have tillid til algoritmen – naturligt vil efterspørge den vanskeligt opnåelige forklarbarhed. I Palantirs demonstrationsvideo fra indledningen til denne rapport forsikrer fortællerstemmen om, at man kan "kigge under kølerhjelmen" på algoritmerne for at se, hvilke datakilder forslagene bygger på. Men selv hvis en sådan brugergrænseflade, der giver operatøren reel mulighed for at undersøge nærmere, faktisk eksisterer, vil det kræve, at man har evnet at overvinde de ovennævnte videns- og uddannelsesudfordringer samt at gøre det på en måde, så der i operationsmiljøet faktisk er tid til at undersøge AI-modellens beslutningsgrundlag.

De ovennævnte udfordringer i forbindelse med indkøb, implementering og drift vil utvivlsomt ligeledes være til stede for de fleste beslutnings-AI-systemer, ligesom tilstedeværelsen af en modstander vil betyde, at der er en yderligere grund til løbende at teste og evaluere systemernes sikkerhed og funktionalitet. Dog vil mindre omfattende C2-AI-applikationer – som generative sprogmodeller og forbedrede søgefunktioner på tværs af databaser – til støtte for stabsofficerens arbejde nemmere og mere intuitivt kunne implementeres og introduceres, da datakilderne, der trækkes på, ofte er kontrolleret af organisationen.

Den tredje kategori, *AI-våbensystemer*, er de AI-applikationer, som generelt benyttes i et dynamisk, foranderligt, uforudsigeligt og delvis ukontrollerbart operationsmiljø, hvor adgang til replikerbar træningsdata samt højhastighedsinternet og cloud-løsninger kan være mere begrænset, men hvor behovet for hurtige informationsprocesser og beslutninger er stort, og konsekvenserne store.[44] AI-våbensystemsmodeller kan fx indgå i luftforsvarssystemer, integrerede maritime våbensystemer eller autonome droner.

Den operative anvendelse af AI-våbensystemer er både den mest omdiskuterede anvendelsesform og den anvendelsesform, der er karakteriseret ved de største udfordringer. Træning af en algoritme på faktisk

44. Danielle Tarraf et al., *The Department of Defense Posture for Artificial Intelligence*, 25-26.

operativ data er ikke nemt.[45] Udviklerne skal sikre sig, at systemet handler som ønsket og planlagt i en konkret situation, særligt i dynamiske operationsmiljøer, hvor der er relativt stor risiko for, at der er afvigelser fra de forhold, modellen er trænet til at kunne fungere under. Det stiller store krav til både systemforståelse og indsigt i de operative forhold og ikke mindst evnen til at kombinere de to og identificere de relevante mitigeringsbehov. Det er med andre ord vanskeligt at teste og evaluere algoritmernes pålidelighed, så de lever op til de folkeretlige forpligtelser. Sammenholdt med uklarhederne med hensyn til ansvarsplacering, etisk kritik og manglede viden og uddannelse samt en modstander med strategisk interesse i at manipulere modellerne kan både tilliden til og villigheden til at udvikle, investere i og implementere operativ AI meget vel blive svær at overvinde.

Tabel 1 opsummerer ovenstående gennemgang af de tre kategorier for anvendelse af militær AI og deres respektive udfordringer. Den illustrerer med farverne rød, gul, grøn og hvid, hvor der er henholdsvis store, mellem, små eller slet ingen udfordringer forbundet med anvendelsen af militær AI.

Tabel 1: Militære anvendelsesformer for AI og deres udfordringer

		Drifts-AI C2	Beslutningsstøtte-AI		AI-våben-systemer
			ISR + TD		
Datakvalitetsudfordring		Små	Mellem	Store	Store
Forklarbarhedsudfordring	Folkeret	Ingen	Små	Mellem	Store
	Tillid	Små	Mellem	Store	Store
Etisk udfordring		Små	Små	Store	Store
Videns- og uddannelsesudfordring		Mellem	Store	Store	Store
Indkøbs- og implementeringsudfordring		Små-mellem	Mellem	Store	Store
Udfordring ved tilstedeværelsen af en modstander		Mellem-Store	Store	Store	Store

45. Derfor produceres data til disse formål ofte syntetisk fra øvelser og scenarier, hvilket medfører en del udfordringer, som beskrevet i forrige afsnit under datakvalitetsudfordringen.

Overordnet illustrerer tabellen vigtigheden af en mere nuanceret forståelse af militær AI. Tabellen viser, at ikke alle typer af militær AI er lige vanskelige at give sig i kast med. Drifts-AI og de C2-systemer, der er afhængige af data, der indsamles og kontrolleres internt i organisationen, kan nemmere og mere uproblematisk integreres i den militære organisation – forudsat at de modeller, der udvikles af fx private virksomheder, faktisk fungerer efter hensigten. Modsat kræver AI-våbensystemer en grundigere afdækning og håndtering af de eksisterende udfordringer.

Fascinationen af de mange spændende og skræmmende visioner for især AI-våbensystemer og de store, globale investeringer i området som helhed skygger for, at der endnu ikke er særligt meget empirisk viden om, hvor militær AI faktisk er blevet taget i anvendelse. Det amerikanske forsvar er den institution, der mest åbent har delt ud af sine erfaringer – og måske særligt interessant vedrørende de mindre fascinerende driftssystemer og C2-AI-systemer. Det følgende kapitel tager udgangspunkt i tabellen og undersøger, hvordan det amerikanske forsvar og de amerikanske forsvarsvirksomheder i praksis har formået at håndtere de beskrevne udfordringer i nogle af de militære AI-applikationer, der er i anvendelse.

3

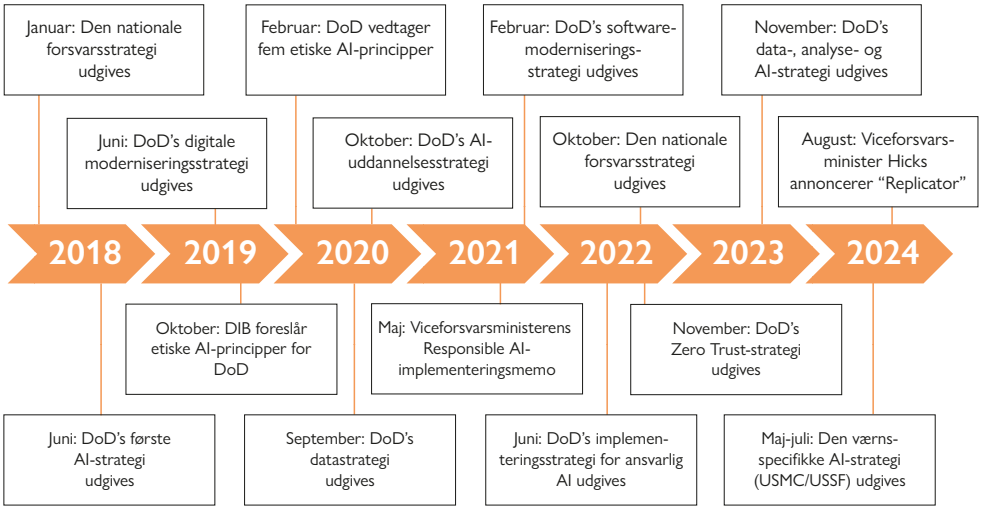
Analyse: De amerikanske erfaringer

Kapitlet starter med en kort beskrivelse af de overordnede strategier og strategiske initiativer, som det amerikanske forsvar har søsat i forsøget på at håndtere udfordringerne forbundet med militær anvendelse af AI. Herefter gennemgås de konkrete amerikanske erfaringer inden for hver af de tre kategorier. Sidst opsummeres analysen ved at opstille centrale overvejelser, som bør vægtes, hvis militær AI skal anvendes i dag. Kapitlet viser, at USA har grundlagt sin evne til delvist at integrere militær AI ved at balancere to modsatrettede dynamikker. På den ene side har man balanceret en omfattende strategisk forandring af organisationen mod et datadrevet og softwarecentrisk forsvar med en AI-strategi, der prioriterer decentrale eksperimenter i samarbejde med industrien og forskningsverdenen, og som sikrer erfaringsopsamling fra disse eksperimenter. På den anden side argumenterer kapitlet for, at evnen også er grundlagt gennem en udvikling af klare tekniske standarder for udvikling og anvendelse af militær AI, alt imens organisationen – blandt andet gennem amerikanske virksomheder engageret i Ukraine – gør sig klar til en virkelighed, hvor risikovilligheden i forbindelse med anvendelsen af militær AI ændrer sig.

3.1. USA's strategiske tilgang

Nye, disruptive teknologier, herunder AI, er i dag i stigende grad blevet et strategisk konkurrenceparameter i international politik.[46] Den amerikanske nationale forsvarsstrategi fra 2018 var det første officielle strategiske dokument, hvori disse teknologiers betydning blev eksplicit anerkendt og integreret i den strategiske tilpasning af det amerikanske forsvar.[47] Og forsvarsstrategien og den første overordnede AI-strategi, der fulgte i dens kølvand få måneder senere,[48] blev startskuddet til en hel række af mere specifikke AI-relaterede strategier og initiativer (se figur 2).

Figur 2: Tidslinje over det amerikanske forsvars AI-relaterede strategier



46. Henrik Breitenbauch og Jens Vesterlund Matthiesen, *Militærteknologisk situationsforståelse,* CMS Rapport (Djøf Forlag, 2021); Henrik Breitenbauch og Tobias Liebetrau, *Teknologikonkurrencen og dens implikationer for Danmark*, CMS Rapport (Djøf Forlag, 2021).
47. U.S. DoD, 'Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's competitive edge' (U.S. Department of Defense, 2018).
48. U.S. DoD, 'The 2018 Department of the Defense Artificial Intelligence Strategy'.

Den omfattende mængde af strategiske dokumenter – illustreret i figuren – og den praktiske udmøntning af disse i forskellige initiativer vidner om det amerikanske forsvars prioriteringer i forsøget på at håndtere udfordringerne med udvikling, implementering og anvendelse af militær AI. Tre forhold springer i øjnene. Det første er den markante prioritering af datakvalitet og dataejerskab – eller nærmere bestemt fundamentet for at kunne sikre den nødvendige datakvalitet på tværs af hele koncernen. Den digitale moderniseringsstrategi fra 2019,[49] datastrategien fra 2020,[50] softwaremoderniseringsstrategien fra 2021[51] og Zero Trust-strategien fra 2022[52] har alle fokus på at sikre en øget indsamling og ensretning af håndtering af data, specifikt med det overordnede mål, at hele det amerikanske forsvar skal være en datadrevet og softwarebaseret organisation. Med andre ord skal det amerikanske forsvar fundamentalt transformeres fra et hardwarecentrisk til et softwarecentrisk forsvar med en grundlæggende dataarkitektur, hvor alle dele af organisationen indsamler og håndterer data på en måde, der er interoperabel, og som sikrer skalerbarhed.[53]

Det andet, der springer i øjnene, er det gennemgående fokus på behovet for tillid til AI-applikationer i de strategiske dokumenter, der mere eksplicit adresserer AI-udfordringer – mest udtalt DoD's etiske principper[54] og den efterfølgende implementeringsstrategi for ansvarlig AI fra 2022[55] og endeligt konsolideret i Præsident Bidens præsidentielle AI-dekret fra 2023.[56] Skal AI-applikationer faktisk tages i anvendelse, kræver det, at slutbrugeren har tillid til, at de virker efter hensigten – og her er

49. U.S. DoD, 'DoD Digital Modernization Strategy' (U.S. Department of Defense, 2019).
50. U.S. DoD, 'DoD Data Strategy: Unleashing Data to Advance the National Defense Strategy' (U.S. Department of Defense, 2020).
51. U.S. DoD, 'Department of Defense Software Modernization Strategy' (U.S. Department of Defense, 2021).
52. U.S. DoD, 'DoD Zero Trust Strategy' (U.S. Department of Defense, 2022).
53. Nand Mulchandani og John N.T. "Jack" Shanahan, *Software-Defined Warfare – Architecting the DoD's Transition to the Digital Age*, CSIS Rapport (Center for Strategic and International Studies, 2022).
54. U.S. DoD, 'DOD Adopts Ethical Principles for Artificial Intelligence', pressemeddelelse, 24. februar 2020, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.
55. U.S. DoD, 'U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway', (U.S. Department of Defense, 2022).
56. Joesph R. Biden Jr., 'Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence', præsidentielt dekret, 30. oktober 2023.

ansvarlighed nøgleordet. Ansvarlig AI stiller krav til design, udvikling og brug af samt tilsyn med AI-applikationer. En hjørnesten er et test- og evalueringsregime. Inden for autonome våbensystemer har DoD allerede med sit direktiv 3000.09 fra 2023 udviklet en grundig proces for test og evaluering.[57] Men i tillæg hertil er det også vigtigt, at slutbrugeren får mulighed for hurtigt at få en applikation mellem hænderne og i forbindelse med fx øvelser levere feedback til softwareingeniøren og derved opnå den nødvendige tillid til AI-modellens funktionalitet og værdi.[58] Med andre ord balancerer DoD's implementering af AI mellem på den ene side et centraliseret regime af regler for ansvarlig AI og på den anden side et decentralt udviklingsregime, der har fokus på eksperimenter og hurtig udrulning af testbare applikationer til slutbrugerne.

For det tredje vidner en sammenligning af de to overordnede AI-strategi-dokumenter fra henholdsvis 2018 og 2023 både om en udvikling og om de fortsatte udfordringer med militær AI. På den ene side er den bredere datatransformation og den specifikke dataanalyse og softwareudvikling smeltet mere sammen i den seneste strategi. Det understreger en mere moden organisation, hvor implementeringen af strategiens delmål nødvendigvis skal ske med øje for de eksisterende erfaringer med både de centraliserede, datatransformative elementer og udviklingen og skaleringen af de decentrale AI-eksperimenter, der allerede nu søger at levere en effekt tættere på enhederne. Dette dobbelte fokus understreges også ved den organisatoriske transition fra en forankring af AI-udvikling i det amerikanske forsvar i Joint Artificial Intelligence Center (JAIC) til det bredere og mere dataorienterede Chief Digital and Artificial Intelligence Office (CDAO).[59] På den anden side gentager strategierne de fortsatte udfordringer med at opbygge den rette AI-kapable arbejdsstyrke samt det rette udviklings- og indkøbsøkosystem, hvor forskningsverdenens og

57. Kathleen H. Hicks, '(DoD) Directive 3000.09, Autonomy in Weapon Systems' (Office of the Under Secretary of Defense for Policy, 2023).
58. U.S. DoD, *U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway*, 18; CSIS, 'Scaling AI-enabled Capabilities at the DOD: Government and Industry Perspectives', transskribering fra event (28. marts 2024), https://www.csis.org/analysis/scaling-ai-enabled-capabilities-dod-government-and-industry-perspectives.
59. Lauren Kahn og Michael C. Horowitz, 'Two Cheers for the Department of Defense's New Data and Artificial Intelligence Leadership Initiative', *CFR Blog*, 1. december 2021, https://www.cfr.org/blog/two-cheers-department-defenses-new-data-and-artificial-intelligence-leadership-initiative.

den private sektors kompetencer udnyttes. U.S. Government Accountability Office (GAO) har også påpeget begge disse udfordringer, og kontoret har foreslået yderligere handling fra Pentagons side, hvad angår udfordringerne.[60] Og det uafhængige Defense Innovation Board (DIB), der rådgiver DoD om integrationen af nye, innovative, disruptive teknologier, og som fx var hovedarkitekt bag implementeringen af etiske AI-principper, har ligeledes udgivet en række anbefalinger til, hvordan DoD får gjort op med den såkaldte "Valley of Death", så succesfulde pilot- og udviklingsprojekter bedre overlever den lange vej mod faktisk indkøb og implementering i det amerikanske forsvar.[61] Således har det amerikanske forsvar både illustreret vigtigheden af og muligheden for at gå på to ben – et centralt, datatransformativt og et decentralt, AI-eksperimenterende – og understreget vigtigheden af at have udefrakommende rådgivningsorganer, der kan anvise vejen hen imod et succesfuldt samarbejde mellem forsvaret, forskningsverdenen og den private sektor.

Det amerikanske forsvar har dog formået succesfuldt at implementere flere AI-systemer i dets organisation, hvor både forskningsverdenen og den private sektor har spillet centrale roller. De følgende casestudier fortæller, hvordan evnen til at integrere AI-systemer blev opnået.

3.2. Drifts-AI

GAO udgav i 2018 en hård kritik af cybersikkerhedsniveauet i de missionskritiske systemer i det amerikanske forsvar.[62] Rapporten vurderede, at våbensystemer for en værdi af 1,6 billioner dollars var udsatte, hvilket potentielt kunne føre til, at USA ikke længere kunne gennemføre mili-

60. GAO, *Artificial Intelligence: DOD Needs Department-wide Guidance to Inform Acquisition*, Rapport til Senatets komite for de væbnede styrker (U.S. Government Accountability Office, 2023); GAO, *Artificial Intelligence: Actions Needed to Improve DOD's Workforce Management*, Rapport til Repræsentanternes Hus' komite for de væbnede styrker (U.S. Government Accountability Office, 2023).
61. Defense Innovation Board, *Terraforming the Valley: Making the Defense Market Navigable for Startups*, DIB-rapport (Defense Innovation Board, 2023), https://innovation.defense.gov/Portals/63/DIB_Terraforming%20the%20Valley%20of%20Death_230717_1.pdf.
62. GAO, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities,* Rapport til Senatets komite for de væbnede styrker (U.S. Government Accountability Office, 2018).

tære missioner, og at amerikanske liv kunne gå tabt.[63] Det amerikanske forsvar havde taget de indledende spadestik til at håndtere problemet – ved hjælp af AI. Og evnen til netop at udnytte AI til at forbedre cybersikkerheden illustrerer også, hvad USA gjorde for at overvinde indkøbs- og implementeringsudfordringen. To år inden GAO's kritik havde det amerikanske forsvars forskningsagentur, DARPA, forsøgt at tilskynde virksomheder og universiteter til at udvikle et autonomt system til opsporing og udbedring af it-sårbarheder.[64] Tilskyndelsen havde form af en konkurrence, the Cyber Grand Challenge. Vinderen, virksomheden ForAllSecure,[65] vandt 2 millioner dollars og tiltrak sig stor opmærksomhed. Alt imens Pentagon var tilbageholdende med at udrulle systemet, stod Forsvarsministeriets eksperimentende satellitenhed i Silicon Valley, the Defense Innovation Unit (DIU), klar med en kontrakt, allerede 26 dage efter at enheden havde opslået et åbent udbud – rettet mod ForAllSecures system – om et automatiseret system, der kunne identificere endnu ikke rapporterede it-sårbarheder.[66] DIU, der har fået i opdrag at bringe de nyeste kommercielle teknologier ind i forsvaret, kortsluttede de tunge indkøbsprocedurer gennem en genfortolkning af en undtagelse for prototypeteknologier i den amerikanske forsvarslov.[67] Projektet fik navnet "Voltron", og AI-løsningen er i dag succesfuldt udrullet i mange af det amerikanske forsvars mest kritiske systemer.

En anden illustration af, at DIU har formået at overvinde indkøbs- og implementeringsudfordringen, er samarbejdet med softwarevirksomheden C3 AI om AI-løsninger i forbindelse med vedligeholdelse af det amerikanske forsvars materiel. På seks måneder leverede C3 AI en prototype til en forudsigende vedligeholdelsesalgoritme, der førte til en 30 % reduktion i det uforudsete vedligeholdelsesbehov for de to flytyper, som systemet blev testet på.[68] Resultatet blev først en udrulning til over 1.200 fly i det amerikanske forsvar, hvilket inkluderede F-16, F-35 samt

63. Scharre, *Four Battlegroups,* 195.
64. Jeppe T. Jacobsen og Dennis Hansen, 'Cyber- og informationssikkerhed: AI som løsning eller trussel?', i *Smart krig: Militær anvendelse af kunstig intelligens*, red. Iben Yde et al. (Djøf Forlag, 2021), 152.
65. ForAllSecure har nu skiftet navn til Mayhem.
66. Scharre, *Four Battlegroups,* 195.
67. John Dobriansky og Patrick O'Farrell, 'Other Transaction Authority: Acquisition Innovation for Mission-Critical Force Readiness', *Contract Management,* juli 2018.
68. Scharre, *Four Battlegrounds,* 196.

hærens Apache- og BLACK HAWK-helikoptere, og derefter yderligere opprioritering af forudsigende vedligeholdelse for hærens og marinekorpsets køretøjer samt for flådens skibe. En lignende vedligeholdelseshistorie er U.S. Army Material Command's Logistic Support Activitys aftale med IBM Watson i 2017, hvor de efter succesfuld implementering af en AI-baseret vedligeholdelseskalender for pansrede mandskabsvogne videreudviklede samarbejdet til også at lade IBM Watson optimere transporten af reservedele.[69] Med en årlig vedligeholdelsesomkostning på 280 milliarder dollars i det amerikansk forsvar er der mange penge at hente ved en optimering af vedligeholdelsesregimet, ligesom forbedret vedligeholdelse kan resultere i en større procentdel af konstant missionsparate køretøjer, fly og skibe.[70] C3 AI vurderer selv, at virksomhedens forudsigende vedligeholdelsesværktøj i det amerikanske luftvåben har øget missionskapaciteten med 6 %.[71]

Casene illustrerer to overordnede pointer. For det første viser både "Voltron" og C3 AI vigtigheden af at være organisatorisk tæt på den kommercielle teknologiske udvikling samt have mod til at tilpasse lovgrundlaget for indkøb af nyt materiel til en virkelighed, der kræver øget hastighed. Og for det andet viser især vedligeholdelsescasene, at de mindre kontroversielle drifts-AI-algoritmer med fordel kan udvikles gennem en eksperimentel tilgang, hvor der startes i det små – det vil sige med få enheder i et enkelt værn – og først skaleres enten i dybden eller i bredden, når klare gevinster kan demonstreres. Samtidig har denne tilgang øget den gensidige forståelse mellem det amerikanske forsvar og de amerikanske AI-virksomheder, hvilket har ført til yderligere samarbejder om flere andre typer af AI-applikationer. C3 AI indgik fx en aftale med Missile Defense Agency om en AI-platform til optimering og evaluering af missilforsvarssystemernes effektivitet.[72]

69. Lauren A. Kahn, 'Risky Incrementalism: Defense AI in the United States', Rapport Defense AI Observatory (juli 2023), 38.
70. Scharre, *Four Battlegrounds*, 196-197.
71. C3 AI, 'C3 AI Readiness for Aircraft Livestream', Webinar (13. maj 2020), https://c3.ai/live/c3-ai-readiness-for-aircraft/.
72. C3 AI, 'C3 AI Awarded Three New Orders from Missile Defense Agency', 13. december 2022, https://c3.ai/c3-ai-awarded-three-new-orders-from-missile-defense-agency/.

3.3. Beslutningsstøtte-AI

"Project Maven" er nok det mest kendte og veldokumenterede AI-projekt i det amerikanske forsvar. "Maven"s historie byder på mange vigtige læringspunkter for udvikling og implementering af militære AI-systemer både til beslutningsstøtte og i bredere forstand – og den illustrerer mere specifikt, hvordan det amerikanske forsvar overvandt de gængse udfordringer med datakvalitet, etik og indkøbs- og implementeringsprocedurer. Trods modstand fra store dele af Pentagon blev "Maven" søsat i april 2017 som et resultat af den daværende viceforsvarsminister Bob Works ønske om en AI-succeshistorie, der kunne understøtte hans vision om endnu en såkaldt *offset strategy*, som ved hjælp af militærteknologisk innovation inden for autonomi og AI skulle sikre fortsat militær overlegenhed i forhold til Kina og Rusland.[73] Work fandt med "Maven" et projekt, der ville løse et faktisk problem for de operative enheder, nemlig den uovervindelige mængde videomateriale, der konstant blev indsamlet fra de ISR-droner, som fløj rundt for at identificere bilbomber i Irak og Afghanistan. Og han kombinerede dette med en AI-teknologi, der faktisk var tilgængelig, nemlig maskinlæring, til *computer vision*.[74] I Works opdrag til "Maven" pålagde han en 90-dages deadline for integration af en algoritmebaseret teknologi, og selvom det tog små otte måneder at få et automatiseret videoanalyseværktøj deployeret til militære efterretningsenheder til støtte i kampen mod Islamisk Stat i Irak og Syrien, var det stadig langt hurtigere end de syv-ti år, der udgør den almindelige indkøbs- og implementeringshorisont i det amerikanske forsvar.[75]

Deployeringen havde krævet en del nytænkning. Vigtigst krævede den en anerkendelse af, at "Maven" ikke selv kunne udvikle AI-algoritmen. Med denne anerkendelse kom behovet for at afklassificere videomateriale, så en privat virksomhed kunne stå for den nødvendige billedkategorisering til forberedelse af maskinlæringsalgoritmen. Og det førte til en succesfuld udvidelse af AI-test- og evalueringsteamet, så det i tillæg til hærens og flyvevåbnets forskningslaboratorier også inkluderede Johns Hopkins University Applied Physics Laboratory og kommercielle virk-

73. Jacobsen og Nørgaard, 'Reading Security Imaginaries as Fantasies', 16.
74. Scharre, *Four Battlegrounds*, 55-56.
75. Ibid., 57-58.

somheder med erfaring med at gøre AI-modeller klar til brug og løbende evaluere dem.[76] I tillæg til disse tiltag krævede algoritmen også optimering og raffinering i dagene efter deployering for at håndtere forskellene mellem træningsdata og virkelig data – en optimering, der imidlertid aldrig fik algoritmens præcision op over 60 %.[77] Deployeringen af "Maven" understregede en central pointe om anvendelsen af militær AI, nemlig at algoritmerne altid skal gentænkes, når de møder den operative virkelighed, og at dette faktum kræver nytænkning af organisation, anskaffelse og drift, således at disse er gearet til løbende tilpasning, test og evaluering. Denne tilpasningsevne – mere end algoritmens middelmådige præstation – gjorde, at "Maven" blev set og præsenteret som en succes, og projektet blev efterfølgende udvidet med henblik på at inkorporere data fra flere kilder. Senere blev erfaringerne fra "Maven" endda integreret i et center under DoD, JAIC, og "Maven" endte i 2023 med at blive formelt godkendt som et dedikeret indkøbsprogram under DoD og driftsoverført til National Geospatial-Intelligence Agency.[78] Men det skete først, efter at "Maven" havde været i modvind på grund af en af de store private partnere involveret i projektet, nemlig Google.

I foråret 2018 underskrev 3.000 Google-ansatte et åbent brev, der fordømte Googles samarbejde med militæret. Sagen fik stor offentlig opmærksomhed, men hverken DoD eller ledelsen i Google valgte at imødegå protesterne eller den udbredte misforståelse, at "Maven" var ved at udvikle sig til et program for dræberrobotter.[79] Da flere ansatte sagde op i protest, valgte Google at lade være med at forny kontrakten med DoD.[80] Kontroversen fik dog flere uventede positive implikationer for

76. National Academies of Sciences, Engineering, and Medicine, *Test and Evaluation Challenges in Artificial Intelligence-Enabled Systems for the Department of the Air Force*, Consensus Study Report (The National Academies Press, 2023), 31.
77. Marcus Weisgerber, 'The Pentagon's New Artificial Intelligence Is Already Hunting Terrorists', *Defence One*, 21. december 2017, https://www.defenseone.com/technology/2017/12/pentagons-new-artificial-intelligence-already-hunting-terrorists/144742/.
78. Det betyder dog ikke, at "Maven" ikke fortsat oplever udfordringer og problemer – men i dag er dette primært knyttet til evnen til at opfylde den store efterspørgsel efter produktet, se Sydney J. Freedberg Jr., "'Success begets challenges': NGA struggles to meet rising demand for Maven AI", *Breaking Defence*, 3. september 2024, https://breakingdefense.com/2024/09/success-begets-challenges-nga-struggles-to-meet-rising-demand-for-maven-ai/.
79. Isobel Asher Hamilton, 'A former Google engineer warned that robot weapons could cause accidental mass killings', *Business Insider*, 16. september, 2019, https://www.businessinsider.com/former-google-engineer-warns-against-killer-robots-2019-9.
80. Scharre, *Four Battlegrounds*, 60.

DoD's implementering af militær AI. Kontroversen blev for det første et wakeupcall for DoD-ledelsen, ikke blot om vigtigheden af AI generelt, men også om, at misforståelser i relationen til den private sektor kunne påvirke forsvarets strategiske kapacitetsudvikling. Udviklingen af etiske standarder – i tråd med DIB's anbefalinger – måtte derfor nødvendigvis gøres til omdrejningspunkt for den videre AI-udvikling.[81] For det andet stod Palantir Technologies klar til at overtage Googles kontrakt og har siden formået at udvikle – med XVIII Airborne Corps som det primære testmiljø – et så effektivt og deployerbart analysesoftware, at virksomheden i 2024 sikrede sig en kontrakt på 480 millioner dollars til udvikling af den seneste generation af "Maven", hærens "Maven Smart System".[82]

Netop XVIII Airborne Corps viste sig at blive en central aktør i forbindelse med den amerikanske støtte til Ukraine i landets kamp mod Rusland – som Anthony King viser, i store træk takket være "Maven" og Palantir. Da Ukrainekrigen brød ud i februar 2022, overgik træningsmissionen "Security Assistance Group – Ukraine" i Wiesbaden, Tyskland, blandt andet til at levere beslutningsstøtte til det ukrainske forsvar. XVIII Airborne Corps blev deployeret for at sikre denne transition.[83] Som testenhed for "Maven" og Palantir havde XVIII Airborne Corps allerede omfavnet en datadrevet tilgang til indhentning, analyse, måludpegning og militær beslutningstagning i kampen mod Islamisk Stat. Og ved at tilpasse sit software til kampen i Ukraine formåede Palantir og XVIII Airborne Corps at sammenkøre open source, klassificeret data og satellitdata, så det ukrainske forsvar kunne få hjælp til hurtigt at lokalisere og destruere russiske enheder.[84] Og partnerskabet mellem Palantir og XVIII Airborne Corps har ikke blot været succesfuldt som et resultat af, at 30 russiske officerer og en række kommandoposter efter signede blev tilintetgjort som følge af samarbejdet. Det har også været succesfuldt, fordi samarbejdsaftalen ekspliciterede, at Palantir har kunnet kommer-

81. Zoe Stanley-Lockman, 'US governance of AI for National Security', i *The AI Wave in Defence Innovation – Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*, red. Michael Raska og Richard A. Bitzinger (Routledge, 2023), 127, 129.
82. Joe Saballa, 'Palantir Awarded $480M to Prototype US Army's "Maven" AI Battlefield Analyzer', *The Defense Post*, 24. maj, 2024, https://www.thedefensepost.com/2024/05/30/palantir-maven-battlefield-analyzer/?utm_content=cmp-true.
83. King, 'Digital Targeting', 11.
84. Ibid.

cialisere AI-systemer, mens de algoritmer, der var udviklet ud fra amerikansk forsvarsdata, fortsat ejes af det amerikanske forsvar.

Kombinationen af den fordelagtige mulighed for at videreudvikle AI-systemer udviklet i samarbejde med DoD samt Ukrainekrigens muligheder for at teste det i en krig har positioneret Palantir som en af verdens førende (og mest profitable) udviklere af militær AI og især af AI til beslutningsstøttesystemer. Uafhængigt af det ovennævnte samarbejde inden for rammen af "Maven" har Palantir således forbedret sine AI-systemer ved at levere dem til Ukraine gratis – systemer, der ikke blot er blevet brugt til at give Ukraine billeder af kampplads en i tæt på realtid, men også til indsamling af beviser på krigsforbrydelser, til støtte for minerydning og til genbosættelse af internt fordrevne.[85] Og som rapportens åbningsscene understreger, fortsætter Palantir med at udvikle sit måludpegnings- og beslutningsstøttesoftware.

Palantirs strategi fra Ukraine har inspireret andre amerikanske AI-virksomheder. Scale AI, der oprindeligt leverede kategoriseret data til støtte for selvkørende biler, begyndte kort efter invasionen at indsamle billeder af ødelagte ukrainske byer med henblik på at udvikle en algoritme til identificering og vurdering af skader i realtid, som virksomheden kunne dele med det ukrainske forsvar.[86] Og den kontroversielle ansigtsgenkendelsesvirksomhed Clearview AI, der få år tidligere var blevet mødt med hård kritik for at bryde privatlivslovgivninger i USA og Europa, så Ukrainekrigen som en mulighed for at genopfinde sig selv. I lyset af krigen har virksomheden således udviklet og delt et AI-ansigtsgenkendelsesværktøj, som Ukraine har brugt til at identificere 230.000 russiske soldater, der blandt andet er blevet gjort til mål for informationsoperationer.[87] Disse eksempler på en kommerciel udvikling af AI til støtte for militære beslutninger er dog kun muliggjort af, at USA i forvejen har haft en spirende teknologisk startup-sektor, som har udnyttet,

85. Bergengruen, 'How Tech Giants Turned Ukraine Into an AI War Lab'.
86. Patrick Tucker, 'How AI Could Predict the Damage to Ukraine from Russian Missiles'. *Defense One*, 9. januar 2023, https://www.defenseone.com/technology/2023/01/how-ai-could-predict-damage-ukraine-russian-missiles/381633/.
87. Vera Bergengruen, 'Ukraine's "Secret Weapon" Against Russia Is a Controversial U.S. Tech Company', *TIME*, 14. november 2023, https://time.com/6334176/ukraine-clearview-ai-russia/; Jean-Marc Rickli og Federico Mantellassi, *The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare*, Geneva Paper 34/24 (Geneva Centre for Security Policy, 2024), 22.

at risikovilligheden for implementering af nye, amerikanske AI-systemer var stor i Ukraine. Selvom risikovilligheden fortsat er stor, er Ukraine dog begyndt at kræve, at algoritmerne, der udvikles på baggrund af data fra krigen, forbliver på ukrainske hænder, fordi landet har anerkendt den kommercielle konkurrencefordel ved software, der er *proven in combat*.[88]

Overordnet set bidrager historien om "Maven", Palantir og kommercialiseringen af militær AI i USA efter Ukrainekrigen med flere læringspunkter om udviklingen af militær beslutningsstøtte-AI. For det første vidner "Maven" om, at tidlige AI-pilotprojekter for at overleve både skal have den rette institutionelle rygdækning og skal adressere konkrete militæroperative udfordringer. For det andet peger "Maven" – ligesom drifts-AI-eksemplerne – på, at udfordringerne ved lange udviklings-, indkøbs- og implementeringsprocedurer kan overvindes, men at det kræver, at data i højere grad afklassificeres, og ikke mindst at virksomheder og forskningsinstitutioner inddrages i de vedvarende udviklings-, test- og evalueringsfaser.[89] Og for det tredje understreger casen, at AI-projekter ikke blot skal kommunikeres overbevisende internt inden for rammen af den strategiske konkurrence, men også at projekterne med fordel bør tale til og udvikles med fokus på de etiske bekymringer og kommercielle muligheder, som eksisterer hos de private partnere, der er nødvendige for at udvikle AI-systemer. I forlængelse af sidstnævnte vidner den kommercielle udvikling af AI i konteksten af Ukrainekrigen om, at beslutningsstøtte-AI for alvor finder praktisk anvendelse, når risikovilligheden til at gøre brug af ny og uprøvet teknologi er stor. Der er således en forskel på en situation karakteriseret ved ikkevæbnet konflikt, hvor etiske standarder og grundige test- og evalueringsregimer dominerer, og væbnet konflikt, hvor der er større vilje og folkeretligt råderum til at deployere AI-systemer, der i fredstid ville have været for kontroversielle, umodne eller underlagt andre regler. Mens dette ikke er overraskende, understreger det behovet for nødvendigheden af – før en krig bryder ud – strategisk at prioritere opdyrkelsen af og partnerskaber med en spiren-

88. Angry Planet, 'How Palantir is Using AI in Ukraine', Podcast (26. marts, 2024), 31:00f.
89. Netop erkendelsen fra "Maven" af, at AI-systemer skal testes og evalueres løbende for at kunne forbedres, blev omdrejningspunktet i CDAO's "Global Information Dominance Experiment" (GIDE) – et initiativ, der skal styrke beslutningsstøtte-AI ved hjælp af en 90 dages øvelsescyklus, hvor softwareingeniører og soldater sidder ved siden af hinanden, mens systemerne testes. Se CSIS, 'Scaling AI-enabled Capabilities at the DOD'.

de kommerciel AI-industri, der kan og vil træde til, når risikovilligheden ændrer sig. Eksistensen af DIU i Silicon Valley vidner om en erkendelse af behovet for og en vilje til at opdyrke relationer, der sikrer denne kommercielle villighed.

3.4. AI-våbensystemer

AI-våbensystemer er uden sammenligning de mest kontroversielle og mest omdiskuterede militære applikationer med AI. Våbensystemer, der autonomt, det vil sige uden behov for menneskelig indblanding efter systemets aktivering, engagerer mål, er dog ikke noget nyt. Amerikansk udviklede defensive autonome våbensystemer som Phalanx og Aegis Combat System har siden 1970'erne været svaret på, at hastigheden på antiskibsmissiler krævede en fuldt autonom reaktion uden menneskelig intervention.[90] Men systemerne var trænet på en række præprogrammerede "hvis X, så Y"-regler. De var ikke designet til at lære af deres beslutninger og reaktioner og bør derfor ikke – jf. denne rapports definition – karakteriseres som AI-systemer.[91] Det er stadig ikke veldokumenteret, hvorvidt og hvordan nutidens versioner af disse systemer gør brug af maskinlæring, når de engagerer mål. Bedst beskrevet er det israelske Iron Dome, der efter sigende har øget systemets præcision og effektivitet efter tilføjelsen af AI-algoritmer.[92] Og senest har flere kilder beskrevet, at mere offensive autonome våbensystemer i form af droner, der ved hjælp af AI selvstændigt kan identificere, følge og engagere mål, er blevet brugt i konflikterne i Gaza, Libyen, Nagorno-Karabakh og Ukraine.[93] Graden

90. Navy Lookout, 'Last ditch defence – the Phalanx close-in weapon system in focus', Technical Briefing, 10. august 2020, https://www.navylookout.com/last-ditch-defence-the-phalanx-close-in-weapon-system-in-focus/.
91. Tara Copp, 'US aims to stay ahead of China in using AI to fly fighter jets, navigate without GPS and more', *AP News*, 12. maj 2024, https://apnews.com/article/ai-military-machine-learning-autonomy-china-gps-5f327918075cea0bfc32e5d36cba801d.
92. Gautam Ramachandra, 'How Artificial Intelligence is improving the Iron Dome', Medium, 13. maj 2023, https://medium.com/@gautamrbharadwaj/how-ai-is-improving-iron-dome-3894cd3668f9.
93. Paul Lushenko, 'Trust but verify: U.S. troops, artificial intelligence, and an uneasy partnership', Brookings Commentary, 22. januar 2024, https://www.brookings.edu/articles/trust-but-verify-u-s-troops-artificial-intelligence-and-an-uneasy-partnership/.

af menneskelig kontrol i disse eksempler forbliver dog uklar. Men det vidner alligevel om, at AI-våbensystemer er virkelighed.

Det amerikanske forsvar indkøber i øjeblikket også en række autonome våbensystemer, herunder droner, der ved hjælp af AI-algoritmer er trænet til at kunne lokalisere og engagere både menneskelige og materielle mål, selv i situationer, hvor de mister kontakten til en menneskelig operatør. Og indkøbene er accelereret, efter at daværende viceforsvarsminister Kahleen Hicks i august 2023 annoncerede "Replicator" – Pentagons stort anlagte initiativ, der har som mål at gøre billige, autonome og udskiftelige robotter operative i 2026.[94] Virksomheder som Anduril og Shield AI har i de seneste år ikke blot vundet en række kontrakter, der skal levere forskellige ubemandede, autonome platforme, der selvstændigt destruerer fjendtlige droner i luften, overvåger områder og afsøger bygninger.[95] Det amerikanske marinekorps og specialstyrkerne har allerede taget flere af dronerne i operativ anvendelse.[96] Disse erfaringer illustrerer, hvordan det amerikanske forsvar arbejder med at håndtere især de folkeretlige og etiske udfordringer samt udfordringerne i forbindelse med at sikre systemer mod udefrakommende angreb.

For at forstå de amerikanske erfaringer med håndteringen af folkerets- og etikudfordringerne er det værd at bemærke, at størstedelen af de AI-baserede autonome systemers faktiske anvendelse i det amerikanske forsvar på nuværende tidspunkt hovedsageligt beskrives og implementeres som ISR-droner til støtte for den militære beslutningstager. Strategic Capabilities Office (SCO's) Perdix Drone Swarms er et illustrativt eksempel. SCO, der siden 2012 har haft i opdrag at finde kreative løsninger på konkrete problemer for de forskellige grene af USA's væbnede styrker,

94. "Replicator" er stadig kun et udviklingsprojekt, i den forstand at de AI-systemer, som i øjeblikket udvikles, stadig kun er på prototypestadiet. Da denne rapport hovedsageligt retter sig mod amerikanske AI-applikationer, der har fundet faktisk operativ anvendelse, vil der ikke blive gået yderligere i dybden med de konkrete "Replicator"-initiativer. Jim Garamone, 'Hicks Discusses Replicator Initiative', *DOD News*, 7. september 2023, https://www.defense.gov/News/News-Stories/Article/Article/3518827/hicks-discusses-replicator-initiative/.
95. Shield AI, 'Shield AI Joins Air Force's $950 million JADC2 effort', pressemeddelelse, 6. juli 2022, https://shield.ai/shield-ai-joins-air-forces-950-million-jadc2-effort/; Jackson Barnett, 'Anduril nabs $1B contract for anti-drone work with SOCOM', FedScoop, 20. januar, 2024, https://fedscoop.com/anduril-nabs-1b-contract-for-anti-drone-work-with-socom/.
96. Frank Bajak, 'Pentagon pushes A.I. research toward lethal autonomous weapons', *CBS News*, 25. november, 2023, https://www.cbsnews.com/sanfrancisco/news/pentagon-pushes-ai-research-toward-lethal-autonomous-weapons/.

videreudviklede Massachusetts Institute of Technology (MIT's) design af en billig sværm af mikrodroner, som ved hjælp af en AI-muliggjort distribueret "hjerne" på tværs af enheder bedre og mere modstandsdygtigt kan udføre ISR-opgaver.[97] Men hvad vigtigere er, så er disse systemer samtidig designet til at bære sprængladninger, så de i fremtiden autonomt kan engagere og destruere mål.[98] Det gør sig fx gældende med prestigeprogrammet Skyborg, der er en af de bærende platforme i det amerikanske flyvevåbens vision om Collaborative Combat Aircrafts (CCA).

CCA, også kendt som *loyal wingman*-konceptet, har til formål at få en formation af droner til at følges med den seneste generation af kampfly – noget, som Skyborg-programmet allerede demonstrerede muligt i 2020.[99] Dronerne indgår i et såkaldt human-machine-team, hvor de skal understøtte piloten med et mere effektivt situationsbillede med henblik på at øge ildkraften. Konkret leverer dronerne information til piloten om potentielle trusler, afdækker afstande, analyserer sandsynligheder og anviser handlingsmuligheder, så piloten kan tage hurtigere og mere informerede beslutninger. DARPA's Air Combat Evolution-program har ydermere vist, at en AI-drone udkonkurrerer en almindelig pilot i dogfights – kampe i luften mellem to kampfly.[100] Den teknologiske udvikling betyder således, at pilotens rolle er under udvikling og bevæger sig i retning af at indtage en mere tilbagetrukket position, der sætter rammerne for luftslaget, mens AI-styrede ubemandede platforme udkæmper kampen.[101]

Ovenstående dobbelthed understreger, at det amerikanske forsvar på den ene side stadig i praksis på nuværende tidspunkt primært ser AI-droner som et beslutningsstøtteværktøj, men på den anden side ønsker at sikre sig, at det teknologiske fundament er på plads, hvis en konflikt-

97. SCO, 'The Strategic Capabilities Office – Perdix Fact Sheet', DoD fact sheet (9. januar 2017).
98. Joseph Trevithick, 'Navy Special Ops Has Adapted RQ-21 Blackjack Drones To Deploy Smaller Quadcopters', *The War Zone*, 20. december 2021, https://www.twz.com/43568/navy-special-ops-has-adapted-rq-21-blackjack-drones-to-deploy-smaller-quadcopters.
99. Greg Hadley, '"Wildly Successful' Skyborg Will Become Program of Record but Won't Stop Developing S&T", *Air & Space Forces Magazine,* 16. august 2022, https://www.airandspaceforces.com/wildly-successful-skyborg-program-of-record-developing-st/.
100. Michael Marrow, 'In a "world first," DARPA project demonstrates AI dogfighting in real jet', *Breaking Defense*, 9. april 2024, https://breakingdefense.com/2024/04/in-a-world-first-darpa-project-demonstrates-ai-dogfighting-in-real-jet/.
101. Graae og Michelsen, 'F-35, Skyborgs og den kommende sværm', 139.

eskalation påkræver fuldt autonome AI-våbensystemer for at opretholde den militære overlegenhed. Samme åbenhed over for udvikling af autonome våbensystemer kan ses i USA's fortolkning af de folkeretlige forpligtelser for anvendelse af autonome våbensystemer. Her hedder det, at anvendelsen af autonome våbensystemer skal være underlagt et passende niveau af menneskelig dømmekraft,[102] hvilket i praksis betyder, at et menneske skal være involveret i beslutninger om, hvordan, hvornår, hvor og hvorfor våben skal anvendes.[103] Det betyder imidlertid *ikke*, som flere stater og NGO'er ellers ønsker, at anvendelsen er underlagt et krav om, at en menneskelig operatør altid skal have magten til – og meningsfuldt skulle kunne vælge – at omgøre en maskines beslutning om at udføre et angreb.[104] USA ser sin folkeretlige forpligtelse som et spørgsmål om at fastsætte og overholde tekniske krav til et autonomt våbensystems gennemsigtighed, auditeringsmulighed og forklarbarhed.[105] Det flugter med det amerikanske forsvars etiske principper for AI, hvor etik ikke formuleres ud fra, hvorvidt der sikres meningsfuld menneskelig kontrol med AI-systemer, men ud fra, hvorvidt udviklingen og implementeringen er i overensstemmelse med et sæt af principper for test, evaluering, validering og verificering, der er underlagt en klar governancestruktur, som løbende skal sikre, at systemet kun gør det, der er hensigten.

Det amerikanske forsvar har således udviklet en konsistent praksis for udvikling af AI-våbensystemer, hvor der er sammenhæng mellem 1) den strategiske anerkendelse af, at AI-baserede fuldautonome våbensystemer hurtigt kan blive nødvendige, 2) understøttelsen af en teknologisk udvikling og klargøring af AI-systemer som mulige våbensystemer og 3) de folkeretlige og etiske fortolkninger, som lægger vægt på vigtigheden af at efterleve tekniske og metodiske kriterier for udvikling og anvendelse af AI-baserede våbensystemer. Men netop de høje tekniske

102. Oversat fra "approapriate levels of human judgement".
103. Kelley M. Sayler, 'Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems', Congressional Research Service – In Focus (opdateret 1. februar 2024); Lutiana V. F. Barbosa, 'Exploring the 2023 U.S. Directive on Autonomy in Weapon Systems', *CEBRI-Journal* 2, nr. 7 (2023): 117-136.
104. Human Rights Watch, 'Killer Robots and the Concept of Meaningful Human Control: Memorandum to CCW Delegates, Human Rights Watch', Human Rights Watch Memo, 11. april, 2023; Ray Acheson, 'Editorial: Convergence Against Killer Robots', *CCW Report* 9, nr. 3 (2021): 1-3; Bonnie Docherty, 'Elements of a Treaty on Fully Autonomous Weapons', Stop Killer Robots Briefing Paper, marts 2019.
105. Hicks, 'Directive 3000.09'.

krav til virksomheder, der udvikler AI-systemer, gør samtidig, at virksomhederne skal gennemgå en tung proces, der skal vurdere, om de lever op til de nødvendige cybersikkerhedsstandarder og udviklingsstandarder i henhold til den nationale forsvarsautorisations lov (NDAA). Mens processerne minimerer sårbarheden over for en modstanders ønske om at underminere AI-systemerne, og selvom DIU har forsøgt at øge hastigheden af disse processer, fx gennem Blue UAS Cleared List for droner,[106] så er processen fortsat for tung for mindre virksomheder, som således ofte søger at blive opkøbt at de større forsvarsindustrielle aktører, der har ressourcerne til at blive certificeret.[107]

3.5. Generelle takeaways

Dette kapitel har søgt at afdække det amerikanske forsvars strategier, initiativer og projekter. Opmærksomheden blev her primært rettet mod de AI-løsninger, der faktisk bliver taget i anvendelse i det amerikanske forsvar, og specifikt med henblik på at afdække, hvad udviklings- og implementeringsforløbene, der er gået forud for anvendelsen, fortæller os om, hvordan de generelle udfordringer for militær anvendelse af AI er blevet søgt imødegået.

Det amerikanske forsvar adresserer *datakvalitetsudfordringerne* ved på den ene side at sikre, at organisationen strategisk prioriterer en overordnet datatransformation, hvor dataindsamling, databearbejdning og dataanalyse strømlines på tværs af alle enheder og med klare juridiske rammer for relationen med de private virksomheder, der støtter med datahåndtering og udvikling (top-down), og på den anden side at tage ved lære af de succesfulde eksperimenter, der er startet i det små med at løse konkrete, mindre udfordringer hos enhederne, men faktisk har evnet at skalere (bottom-up). Sidstnævnte er blandt andet sket med fokus på at udvikle nogle tekniske og metodiske standarder for en ansvarlig

106. Defense Innovation Unit, 'Blue UAS', DIU's hjemmeside (ingen dato), https://www.diu.mil/blue-uas.
107. Jackson Barnett, 'Anduril buys small drone company, expanding its innovative tech portfolio', *FedScoop* (1. april 2021), https://fedscoop.com/anduril-buys-small-drone-company-expanding-innovative-tech-portfolio/; GAO, 'Artificial Intelligence: DOD Needs Department-wide Guidance to Inform Acquisition'.

AI-produktcyklus – fra design over udvikling til deployering og faktisk anvendelse.

Kombinationen af at udvikle standarder for AI-udvikling og introducere sprints og øget øvelseshastighed er samtidig et forsøg på at håndtere den *tillidsudfordring*, som ofte gør sig gældende, når militær AI skal tages i anvendelse. Jo hurtigere pilotprojekter placeres i hænderne på slutbrugeren, desto bedre forståelse – og ultimativt tillid – får denne til AI-applikationerne. Udviklingen af ansvarlige AI-standarder vidner også om et ønske om at håndtere de *folkeretlige og etiske udfordringer*, der ligeledes kan påvirke tilliden hos de operative enheder. Ved hjælp af tekniske praksisser og metoder samt en klar governancestruktur søger det amerikanske forsvar at skabe tilstrækkelig gennemsigtighed, så både brugere og tilsyn kan verificere systemernes pålidelighed. Men med sin meget tekniske forståelse af etisk AI undgår det amerikanske forsvar at skulle forholde sig til spørgsmålet om, hvad meningsfuld menneskelig kontrol over AI-(våben)systemer egentlig indebærer. Dog er prioriteringen af overholdelse af tekniske krav til sikkerhed og ansvarlighed hjælpsomt i forsøget på at imødegå *udfordringen ved tilstedeværelsen af en modstander,* der ønsker at forstyrre systemerne.

Det amerikanske forsvars mest succesfulde AI-projekter kan føres tilbage til, at man har evnet delvist at *håndtere indkøbsudfordringen*. Oprettelsen af DIU, der fik i opdrag at få kommercielle teknologier ind i det amerikanske forsvar, førte til en genfortolkning af de eksisterende, tunge indkøbs- og valideringsprocesser. Samtidig var samarbejdet med de private virksomheder og universiteter – fx i forbindelse med test og evaluering af AI-modeller – en måde at forsøge at *minimere udfordringen med en utilstrækkelig AI-parat arbejdsstyrke* på. Selvom der stadig er udfordringer med at få selv succesfulde pilotprojekter fuldt udrullet (Valley of Death-problematikken) og med at sikre tilstrækkelig AI-viden i arbejdsstyrken,[108] har især mange af de drifts-AI-systemer, der bliver anvendt i dag, nydt godt af den mere eksperimentelle tilgang, som DIU og SCO blandt andet repræsenterer, og de har demonstreret, at AI-systemer tilfører merværdi til det amerikanske forsvar. Samtidig har DIU succesfuldt prioriteret at knytte tættere bånd til en spirende AI-industri i Silicon Valley, så det amerikanske forsvar ikke længere er en politisk

108. Kahn, 'Risky Incrementalism'.

ukorrekt samarbejdspartner. I stedet har flere og flere AI-virksomheder i dag i stigende grad både viljen og evnen til at støtte det amerikanske forsvar. Til tider kan disse virksomheder endda selvstændigt videreudvikle og teste AI-applikationer til støtte for amerikanske strategiske interesser i fx Ukrainekrigen, hvor risikovilligheden for militær AI er stor, og afprøvningen af selv de stadig kontroversielle AI-applikationer derfor er mulig.

Ovenstående illustrerer to modsatrettede dynamikker, som ethvert nationalt forsvar, der ønsker at anvende militær AI, bør balancere.

For det første bør et forsvar balancere en omfattende strategisk forandring af organisationen fra et hardwarebaseret til et datadrevet, softwarebaseret forsvar med en AI-strategi, der organisatorisk muliggør en prioritering af eksperimenter og AI-pilotprojekter i de centrale enheder, som søger at problemløse i den operative praksis.

Og for det andet bør et forsvar balancere udviklingen af ansvarlige standarder for udvikling og deployering af militær AI med forberedelsen af en situation, hvor risikovilligheden for deployeringen af militær AI hurtigt har ændret sig.

Men USA har verdens suverænt største forsvarsbudget og verdens førende tech-industri. Det skaber selvfølgelig et stærkt fundament for udvikling af militær AI, som ikke bare kan kopieres til andre lande. Hvordan balancering af de to modsatrettede dynamikker således konkret bør tage sig ud for andre stater, der overvejer at udvikle militær AI, afhænger af, hvad de strategiske ambitioner er, hvor stor den politiske og økonomiske appetit på militær AI er, hvor langt det nationale forsvar er i udviklingen af militær AI, hvordan den nationale kommercielle industri og forskningsverden inden for AI ser ud, hvordan samarbejdet i øjeblikket fungerer, og hvordan de kommercielle og strategiske internationale partnerskaber ser ud. Det næste kapitel adresserer de to dynamikker i konteksten af det danske forsvar.

4

Diskussion: Danske læringspunkter

Dette kapitel indledes med en gennemgang af de danske strategier, initiativer og projekter, der knytter sig til anvendelsen af militær AI. Herefter følger to afsnit, hvori den danske tilgang holdes op imod og diskuteres i relation til hver af de to modsatrettede dynamikker: *transformation versus eksperiment* og *ansvarlighed versus risikovillighed*. Afsnittene viser, hvordan Forsvarsministeriets koncern kan begynde at leve op til sit strategiske mål om at være en datadrevet organisation, der kan bidrage til NATO's interoperable multidomænevision. Kapitlet argumenterer for, at der mangler en strategisk retning og en systematisk udnyttelse af de danske styrkepositioner. Det kræver en strategi og samarbejde.

4.1. Militær AI i Danmark

Forsvarsministeriet og Forsvaret anerkender fuldt ud, at den hastige teknologiske udvikling og dennes indvirkning på geopolitikken kræver strategiske prioriteringer og investeringer, blandt andet i den digitale rygrad, som skal styrke datagrundlaget og dermed mulighederne for bedre integration af militær AI. Det lader til, at Forsvarsministeriet ikke længere ser det som en mulighed udelukkende at fortsætte med at købe udenlandske *off-the-shelf*-teknologier til Forsvaret, men faktisk har valgt at bevæge sig i retning af en datacentrisk organisationsændring, der er interoperabel med NATO's multidomænevision. Denne bevægelse underbygges af, at Forsvarsministeriet er i gang med flere AI-relaterede strategier, inklusive en koncernfælles digital transformationsstrategi,

strategi for AI og dataanalyse, it-støtte og digital kompetenceudvikling.[109] Centralt for den digitale transformation står Danish Common Operational Information Environment (DA-COIE) – visionen om at samle arkitekturer og systemer på en måde, der muliggør en datadrevet militær organisation og en interoperabel (multidomæne)praksis.[110] Mere håndgribeligt er her ønsket om en operativ udmøntning af DA-COIE i en såkaldt *defence information cloud*, som er det cloudmiljø, der skal sikre dataejerskab og muliggøre deling af information på tværs af organisationen. Et måske endnu mere konkret initiativ er "Projekt IT-konsolidering og Transformation" (PIT) – i dag integreret i FMI's Cyberdivision – som fik i opdrag at strømline og optimere koncernens it-infrastruktur.[111]

Anerkendelsen af et behov for øget forsvarsteknologisk udvikling førte i 2021 til udgivelsen af regeringens forsvarsindustrielle strategi.[112] Og senest har FMI også oprettet en stilling som materieldirektør og en Danish Defence Innovation Unit med ansvar for samarbejdet med industrien samt med EU, NATO og NORDEFCO. Det bygger oven på FMI's eksisterende Værnsfælles Videnscenter, som tidligere har stået for medfinansiering af udviklingsprojekter med danske vidensinstitutioner og virksomheder, blandt andet forsøgsprojekter til afprøvning og udvikling af AI-software til klassificering af fly og udvikling af AI-analysekapacitet i satellitter.[113]

Samtidig med det overordnede strategiske og organisatoriske arbejde er Forsvaret engageret i programmer, der gør brug af AI. På udviklingsfronten indgik Hærens 1. Brigade i 2023 en kontrakt med virksomheden TERMA om et luftforsvarssystem, som indeholder et AI-assisteret C2-system. Og TERMA udvikler allerede *computer vision*-software i regi af F-35-kampflyprogrammet, der skal få mening ud af den store mængde data, som flyets sensorer indsamler.[114] Virksomheden Systematic, der le-

109. Graae, 'Servers Before Tanks?', 174.
110. Bollmann og Jacobsen, 'Militær dataoversættelse og digital transformation', 91.
111. Ibid., 100.
112. Regeringen, 'Regeringens strategi for dansk forsvarsindustri – Styrket samarbejde for dansk sikkerhed' (2021).
113. Forsvaret, 'Årsberetning, Forsvarskommandoen 2022' (2023); Jan Schelbech, 'Norden kan sætte NATOs dagsorden for Østersøområdet', *FMI Nyheder*, 30. maj 2024, https://www.fmi.dk/da/nyheder/2024/norden-kan-satte-natos-dagsorden-for-ostersoomradet/.
114. Jens Bertelsen, 'Dansk virksomhed udvikler livsvigtig software til F-35 kampfly – kan overvåge malkekøer i Jylland og nedkæmpe missiler i Østersøen', *AvisenDanmark*, 2. sep-

verer sit *battle management-system* til Hæren (og NATO), har også i sin seneste version af systemet inkorporeret AI i forsøget på bedre at kunne identificere afvigelser fra det almindelige operationsbillede.[115] Derudover har Søværnet indkøbt KATFISH sonarsystemet fra canadiske Kraken Robotics, der gør brug af AI til minemonitorering af havbunden,[116] og Arktisk Kommando har rekvireret et AI-baseret system, der sammenkører sensordata med henblik på at identificere skibe, som har slukket for deres automatiske identifikationssystem (AIS). Palantirs AI-software til datasammenkørsel bruges også i dele af organisationen.

Disse og lignende programmer vidner om, at anvendelsen af militær AI i Forsvaret stadig er i et tidligt stadie. Men hvad vigtigere er, så vidner det om, at AI-integrationen hovedsageligt er foranlediget af forsvarsvirksomhederne i forsøget på at forbedre deres respektive produkter og dermed hverken er baseret på Forsvarets specifikke ønske om at eksperimentere med AI for at løse konkrete operative problemer eller på en klar strategisk ambition om at tage kontrol med data og skalere brugen af AI-løsninger på tværs af organisationen. At både den danske forskningsverden og den danske forsvarsindustri i øjeblikket prioriterer udviklingen af AI, er dog ikke nødvendigvis et problem, men kan med fordel udnyttes i den videre udvikling af militær AI i regi af Forsvaret. Systematics nyvundne 12-årige kontakt med NATO om levering af virksomhedens C2-softwareløsning, SitaWare Edge, er en oplagt mulighed for, at Danmark tilegner sig værdifulde erfaringer om den militære anvendelse af AI. Det samme gør sig gældende for det TERMA-ledede, EU-finansierede "AI4Def"-projekt, som samler både virksomheder og vidensinstitutioner med henblik på at støtte implementeringen af AI i Europas væbnede styrker.[117] Netop fordi projektet baserer sig på data fra blandt andet det danske forsvar og FMI, står Forsvaret også først for

tember 2023, https://avisendanmark.dk/erhverv/skolebus-eller-kampvogn-dansk-firma-udvikler-livsvigtig-software-til-f-35-kampfly.

115. Graae, 'Servers Before Tanks?', 184, 188.

116. AIT News Desk, 'Kraken Delivers Significant Technical Upgrade for Royal Danish Navy's Mine Countermeasures (MCM) Efforts', *AIThority News*, 11. juni 2022, https://aithority.com/robots/kraken-delivers-significant-technical-upgrade-for-royal-danish-navys-mine-countermeasures-mcm-efforts/.

117. TERMA, 'Terma will lead one EU-funded R&D project, participate in two others', TERMA News, 2. juli 2021, https://www.terma.com/news-events/news/news-archive/2021/terma-will-lead-one-eu-funded-rd-project-participate-in-two-others/.

med hensyn til at kunne få operativ glæde af projektet. Men **det kræver udvikling af en fælles Forsvarskommando (FKO)-FMI-proces for erfaringsopsamling og implementering i de operative enheder, herunder gentænkning af de eksisterende udbuds- og indkøbsprocedurer.** Sidstnævnte ville bidrage til håndteringen af de velkendte indkøbs- og implementeringsudfordringer, der generelt karakteriserer integrationen af militær AI.

Forsvarets manglende strategiske prioritering af militær AI ses tydeligst i de store indkøbsprogrammer som F-35-kampflyprogrammet og kapacitetspakken til overvågning af Arktis. Her blev indledningsvist kun afsat meget begrænsede midler til dataindsamling, dataprocesser og dataanalyse, og der var ingen officielle tanker vedrørende udviklingen af AI til systematisk udnyttelse af heraf.[118] AI-kapacitet til analyse bør indtænkes fra starten ved fremtidige dataindsamlingstunge materielinvesteringer, og samtidig bør ekstra ressourcer sættes af til vedvarende test og evaluering før, under og efter AI-systemernes operative anvendelse. En af grundene til disse udeladelser kan meget vel – som Bollmann og Jacobsen påpeger[119] – være utilstrækkelig viden om og forståelse af data og brugen heraf, og en del af løsningen er således givetvis en bedre uddannelsesindsats og mere fokus på dataoversættelseskompetencer og -funktioner på tværs af organisationen. **Her kan Forsvarsakademiet med fordel løse de gængse uddannelsesudfordringer for integration af militær AI ved at udvikle strategiske uddannelsessamarbejder på det teknologiske område med det eksisterende danske teknologiske videnskab.** Og FKO kan ligeledes understøtte denne indsats ved at beslutte, at alle enheder fremover skal have officerer med dedikerede AI-funktioner.

I tillæg hertil står Forsvarsministeriets koncern over for nogle valg og prioriteringer, som den resterende del af kapitlet vil diskutere.

118. Graae, 'Servers Before Tanks?', 177-179.
119. Bollmann og Jacobsen, 'Militær dataoversættelse og digital transformation', 117-178.

4.2. Transformation versus eksperiment

Det amerikanske forsvar har været igennem en modningsproces, hvor de bredere, strategiske tanker om en datatransformation er gået hånd i hånd med en mere eksperimentel og decentral tilgang til udvikling og implementering af AI-understøttede systemer ude i værnene og med støtte fra forskningen og industrien. Det har konkret betydet, at erfaringer fra de faktiske forsøg på at implementere militær AI ikke blot i stigende grad bliver udviklet med blik for skalerbarheden, men også har påvirket den strategiske udvikling, fx med hensyn til hvilke udviklingspraksisser der konkret konstituerer ansvarlig udvikling af AI.

Danmark er slet ikke samme sted. Forsvarsministeriet arbejder fortsat på de første strategiske dokumenter om anvendelse af militær AI. Det til trods for at Danmark allerede er forpligtet til at implementere NATO's (reviderede) AI-strategi – en strategi, der ikke stemmer overens med Danmarks eksisterende generelle nationale AI-strategi, som i udgangspunktet afviser anvendelse af AI til militære formål. **En strategi, der fastholder et strategisk fokus på simultant at sikre transformation og eksperiment, er en nødvendighed.** Samtidig har FKO endnu ikke prioriteret at uddrage generelle erfaringer fra faktiske, decentrale AI-eksperimenter i enhederne og i FMI. Selvom visionen om en bredere datatransformation er til stede (i hvert fald på ministerielt niveau), har den lange strategiudviklingsproces og langsomme udmøntning af de mange ekstra økonomiske midler til Forsvaret i praksis fungeret som en undskyldning for ikke at gå i gang med at udvikle og eksperimentere med AI-systemer til faktisk operativ problemløsning. Erfaringerne fra USA viser dog, at de decentrale eksperimenter bidrager med vigtige erfaringer til strategiudvikling – både når de virker, når de fejler, og når de møder offentlighedens kritik. Ufærdige og langsommelige strategiprocesser må således ikke blive en sovepude. Selvom det er nemmere for USA med verdens største forsvarsbudget at eksperimentere og acceptere fejlskud, må danske AI-eksperimenter nødvendigvis også tilskyndes, hvis Danmark vil gøre sig håb om at udvikle militær AI – og en sådan tilskyndelse bør ledsages af et krav om mere åbenhed om både succeshistorier og fejlskud samt om, at de brugte datasæt er gennemsigtige og tilgængelige på tværs af koncernen. Hvor førstnævnte skal inspirere andre dele af Forsvaret, skal sidstnævnte støtte visionen om interoperabilitet og skalerbarhed – også på tværs af NATO-alliancen. Forsvarspolitisk er Danmark dog

risikoavers, når det kommer til eksperimenter, og kun enkelte steder i koncernen, fx i specialstyrkerne, er der en stærk tradition herfor. En bredere kulturændring er derfor nødvendig. **Et naturligt sted at starte er drifts-AI-projekter, der er forbundet med færre udfordringer og stadig bidrager med erfaringer, der kan hjælpe det strategiske arbejde med at håndtere de typiske datakvalitetsudfordringer.** Forsvaret gør fx allerede brug af en robot, der støtter registreringen af værnepligtige.[120] Tydeliggøres den konkrete håndtering af data og brugen af AI i sådanne systemer, vil det kunne inspirere både strategiudviklingen og den eksperimentelle udvikling andre steder i organisationen.

En tilskyndelse til, at alle enheder fra Føringsstøtteregimentet til specialstyrkerne til Personalestyrelsen søger at optimere processer ved hjælp fra AI, kræver dog ikke blot, at det ansatte personel har forståelse for, hvad AI kan og ikke kan. Det kræver også, at der faktisk er tekniske kompetencer til stede, der kan udvikle og teste AI-modeller og AI-applikationer. Det er sjældent tilfældet i Forsvarsministeriets koncern. Men i stedet for – i hård konkurrence med både forskningsverdenen og industrien – at forsøge at rekruttere de eftertragtede medarbejdere med de rette datavidenskabelige kompetencer, **kan Forsvarsministeriets koncern med fordel – og med inspiration fra USA – forsøge at håndtere videns- og rekrutteringsudfordringerne ved at søge at finde de mest optimale konstellationer for indgåelse i flere såkaldte triple helix-samarbejder med industrien og forskningsverdenen**. Det kræver dog en række konkrete tiltag, før et sådant samarbejde kan skabe værdi. For det første må Forsvarsministeriet afsætte ekstra ressourcer og prioritere at sikkerhedsgodkende universitetsforskere og medarbejdere i virksomheder. Det kræver opbygning af tillid – begge veje. For det andet skal der udvikles en kontraktramme, der kan håndtere eksisterende indkøbsudfordringer, så det bliver muligt for virksomheder at kommercialisere de udviklede AI-modeller, mens Forsvaret af nationale sikkerhedsgrunde beholder ejerskabet over de algoritmer, som er udviklet på baggrund af Forsvarets data. Og for det tredje bør Forsvaret sikre, at DIU-lignende strukturer har en kapacitet, så de ikke blot kan koble innovative AI-virksomheder med de decentrale enheder i Forsvaret, der ønsker at eksperimentere, men også faktisk kan understøtte og øge hastigheden i udviklings- og

120. Graae, 'Servers Before Tanks?', 188.

testarbejdet. Givet den nuværende tilbageholdenhed med at tilføre ekstra administrative årsværk til Forsvaret, ønsket om minimal politisk risiko samt strikse fortolkninger af eksisterende udbudsregler i FMI kunne sådanne samarbejdsstrukturer med fordel tage form af partnerskabsmodeller og forankres uden for Forsvarsministeriets koncern.

Netop vigtigheden af at opdyrke et stærkt triple helix-samarbejde knytter sig også til den næste afvejning.

4.3. Ansvarlighed versus risikovillighed

USA balancerer et ansvarlighedsregime i den tekniske udvikling af militær AI med en bevidsthed om nødvendigheden af at være teknologisk beredt, når risikovilligheden for anvendelsen af AI ændrer sig i tilfælde af konflikteskalation. USA's ansvarlighedsregime repræsenterer således en bestemt måde at fortolke de etiske og folkeretlige udfordringer og forpligtelser ved militær AI på, nemlig en måde, hvor det er sigtet at skabe mere gennemsigtighed i udviklingsprocessen gennem standarder og grundige test- og evalueringsprocesser. Denne fortolkning har også til hensigt at inspirere andre staters AI-udvikling og ultimativt sikre, at anvendelse af militær AI sker inden for – hvad USA ser som – forudsigelige og kontrollerbare rammer.

Danmark har ikke udviklet en politik eller en retlig ramme for udvikling og anvendelse af ansvarlig militær AI. **En strategi for militær AI bør indeholde klare rammer for ansvarlig AI**. Den amerikanske prioritering af ansvarligheden på det tekniske og metodiske udviklingsniveau samt i forhold til at have en klar governancestruktur kunne fint fungere som inspiration for en dansk forsvarsstrategi for AI. Her er DoD's *Responsible Artificial Intelligence Strategy and Implementation Pathway* fra 2022 særligt relevant, da den netop opstiller klare mål og konkrete indsatser. En dansk pendant kunne således med fordel indeholde lignende elementer: a) etablere en governancestruktur med fokus på vidensdeling og tilsyn; b) opbygge et robust test-, evaluerings-, verificerings- og valideringsregime (TEVV) med realtidsmonitorering og brugerfeedback; c) strømline implementering af AI-produkter gennem hele indkøbsforløbet, fx med inspiration fra den private sektors risikohåndtering; og d) opdyrke et ansvarligt AI-økosystem i industrien og forskningsverde-

nen.[121] En implementeringsplan med disse elementer vil således adressere de typiske udfordringer vedrørende datakvalitet, tillid, folkeret, etik og sårbarheden over for fjendtlige forstyrrelser.

Og netop en dansk selvforståelse om at være en *ansvarlig* småstat med hensyn til udenrigs- og forsvarspolitikken gør det oplagt for Danmark at etablere sig som en stærkere stemme i de internationale drøftelser om ansvarlig brug af militær AI. **Her vil især opbygningen af et robust TEVV-regime være en naturlig dagsorden at sætte sig på.** Der er internationalt behov for og efterspørgsel efter at få afdækket, fx hvordan stater overholder deres folkeretlige våbenscreeningsforpligtelser, når våbnene understøttes af AI. Et sådant arbejde kræver en god relation til de virksomheder, som udvikler algoritmerne, og med TERMA og Systematic som to af Europas førende virksomheder inden for netop militær softwareudvikling står Forsvaret, FMI og Forsvarsministeriet godt med hensyn til at kunne løfte TEVV-opgaven. Med Sveriges og Finlands indtræden i NATO bør mange af de forhindringer, der tidligere eksisterede i de mere praktiske NORDEFCO-samarbejder, også være skaffet af vejen. Stiller Danmark sig i spidsen for et sådant nordisk offentlig-privat TEVV-udviklingsprojekt, åbner det døre for hjemtagning af EU-midler, fx i regi af PESCO-samarbejdet eller European Defence Fund, til gavn for det danske forsvar.

Som nævnt udvikler det amerikanske forsvar imidlertid også militær AI med øje for fremtidige situationer, hvor der kan blive behov for at accelerere deployering af AI-systemer i krig. Ikke nok med at mange af de anvendte AI-systemer til ISR i det amerikanske forsvar er klargjort til i fremtiden at blive brugt som autonome våbensystemer – Ukrainekrigen har også omdannet Ukraine til et centralt laboratorium for hurtig anvendelse af militær AI, fx for amerikanske virksomheder. Det ukrainske forsvar og den ukrainske regering har af naturlige årsager en anden risikovillighed, når det kommer til hastig brug af nye AI-assisterede systemer i deres kamp for overlevelse. Det betyder, at den accelererede anvendelse af militær AI – blandt andet faciliteret af amerikanske virksomheder – ikke nødvendigvis lever op til de krav og standarder, som det

121. Disse principper og prioriteter flugter også med NATO's AI-strategi, som Danmark er underlagt og skal implementere. NATO, 'Summary of the NATO Artificial Intelligence Strategy', officiel tekst, 22. oktober 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

amerikanske forsvar har fastsat for ansvarlig AI. Paradoksalt nok er den igangværende krig i Ukraine den bedste måde at få testet og evalueret militære AI-applikationer på i et virkeligt miljø – og dermed ultimativt på længere sigt sikre en anvendelse, der faktisk kun fungerer efter hensigten og dermed kan demonstrere overholdelse af folkeretlige konventioner. I dette lys kan Danmarks store politiske vilje til økonomisk at støtte Ukraines frihedskamp også gavne det danske forsvars anvendelse af militær AI – og uden at Danmark selv påtager sig nogen stor risiko.

Danmark har tidligt i krigen etableret sig som en – i forhold til sin størrelse – stor donor af materiel til Ukraine. Ukraines behov har dog ændret sig i takt med krigens og herunder teknologiens udvikling. Ukraines forsvar ønsker ikke længere blot konventionelt materiel, men innovative løsninger, der kan løse operative problemer på jorden, fx AI-understøttede løsninger i forbindelse med ISR, TD og C2 eller anti-drone-teknologi. Samtidig har den ukrainske regering ændret sin strategiske prioritering vedrørende udenlandske virksomheder. Ukrainerne inviterer ikke længere ukritisk udenlandske virksomheder indenfor og overdrager dem ukrainske data fra kampplads en. De har set, at "testet i Ukraine" er et kommercielt værdifuldt stempel, og de kobler derfor ukrainske virksomheder på projekterne for at holde ukrainske data i landet og derved sikre en konkurrencefordel for en spirende ukrainsk AI-forsvarsindustri.[122] Udmøntes dele af den fremtidige danske militærstøtte til Ukraine til finansiering af innovative partnerskabskonstruktioner mellem danske forskningsinstitutioner og forsvarsvirksomheder og de tilsvarende ukrainske aktører, med fokus på løsninger af faktiske operative udfordringer på kampplads en, kan det styrke et dansk vidensmiljø for militær AI og dermed ultimativt støtte det danske forsvar. FMI, FKO, Dansk Industri og Udenrigsministeriet opbygger i øjeblikket tætte bånd til det ukrainske forsvar og søger løbende dialog om dets aktuelle behov. Mens dette er et godt sted at starte, skal sådanne konstruktioner samtidig have det økonomiske grundlag og handlerum til at kortslutte de tunge indkøbs- og implementeringsregimer samt spændingerne på tværs af Forsvarsministeriets nuværende styrelsesstruktur.

En succesfuld partnerskabskonstruktion med dertilhørende udlicitering af risikovillighed til Ukraine i forbindelse med anvendelsen af ukra-

122. Bergengruen, 'How Tech Giants Turned Ukraine Into an AI War Lab'.

insk-danske militære AI-løsninger forudsætter dog et tæt samarbejde om løsningen af konkrete, operative problemer med militær AI mellem danske AI-virksomheder, danske AI-forskere og Forsvaret og de tilsvarende ukrainske aktører. Men **det kræver, at Forsvarsministeriet politisk får mulighed for at støtte Ukraine med andet end konventionelt materiel, så ministeriet kan dedikere en separat pulje under Ukrainestøtten til AI-udvikling og innovation.** En sådan pulje bør ydermere indeholde en systematisk erfaringsopsamling med henblik på at videreudvikle løsningerne i samarbejde med de danske virksomheder, så de kan demonstrere, at de lever op til nogle klare krav for ansvarlig AI. Men det kræver som minimum, at Danmark i en forsvarsstrategi for ansvarlig AI har forholdt sig til, hvad ansvarlig AI faktisk er.

5

Konklusion og anbefalinger

Rapporten indledtes med en vision for fremtidens kampplads – en kampplads, hvor AI er med hele vejen, fra målidentifikation til udvikling af operationsplaner og ultimativt til engagement af det enkelte mål. Men selvom udviklingen går stærkt, er nutidens forsvarsorganisationer stadig et stykke fra bredt at kunne anvende militær AI på den måde, som en virksomhed som Palantir Technologies forsøger at sælge. Rapporten har forsøgt at se nærmere på den virkelighed, hvori militær AI faktisk har fundet operativ anvendelse i dag – og samtidig gøre det på en måde, der, frem for en kritisk undersøgelse af militær AI som begreb og strategi, er rettet mod et praksisnært og handlingsanvisende mulighedsrum for det danske forsvar, der ønsker organisatorisk at tilpasse sig til en multidomænevirkelighed. Rapporten har brugt USA som empirisk inspiration – ikke blot fordi det amerikanske forsvar og de amerikanske forsvarsvirksomheder er længst fremme med udvikling og implementering af AI, men også fordi der har været en åben drøftelse om, hvor langt USA er, og hvilke udfordringer landet har haft.

Rapporten foretog indledningsvist en række konceptuelle afgrænsninger, herunder identificerede den syv udfordringer for udvikling og implementering af militær AI samt tre forskellige kategorier af militær AI. Struktureret ud fra de tre kategorier – drifts-AI, beslutningsstøtte-AI og AI-våbensystemer – analyserede rapporten, hvordan det amerikanske forsvar, til tider succesfuldt, har forsøgt at overvinde de gængse udfordringer. Analysen gennemgik en række amerikanske eksempler og viste, at:

1) De mindre kontroversielle drifts-AI-systemer blev succesfuldt udviklet gennem en eksperimentel og innovativ tilgang til udvikling og

implementering i samarbejde med forskningsverdenen og private virksomheder

2) Beslutningsstøtte-AI-projekter som "Maven" overvandt data-, implementerings-, og tillidsudfordringerne, fordi projekterne var forankret øverst i hierarkiet, men adresserede konkrete militæroperative udfordringer, fordi de inddrog forskningsinstitutioner og virksomheder til test og evaluering, og fordi de evnede at balancere et behov for tillid, etiske bekymringer og ansvarlighed med et behov for at tage risici

3) AI-våbensystemer overvinder de folkeretlige og etiske udfordringer ved at fortolke disse problematikker som et spørgsmål om at efterleve tekniske og metodiske kriterier for udvikling og test, men samtidig udvikle mindre kontroversielle AI-baserede ISR-systemer med en bevidsthed om, at en mere risikovillig situation kan opstå, hvori disse systemer hurtigt skal kunne klargøres som faktiske AI-våbensystemer.

Baseret på disse fund blev de amerikanske erfaringer opsummeret som to modsatrettede dynamikker, som ethvert forsvar, der søger at anvende militær AI, bør balancere og tilpasse til sin specifikke kontekst: *Transformation versus eksperiment* og *ansvarlighed versus risikovillighed*.

De to modsatrettede dynamikker blev strukturerende for diskussionen af de danske muligheder for at anvende militær AI i overensstemmelse med Forsvarets strategiske mål om at være en datadrevet organisation, der kan spille ind i NATO's interoperable multidomænevision. Forsvaret er sporadisk og langsomt ved at tilpasse sig til en virkelighed, hvor AI er en uundgåelig del af den militære organisation og operation. Der mangler dog ikke blot specialiseret viden og oversættelseskompetencer i organisationen,[123] men også en klar strategisk retning og en systematisk udnyttelse af de særlige styrkepositioner, som især danske softwarevirksomheder og forskningsverdenen har tilegnet sig på det militære AI-område. Heldigvis er der stadig rum for, at det danske forsvar får militær gavn af AI og derved kan følge med den teknologiske udvikling, de alliancemæssige forventninger og det ændrede trusselsbillede.

Fem anbefalinger med inspiration fra USA, men tilpasset de særlige forhold, der gør sig gældende i Danmark, kan hjælpe det danske forsvar på vej:

123. Bollmann og Jacobsen, 'Militær dataoversættelse og digital transformation'.

Anbefaling 1 – Strategi: Det er afgørende, at Forsvarsministeriet i den kommende militære AI-strategi a) eksplicit afdækker de danske krav til ansvarlig militær AI og b) fastholder det strategiske fokus med en ambitiøs implementeringsplan, der indeholder:

v. En governancestruktur med fokus på vidensdeling og tilsyn
vi. Opbygning af et test-, evaluerings-, verificerings- og valideringsregime (TEVV) med realtidsmonitorering og løbende brugerfeedback
vii. En strømlinet proces for implementering af AI-produkter gennem hele indkøbs- og implementeringsforløbet med fokus på håndtering af risici
viii. Opdyrkning af et ansvarligt AI-økosystem i industrien og forskningsverdenen.

Anbefaling 2 – Eksperimenter: Uafhængigt af det igangværende strategiarbejde bør Forsvarsministeriet tilskynde underliggende myndigheder til at igangsætte konkrete projekter (eksperimenter) med AI-løsninger i den praktiske opgaveløsning, især i forbindelse med optimeringen af driftsfunktionerne, og gerne i samarbejde med virksomheder og vidensinstitutioner. Det kræver dog samtidig:

iv. At der afsættes en pulje, som de underliggende myndigheder kan søge til igangsættelsen af sådanne projektet – gerne i samarbejde med industrien og forskningsverdenen
v. Igangsættelsen af en systematisk afdækning af muligheder for undtagelser til eller opdatering af eksisterende udbuds-, indkøbs-, kontrakts-, klassificeringsprocedurer
vi. Etableringen af en proces for systematisk erfaringsindhentning fra de igangsatte projekter, der kan inspirere de videre strategiudviklingsprocesser.

Anbefaling 3 – Uddannelse: Forsvarskommandoen bør oprette AI-officersfunktioner hos de underliggende myndigheder og sikre tilstrækkelig uddannelse og kapacitetsopbygning på tværs af organisationen, eventuelt gennem innovative uddannelsessamarbejder mellem Forsvarsakademiet og det eksisterende teknologiske vidensmiljø i Danmark.

Anbefaling 4 – Samarbejde: Givet tilbageholdenheden i forbindelse med at tilføje ekstra administrative årsværk, tage politiske risici og gentænke armslængdeprincippet bør Forsvarsministeriet, FKO og Forsvarsministeriets Materiel- og Indkøbsstyrelse etablere nye partnerskabsmodeller med industrien og forskningsverdenen, der er forankret uden for Forsvarsministeriets koncern, og samtidig sikre, at:

iv. Sikkerhedsgodkendelse af forskere og medarbejdere i virksomheder aktivt prioriteres
v. Kontraktrammer, der balancerer muligheden for kommercialisering af AI-modeller med Forsvarets behov for at eje AI-algoritmerne, der er udviklet på baggrund af egne data, afklares
vi. De nye partnerskabsmodeller tilføres tilstrækkelige økonomiske midler.

Anbefaling 5 – Ukrainestøtten: Forsvarsministeriet bør dedikere en separat indsats i regi af Ukrainestøtten til AI-udvikling og innovation, der får i opdrag at koble danske AI-virksomheder, danske AI-forskere og Forsvaret med de tilsvarende ukrainske aktører med henblik på konkret, operativ problemløsning på slagmarken samt hjemtagning og videreudvikling af AI-løsningerne, så de lever op til NATO's krav til ansvarlig AI.

Anbefaling 6 – Internationalt: Forsvarsministeriet og FKO bør prioritere en dansk indsats for udvikling af internationale standarder for et robust test-, evaluerings-, verificerings- og valideringsregime i tæt samarbejde med danske virksomheder og vidensinstitutioner og eventuelt i regi af NORDEFCO eller PESCO. Det ville understøtte det danske udenrigs- og sikkerhedspolitiske selvbillede som en ansvarlig småstat – også inden for militær AI.

Litteraturliste

Acheson, Ray. »Editorial: Convergence Against Killer Robots«. *CCW Report* 9, nr. 3 (2021).

AIT News Desk. »Kraken Delivers Significant Technical Upgrade for Royal Danish Navy's Mine Countermeasures (MCM) Efforts«. *AIThority News*, 11. juni 2022. https://aithority.com/robots/kraken-delivers-significant-technical-upgrade-for-royal-danish-navys-mine-countermeasures-mcm-efforts.

Angry Planet. »How Palantir is Using AI in Ukraine«. Podcast, 26. marts, 2024.

Arrieta, Alejandro Barredo et al. »Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI«. *Information Fusion* 58 (2020): 82-115.

Bajak, Frank. »Pentagon pushes A.I. research toward lethal autonomous weapons«. *CBS News*, 25. november, 2023. https://www.cbsnews.com/sanfrancisco/news/pentagon-pushes-ai-research-toward-lethal-autonomous-weapons/.

Barbosa, Lutiana V. F. »Exploring the 2023 U.S. Directive on Autonomy in Weapon Systems«. *CEBRI-Journal* 2, nr. 7 (2023): 117-136.

Barnett, Jackson. »Anduril buys small drone company, expanding its innovative tech portfolio«. *FedScoop*, 1. april 2021. https://fedscoop.com/anduril-buys-small-drone-company-expanding-innovative-tech-portfolio/.

Barnett, Jackson. »Anduril nabs $1B contract for anti-drone work with SOCOM«. *FedScoop*, 20. januar, 2024. https://fedscoop.com/anduril-nabs-1b-contract-for-anti-drone-work-with-socom/.

Bergengruen, Vera. »Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company«. *TIME*, 14. november 2023. https://time.com/6334176/ukraine-clearview-ai-russia/.

Bergengruen, Vera. »How Tech Giants Turned Ukraine Into an AI War Lab«. *TIME,* 8. februar 2024. https://time.com/6691662/ai-ukraine-war-palantir/.

Bertelsen, Jens. »Dansk virksomhed udvikler livsvigtig software til F-35 kampfly – kan overvåge malkekøer i Jylland og nedkæmpe missiler i Østersøen«. *AvisenDanmark*, 2. september 2023. https://avisendanmark.dk/erhverv/skolebus-eller-kampvogn-dansk-firma-udvikler-livsvigtig-software-til-f-35-kampfly.

Biden Jr., Joesph R. »Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence«. Præsidentielt dekret, 30. oktober 2023.

Bode, Ingvild og Hendrik Huelss. »Constructing expertise: the front- and backdoor regulation of AI's military applications in the European Union«. *Journal of European Public Policy* 30, nr. 7 (2023): 1230-1254.

Bode, Ingvild og Tom Watts. »Meaning-Less Human Control – Lessons from Air Defence Systems on Meaningful Human Control for the Debate on AWS«. Center for War Studies, SDU, 2021.

Bollmann, Anders Theis og Katja Lindskov Jacobsen. »Militær dataoversættelse og digital transformation: Erfaringer fra Ukraine og fokuspunkter for det danske forsvar«, Djøf Forlag, 2023.

Boulanin, Vincent et al. »Limits of Autonomy in Weapon Systems – Identifying Practical Elements of Human Control«. SIPRI-ICRC Report. Stockholm International Peace Research Institute, 2020.

Breitenbauch, Henrik og Jens Vesterlund Matthiesen, *Militærteknologisk situationsforståelse*. CMS Rapport. Djøf Forlag, 2021.

Breitenbauch, Henrik og Tobias Liebetrau. *Teknologikonkurrencen og dens implikationer for Danmark*. CMS Rapport. Djøf Forlag, 2021.

C3 AI. »C3 AI Readiness for Aircraft Livestream«. Webinar, 13. maj 2020. https://c3.ai/live/c3-ai-readiness-for-aircraft/.

C3 AI. »C3 AI Awarded Three New Orders from Missile Defense Agency«. 13. december 2022. https://c3.ai/c3-ai-awarded-three-new-orders-from-missile-defense-agency/.

Chahal, Husanjot, Ryan Fedasiuk og Carrick Flynn. »Messier than Oil: Assessing Data Advantage in Military AI«. CSET Issue Brief, Center for Security and Emerging Technology, 2020.

Copp, Tara. »US aims to stay ahead of China in using AI to fly fighter jets, navigate without GPS and more«. *AP News*, 12. maj 2024. https://apnews.com/article/ai-military-machine-learning-autonomy-china-gps-5f327918075cea0bfc32e5d36cba801d.

Crootof. Rebecca. »War Torts: Accountability for Autonomous Weapons«. *University of Pennsylvania Law Review* 164, nr. 6 (2016): 1347-1402.

Csernatoni, Raluca og Bruno Oliveira Martins. »Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination«. *Geopolitics* 29, nr. 3 (2024): 849-872.

CSIS. »Scaling AI-enabled Capabilities at the DOD: Government and Industry Perspectives.« Transskribering fra event, 28. marts 2024. https://www.csis.org/analysis/scaling-ai-enabled-capabilities-dod-government-and-industry-perspectives.

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

Defense Innovation Board. *Terraforming the Valley: Making the Defense Market Navigable for Startups*. DIB-rapport, Defense Innovation Board, 2023.

Defense Innovation Unit. »Blue UAS«. DIU's hjemmeside (ingen dato). https://www.diu.mil/blue-uas.

Dobriansky, John og Patrick O'Farrell. »Other Transaction Authority: Acquisition Innovation for Mission-Critical Force Readiness«. *Contract Management,* juli 2018.

Docherty, Bonnie. »Elements of a Treaty on Fully Autonomous Weapons«. Stop Killer Robots Briefing Paper, marts 2019.

Forsvaret. »Årsberetning, Forsvarskommandoen 2022«. 2023.

Freedberg Jr., Sydney J. »'Success begets challenges': NGA struggles to meet rising demand for Maven AI«. *Breaking Defence*, 3. september 2024, https://breakingdefense.com/2024/09/success-begets-challenges-nga-struggles-to-meet-rising-demand-for-maven-ai/.

GAO. *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*. Rapport til Senatets komite for de væbnede styrker. U.S. Government Accountability Office, 2018.

GAO. *Artificial Intelligence: DOD Needs Department-wide Guidance to Inform Acquisition*. Rapport til Senatets komite for de væbnede styrker. U.S. Government Accountability Office, 2023.

GAO. *Artificial Intelligence: Actions Needed to Improve DOD's Workforce Management*. Rapport til Repræsentanternes Hus' komite for de væbnede styrker. U.S. Government Accountability Office, 2023.

Garamone, Jim. »Hicks Discusses Replicator Initiative«. DOD News, 7. september 2023. https://www.defense.gov/News/News-Stories/Article/Article/3518827/hicks-discusses-replicator-initiative/.

Goldfarb, Avi og Jon R. Lindsay. »Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War«. *International Security* 46, nr. 3 (2022): 7-50.

Graae, Andreas I. »Servers Before Tanks? Defence AI in Denmark«. I *The Very Long Game – 25 Case Studies on the Global State of Defence AI*, redigeret af Heiko Borchert et al. Springer, 2024.

Graae, Andreas I. og Hans Peter H. Michelsen. »F-35, Skyborgs og den kommende sværm: Kunstig intelligens i våbensystemer«. I *Smart krig: Militær anvendelse af kunstig intelligens*, red. Iben Yde, et al. Djøf Forlag, 2021.

Grand-Clément, Sarah. »Artificial Intelligence Beyond Weapons – Applications and Impact of AI in the Military Domain«. UNIDIR Report, United Nations Institute for Disarmament Research, 2023.

Hadley, Greg. »'Wildly Successful' Skyborg Will Become Program of Record but Won't Stop Developing S&T«. *Air & Space Forces Magazine,* 16. august 2022. https://www.airandspaceforces.com/wildly-successful-skyborg-program-of-record-developing-st/.

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

Hamilton, Isobel Asher. »A former Google engineer warned that robot weapons could cause accidental mass killings«. *Business Insider*, 16. september, 2019. https://www.businessinsider.com/former-google-engineer-warns-against-killer-robots-2019-9.

Hansen, Jens Ulrik. »En Introduktion til kunstig intelligens og maskinlæring«. I *Smart Krig: Militær anvendelse af kunstig intelligens*, redigeret af Iben Yde et al. Djøf Forlag, 2021.

Henshall, Will. »The U.S. Military's Investments Into Artificial Intelligence Are Skyrocketing«. *TIME*, 3. marts 2024. https://time.com/6961317/ai-artificial-intelligence-us-military-spending/.

Hicks, Kathleen H. »(DoD) Directive 3000.09, Autonomy in Weapon Systems«. Office of the Under Secretary of Defense for Policy, 2023.

Human Rights Watch. »Killer Robots and the Concept of Meaningful Human Control: Memorandum to CCW Delegates, Human Rights Watch«. Human Rights Watch Memo, 11. april, 2023.

Jacobsen, Jeppe T. og Dennis Hansen. »Cyber- og informationssikkerhed: AI som løsning eller trussel?«. I *Smart krig: Militær anvendelse af kunstig intelligens*, redigeret af Iben Yde et al. (Djøf Forlag, 2021).

Jacobsen, Jeppe T. og Katrine Nørgaard. »Reading Security Imaginaries as Fantasies – Loss, Desire, and Enjoyment in the Military Quest for Explainable AI«. *Millennium: Journal of International Studies* 52, nr. 2 (2024): 408-433.

Jacobsen, Jeppe T. og Tobias Liebetrau. »Kunstig intelligens, militærstrategi og international konkurrence«. I *Smart krig: Militær anvendelse af kunstig intelligens*, redigeret af Iben Yde et al. Djøf Forlag, 2021.

Jacobsen, Jeppe T. og Tobias Liebetrau. »Artificial Intelligence and Military Superiority – How the 'Cyber-AI Offensive-Defensive Arms Race' Affects the US Vision of the Fully Integrated Battlefield«. I *Artificial Intelligence and International Conflict in Cyberspace*, redigeret af Fabio Cristiano et al. Routledge, 2023.

Jacobsen, Jeppe T. og Tobias Liebetrau. »Big tech at war: The infrastructural politics of public-private relations«. *European Journal of International Relations*, under udgivelse.

Jakobsen, Peter Viggo og Steen Rynning. »Denmark: Happy to fight, will travel«. *International Affairs* 95, nr. 4 (2019): 877-895.

Jensen, Benjamin M., Christopher Whyte, og Scott Cuomo. »Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence«. *International Studies Review* 22, nr. 3 (2020): 526-550.

Kahn, Lauren A. *Risky Incrementalism: Defense AI in the United States.* Rapport Defense AI Observatory, 2023.

Kahn, Lauren og Michael C. Horowitz. »Two Cheers for the Department of Defense's New Data and Artificial Intelligence Leadership Initiative«. CFR Blog, 1. december 2021. https://www.cfr.org/blog/two-cheers-department-defenses-new-data-and-artificial-intelligence-leadership-initiative.

King, Anthony. »Digital Targeting: Artificial Intelligence, Data, and Military Intelligence«. *Journal of Global Security Studies* 9, nr. 2 (2024): 1-16.

Lindsay, Jon R. »War Is from Mars, AI Is from Venus: Rediscovering the Institutional Context of Military Automation«. *Texas National Security Review* 7, nr. 1 (2023): 30-47.

Lushenko, Paul. »Trust but verify: U.S. troops, artificial intelligence, and an uneasy partnership«. Brookings Commentary, 22. januar 2024. https://www.brookings.edu/articles/trust-but-verify-u-s-troops-artificial-intelligence-and-an-uneasy-partnership/.

Marrow, Michael. »In a 'world first,' DARPA project demonstrates AI dogfighting in real jet«. *Breaking Defense*, 9. april 2024. https://breakingdefense.com/2024/04/in-a-world-first-darpa-project-demonstrates-ai-dogfighting-in-real-jet/.

Michel, Arthur Holland. »The Black Box, Unlocked: Predictability and Understandability in Military AI«. Report. United Nations Institute for Disarmament Research, 2020.

Mulchandani, Nand og John N.T. 'Jack' Shanahan. *Software-Defined Warfare – Architecting the DoD's Transition to the Digital Age*, CSIS Rapport, Center for Strategic and International Studies, 2022.

National Academies of Sciences, Engineering, and Medicine. *Test and Evaluation Challenges in Artificial Intelligence-Enabled Systems for the Department of the Air Force*. Consensus Study Report. The National Academies Press, 2023.

NATO. »Summary of the NATO Artificial Intelligence Strategy«. Officiel tekst, 22. oktober 2021. https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

Navy Lookout. »Last ditch defence – the Phalanx close-in weapon system in focus«. Technical Briefing, 10. august 2020. https://www.navylookout.com/last-ditch-defence-the-phalanx-close-in-weapon-system-in-focus/.

Palantir. »Palantir AIP – Defense and Military«. YouTube. 25. april 2023. https://www.youtube.com/watch?v=XEM5qz__HOU.

Pettyjohn, Stacie L. »Drones are Transforming the Battlefield in Ukraine But in an Evolutionary Fashion«. *War on the Rocks*, 5. marts 2024. https://warontherocks.com/2024/03/drones-are-transforming-the-battlefield-in-ukraine-but-in-an-evolutionary-fashion/.

Ramachandra, Gautam. »How Artificial Intelligence is improving the Iron Dome«. Medium, 13. maj 2023. https://medium.com/@gautamrbharadwaj/how-ai-is-improving-iron-dome-3894cd3668f9.

Regeringen. »Regeringens strategi for dansk forsvarsindustri – Styrket samarbejde for dansk sikkerhed«. 2021.

Reichborn-Kjennerud, Erik. »Krig i en verden av fremmed intelligens«. I *Digitalisering og internasjonal politikk*, redigeret af Håkon Bergsjø og Karsten Friis. Scandinavian University Press, 2022.

Renic, Neil. »Tragic Reflection, Political Wisdom, and the Future of Algorithmic War«. *Australian Journal of International Affairs* 78, nr. 2 (2024): 247-256.

Renic, Neil og Elke Schwarz. »Crimes of Dispassion: Autonomous Weapons and the Moral Challenge of Systematic Killing«. *Ethics & International Affairs* 37, nr. 3 (2023): 321-343.

Rickli, Jean-Marc og Federico Mantellassi. *The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare*. Geneva Paper 34/24. Geneva Centre for Security Policy, 2024.

Saballa, Joe. »Palantir Awarded $480M to Prototype US Army's 'Maven' AI Battlefield Analyzer«. *The Defense Post*, 24. maj, 2024. https://www.thedefensepost.com/2024/05/30/palantir-maven-battlefield-analyzer/?utm_content=cmp-true.

Sayler, Kelley M. *Artificial Intelligence and National Security*, Congressional Research Service Report, 2020.

Sayler, Kelley M. »Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems«. Congressional Research Service – In Focus, opdateret 1. februar 2024.

Scharre, Paul. *Four Battlegrounds – Power in the Age of Artificial Intelligence*. W. W. Norton & Company, 2024.

Scharre, Paul og Michael C. Horowitz. *Artificial Intelligence: What Every Policymaker Needs to Know*. The Artificial Intelligence and International Security Series, Center for New American Security, 2018.

Schelbech, Jan. »Norden kan sætte NATOs dagsorden for Østersøområdet«. *FMI Nyheder*, 30. maj 2024. https://www.fmi.dk/da/nyheder/2024/norden-kan-satte-natos-dagsorden-for-ostersoomradet/.

Schwarz, Elke. »Autonomous Weapons Systems, Artificial Intelligence, and the Problem of Meaningful Human Control«. *The Philosophical Journal of Conflict and Violence* 5, nr. 1 (2021): 53-72.

SCO. »The Strategic Capabilities Office – Perdix Fact Sheet«. DoD fact sheet, 9. januar 2017.

Shield AI. »Shield AI Joins Air Force's $950 million JADC2 effort«. Pressemeddelelse, 6. juli 2022. https://shield.ai/shield-ai-joins-air-forces-950-million-jadc2-effort/.

Soare, Simona R. »European Military AI: Why Regional Approaches Are Lagging Behind«. I *The AI Wave in Defence Innovation – Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*, redigeret af Michael Raska og Richard A. Bitzinger. Routledge, 2023.

Stanley-Lockman, Zoe. »US governance of AI for National Security«. I *The AI Wave in Defence Innovation – Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*, redigeret af Michael Raska og Richard A. Bitzinger. Routledge, 2023.

Suchman, Lucy. »Imaginaries of omniscience: Automating intelligence in the US Department of Defense«. *Social Studies of Science* 53, nr. 5 (2022): 761-786.

Svenmarck, Peter et al. »Possibilities and Challenges for Artificial Intelligence in Military Applications«. NATO Big Data and Artificial Intelligence for Military Decision Making – Specialists' Meeting, Bordeaux, 2018.

Tarraf, Danielle et al. *The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations*. RAND Corporation, 2019.

TERMA. »Terma will lead one EU-funded R&D project, participate in two others«. TERMA News, 2. juli 2021. https://www.terma.com/news-events/news/news-archive/2021/terma-will-lead-one-eu-funded-rd-project-participate-in-two-others/.

Tharoor, Ishaan. »Israel offers a glimpse into the terrifying world of military AI«. *The Washington Post,* 5. april 2024. https://www.washingtonpost.com/world/2024/04/05/israel-idf-lavender-ai-militarytarget/.

Trabucco, Lena. »International Humanitarian Law and Lethal Autonomous Weapons Systems – Legal Considerations for Acquisition and Procurement«. CMS Rapport. Djøf Forlag, 2023.

Trevithick, Joseph. »Navy Special Ops Has Adapted RQ-21 Blackjack Drones To Deploy Smaller Quadcopters«. *The War Zone*, 20. december 2021. https://www.twz.com/43568/navy-special-ops-has-adapted-rq-21-blackjack-drones-to-deploy-smaller-quadcopters.

Tucker, Patrick. »How AI Could Predict the Damage to Ukraine from Russian Missiles«. *Defense One*, 9. januar 2023. https://www.defenseone.com/technology/2023/01/how-ai-could-predict-damage-ukraine-russian-missiles/381633/.

U.S. DoD. »Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's competitive edge«. U.S. Department of Defense, 2018.

U.S. DoD. »Summary of the 2018 Department of Defense Artificial Intelligence Strategy – Harnessing AI to Advance Our Security and Prosperity«. U.S. Department of Defense, 2018.

U.S. DoD. »DoD Digital Modernization Strategy«. U.S. Department of Defense, 2019.

U.S. DoD. »DOD Adopts Ethical Principles for Artificial Intelligence«. Pressemeddelelse, 24. februar 2020. https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

U.S. DoD. »DoD Data Strategy: Unleashing Data to Advance the National Defense Strategy«. U.S. Department of Defense, 2020.

U.S. DoD. »Department of Defense Software Modernization Strategy«. U.S. Department of Defense, 2021.

U.S. DoD. »DoD Zero Trust Strategy«. U.S. Department of Defense, 2022.

U.S. DoD. »U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway«. U.S. Department of Defense, 2022.

U.S. DoD Joint AI Center. *DoD AI Education Strategy – Cultivating an AI Ready Force to Accelerate Adoption.* U.S. Department of Defense, 2020.

Weisgerber, Marcus. »The Pentagon's New Artificial Intelligence Is Already Hunting Terrorists«. *Defence One*, 21. december 2017. https://www.defenseone.com/technology/2017/12/pentagons-new-artificial-intelligence-already-hunting-terrorists/144742/.

Yde, Iben. »Introduktion«. I *Smart Krig: Militær Anvendelse Af Kunstig Intelligens*, redigeret af. Iben Yde et. al. Djøf Forlag, 2021.

Yde, Iben. »Sorte bokse, kontroltab og ansvarsflugt: Folkeretten og militær anvendelse af kunstig intelligens«. I *Smart krig: Militær anvendelse af kunstig intelligens*, redigeret af Iben Yde et al. Djøf Forlag, 2021.

OM FORFATTEREN

Jeppe T. Jacobsen, ph.d., er strategisk rådgiver og informationschef hos Nationalt Forsvarsteknologisk Center. Jeppe har de seneste 13 år forsket i cybersikkerhedspolitik, cyberkrig og den militære anvendelse af nye, disruptive teknologier både på Dansk Institut for Internationale Studier og Forsvarsakademiet.

9 788757 464658